ISSN : 2456-3307

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Techno Science Academy
The International Open Access Publisher

IJSRCSEIT

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"

Organized by
School of Computer Science,
MIT-World Peace University (MIT-WPU), Kothrud,
Pune, Maharashtra, India

Volume 8, Issue 6, January-February-2022

INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN COMPUTER SCIENCE, ENGINEERING AND INFORMATION TECHNOLOGY

Email: editor@ijsrcseit.com

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"

On

28th Feb, 2022

Organized by

School of Computer Science, MIT-World Peace University (MIT-WPU), Kothrud, Pune, Maharashtra, India

In association with

International **J**ournal of **S**cientific **R**esearch in **C**omputer **S**cience, **E**ngineering and **I**nformation **T**echnology

ISSN : 2456-3307

Volume 8, Issue 6, January-February-2022

Published By

website : www.technoscienceacademy.com

Chief Patron

Revered Prof. Dr. Vishwanath D. Karad

UNESCO Chair Holder, Founder & Chief Patron,

MAEER's MIT, Pune & President, MIT-WPU

Patron

Rahul V. Karad

Managing Trustee, MAEER's MIT

Executive President, MIT-WPU

Chairman

Dr. R. M. Chitnis

Vice Chancellor, MIT-WPU

Co-Chairman

Dr. Prasad D. Khandekar

Dean FoET, MIT-WPU

Chief Guest - Inauguration

Dr. R. Saravanan

Professor and Dean

Vellore Institute of Technology

Keynote Speakers

Dr. Susan Lincke

Director MSCIS Program,

Chair Computer Science Department,

University of Wisconsin, Parkside, USA

Chief Guest – Valediction

Prof. Dr. Umesh Deshapande

Visvesvaraya National Institute of Technology,

Nagpur, Maharashtra

Prof. Dr. Madhuri Bhavsar

Head of Department, Computer Science &

Engineering, Nirma University, Ahmedabad

Conveners

Dr. Shubhalaxmi Joshi

Associate Dean, Faculty of Science, MIT-WPU

Co-Conveners

Dr. Chandrashekhar Patil

Head of School of Computer Science, MIT-WPU

Dr. Rajeshree Khande

Associate Head of School of Computer Science,

MIT-WPU

About the Conference

On the occasion of Science day on 28th February, the Faculty of Science at MIT World Peace University is organizing Science week from 28th February 2020 to 4th March 2022. The School of Computer Science is hosting National Students' Research Conference on 28th February 2022. The theme of this conference revolves around sustainable frameworks using technology. This conference provides a platform for budding researchers to present their ideas and solutions in the form of Poster and Paper Presentation. The conference brings together academicians, research scholars and industry experts to present, share and discuss technical work in emerging topics like Artificial Intelligence, Blockchain technology, Cyber Security and IoT.

About MIT-WPU

MIT-World Peace University (MIT-WPU) is defined as one of the top education institutions in India since its establishment of the MIT Group of Institutes in 1983. The 'MIT World Peace University' is recognized by the UGC under the Govt. of Maharashtra Act XXXV 2017, since 2017. Today MIT-WPU is at the epicenter for imparting a holistic value-based education for the promotion of a universal culture of peace and welfare among the youth Looking at the rapid growth & expansion of the MIT Group now encompasses 10+ campuses across India covering more than 1000

acres, all equipped with state-of-the-art infrastructure and amenities. At any given point in time, more than 50,000 students are pursuing various courses across 65+ Institutes of MIT World Peace University.

About Faculty of Science

The Faculty of Science at MIT-WPU offers numerous higher learning courses as well as research programs. We pride ourselves on developing skilled professionals who excel at addressing myriad issues. During their period of study under the Faculty of Science, students are expected to spend more time in laboratories than in classrooms. Our specially crafted Industry oriented curriculum helps to bridge the gap between academics and the industry. Our Teaching and Research endeavours are supported by the state of art infrastructure that we possess as well as the qualified and highly competent teaching faculty members who provide students with hands-on practical experiences.

CALL FOR PAPERS

The Conference invites original research papers and contributions in the following domains/tracks but not limited to:

- **Artificial Intelligence and Machine Learning**
  - Machine Learning
  - Deep Learning
  - Predictive & Prescriptive Analysis
  - Human Machine interface
  - Robotics & Cognitive Computing
- **Blockchain Technology & Internet of Things**
  - Blockchain Ecosystem
  - Blockchain Architecture
  - IoT for Social Sustenance
  - Energy harvesting sensors
  - IoT architecture design and optimization
- **Network/Information/Cyber Security**
  - Security and privacy in online social networks
  - Cyber Security applications in AI/ML/IoT
  - Privacy-preserving computing
  - Other new cryptographic primitives
- **Data Science and Big Data**
  - Big Data Management and Technology
  - Data intensive systems for efficient and distributedtraining
  - Green, energy - efficient models and sustainabilityissues for Big Data
- **Others**
  - Software engineering Applications
  - Cloud Computing
  - Augmented Reality and Virtual Reality
  - Computational Mathematics
  - Other topics related to ICT and its Applications

CONTENTS

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

A Study on Node Failure Detection Techniques In Software Defined Networks

Pragati Gandhi[1], Neetu Gyanchandani[2], Gayatri Bhoyar[3]
[1]M.Tech Student, Department of Electronics & Telecommunication, JD College of Engineering and Management, Nagpur, Maharashtra, India
[2,3]Assistant Professor, Department of Electronics & Telecommunication, JD College of Engineering and Management, Nagpur, Maharashtra, India

ABSTRACT
Software Defined Networking (SDN) is considered as a promising approach in networking paradigm. It distinguishes the control plane of the network from the plane which is used for data forwarding. This technique not only helps in optimal resource utilization in the network, but it also simplifies the complexity in management of the network, reduces the operating cost of the network and also encourages the innovative and evolutionary ideas. An emerging way to achieve this requirement that optimizes a network and helps in the improvisation of the network robustness is traffic engineering. Traffic Engineering can reduce link failure and service degradation in the network. Research communities have worked a lot on methods for traditional networking structures, which allows the network to adapt to the changes in traffic patterns. This paper mainly focuses on the review of the various state of the art methods for traffic engineering for Software Defined Network. It mainly concentrates on the techniques for traditional network architecture and to study the challenges in the implementation and future scope of such methods.

Keywords :— Traffic Engineering, Software Defined Networking, Linear Programming, Failure Recovery, Optimal Rerouting

I. INTRODUCTION

The entire set of activities is linked together via the internet or networking. The internet is made up of a huge number of devices, such as switches, routers, servers, and host systems, that work together. Routers and switches are the most common components of a traditional network. A network is made up of a collection of protocols that have been statically defined in routers and switches, for example. The current network design only partially serves the needs of today's businesses, carriers, and end users. In routers, control and forwarding rules are defined statically, rather than dynamically. Changing patterns, applications, and user demand are not well served by the network architecture that is currently in place. SDN (software-defined networking) is a developing technique that aims to alter present network architecture.

An administrator controls the flow of information across the control plane [1] and the data plane [2]. Open Flow [3] is a communication protocol that allows a network switch to communicate with a router across the network or forwarding plane. In the control plane, open flow specifies a standard for all event

processing that occurs between the controller and the data plane switch or router.

The traffic is moved by the data plane. It takes hold of the forwarding table, which specifies the interface to which the packet will be sent, and moves it to the foreground. The actions of the data plane are determined by the actions of the control plane. Depending on the configuration, the SDN network might be centralised or decentralised. A single controller manages the flow table of all switches in a centralised configuration. In contrast, numerous controllers are unscrewed and distributed among multiple sites in a decentralised configuration to manipulate the flow table as Hyper flow. SDN is reliant on the controller's ability to function; if the controller fails, everything but the traffic going through switches will be stopped according to the rules that were previously installed in the flow table before the controller failed. The controller acts as the "brain" of the SDN architecture, and its performance has the greatest impact on the overall throughput.

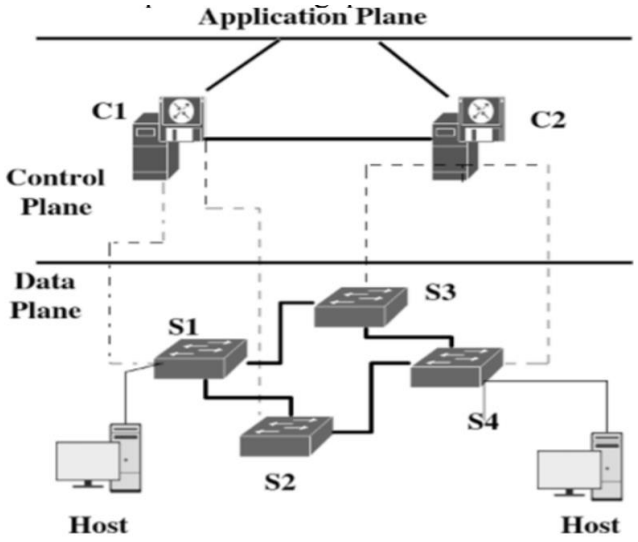


Figure 1. Traditional Network Architecture

To overcome these issues the researchers are working on traffic engineering and proposed many new methods to improvise the robustness of the network with respect to the increase in the demands of the network traffic. Fault tolerance plays a crucial role in network management and it is one of the important features of any network. It ensures that if a there is a failure in the network, the request from the user for accessing any data can still be delivered to the destination. The computer network is a structure which contents the number of networking devices, such as routers, switches, and security firewalls. The traditional structure of the network is distributed, as shown in Fig. 1. Here each networking device contents both the control plane as well as the data plane. The control plane is the intelligent part of networking devices with a role in decision making about the routing and forwarding data. Whereas the data plane carries and manages the user traffic in the network. In simple words, it follows the instructions given by the control plane's and forwards the data.

Network administrators need to physically arrange these multivendor gadgets to react to an assortment of utilization and occasion in the network. This makes the administration and improvement of a network troublesome, which can present blunders in the network. Different issues with this engineering can cause motions in the network since control planes of the gadgets are appropriated, development is troublesome on the grounds that the merchants forbid alteration of the hidden software in the gadgets.

For the purpose of safeguarding the data pane, there are two types of mechanisms. The first regression and recovery path can be allocated in a dynamic manner. Additional resources are neither planned nor available. Failure must be communicated to the user through signalling. The pathways are reserved before a link fails as a second layer of protection. This method does not necessitate the use of signals. Protection can be used to keep the control plane safe. A number of controllers have been set aside as backups. When a controller fails, a backup controller is automatically activated and takes over for the failed controller. Because more instances of controllers are necessary to boost dependability, it is critical to determine how many backup controllers are required and where these backup controllers should be installed.

II. Literature Review

An extraordinarily efficient traffic rerouting method is proposed in this study [5] to deal with constructing an optimal BPT for a connection on a given topology and traffic vector, which is referred to as Universal Single-interface Traffic Rerouting. USTR can find out a (1+)-ideal BPT that has an optimality dimension that is indistinguishable from LPTR by using a productive method. When it comes to TE execution, USTR is on par with LPTR and far better than CSPF. When it comes to running time, USTR is a couple of requests of brilliance faster than LPTR and nearly identical to CSPF in terms of performance. The operating period of USTR is totally justified in order to ensure that all of the connections are maintained during the TE gap. In this example, the creator uses SDN to execute a USTR model and verify the model's execution. The controller is designated as ODL because it is capable of operating in OpenFlow, MPLS, and IP networks. In the information plane of the reinforcement direction, ODL makes use of VLAN ID to carry out name transmitting operations on the network.

During the course of this paper [6,] IP rapid reroute algorithms are used to recover packages in the information plane when a connection failure occurs. Previous research has identified ways that ensure disappointment recovery from disappointments with a maximum of two connections. In a k-edge-associated network, we provide an IP rapid reroute technique that makes use of established curve disjoint spreading over trees to assure recovery from interface failures of up to (k-1) magnitude. The fact that bend disjoint traversal trees may be created in sub-quadratic time to the size of the network means that our technology is extremely adaptable and flexible. Based on our findings in the exploration phase, we demonstrate that using circular segment disjoint crossing trees to recover from various disappointments reduces the amount of time spent in comparison with recently discovered approaches in the examination phase.

If a switch or a connection fails in a circuit exchanging or a bundle exchanging network, the parcels that are travelling on the failed connection, way, or switch will be lost and dropped until the network self-re-meets, notwithstanding the fact that a substitute way exists that keeps a strategic distance from or bypasses the network disappointment. During this time period, the specific targets will not be reachable from the source, resulting in increased network traffic and a deterioration of the network's quality characteristics. The network re-merges procedure necessitates a significant amount of energy and can take anything from a few milliseconds to many seconds. The Internet Engineering Task Force (IETF) developed a distributed IP Fast ReRoute (IPFRR) system to address this issue [7]. When an IPFRR system failure occurs, many different guiding conventions are created in order to recover the network from this type of failure.

Several solutions for dealing with "the network structure issue with availability prerequisites" are discussed in this research [8]. They plan a base cost network (beginning from the earliest stage) that is ready to transmit its requests without clogging under a specific arrangement of disappointment conditions, each of which consists of a large number of connection failures, in order to avoid clogging. Following the disappointments of the double-edged sword, a few plans have been offered for distributing the network. Generally speaking, these do not address the issue of anticipating clog (other than by multiplying limits where streams cover). Furthermore, they do not actually add up to disappointments from a larger selection. A few studies have been recommended to widen the development of disjunct trees.

An answer reliably exists for all twofold edge disillusionments as long as the network graph is 3-related, and a heuristic is provided in this investigation [9]. An alternative method of dealing with disillusionments in pre-configured support routes is to re-configure the routes themselves. This document discusses and describes the philosophy that underpins

our arrangements, as well as the prologue to those arrangements. The fact that the fortification path for the second failed edge is chosen based on the right learning of what has already tumbled makes reconfiguration an incredible framework since it provides an incredible framework (instead of dealing with each and every possible dissatisfaction). In a similar vein, reconfiguration contrivances add up to more feasible to higher-assortment frustrations in the long run. Regardless, and not in the least as our most cynical situation ensures, the emphasis is on the evaluation and structure of reconfiguration plans in the context of a settled veiled network. The work in also takes into account the re-provisioning of support routes, but only up to the level of affiliation. There is a significant amount of work being done on "p-cycles." A p-cycle is a cycle of unit limit that has been preconfigured and created from as many nodes as possible in the network. When dissatisfactions occur on the cycle, it acts in a similar way to "straddling" ranges with both end-centers around the cycle in that it allows for quick recreating.

Even though the basic structure was originally recommended for single disillusionments [10], it has since been enhanced to include twofold dissatisfactions as well as SRG (shared peril gathering) disappointments. While one of our arrangements does make use of cycles, it does so on an incredibly important dimension that is distinct from that of p-cycles, as we shall see. There is no p-cycle improvement that can guarantee blockage free modifying for an infinite number of frustrations, to the extent that anyone is concerned about it. Furthermore, whereas numerous studies on p-cycles propose number direct tasks (ILPs) to identify "perfect" cycles in a given network, we propose a clear (and practically perfect) design of edges that can be implemented with guaranteed execution and without estimation into a network.

In this paper [11], an ILP is presented that provides a fundamental stream errand (with stream part) and a "stream redistribution" plot that guarantees no blockage with k frustrations under the following condition: given any set F of edges with full scale utilization up to k, all of the streams can be directed on F without stop up under the following condition: However, while their research is close to but not exactly equivalent to our own, they provide proof on the existence of a network that fulfils a pre-condition without explicitly considering the most efficient approach to put together such a structure.

In this research [12], a fast-reroute method is used specifically to build up reinforcement paths during interface disappointments; nevertheless, it is not successful for the different disappointments that can occur in spine networks on a regular basis due to the nature of the network. Consider the following scenario: a convention is established to rearrange affected reinforcement ways following a connection disappointment, hence increasing survival from a subsequent disappointment. Spine networks with switch-to-switch connections carry the traffic of various start-to-finish connections. All of the associations going through the interface that experience failure fizzle out on the off chance that a failure occurs at the interface level. The primary emphasis is on reestablishing complete and total relationships through the use of transportation security systems. Despite the fact that insurance is beneficial in asset utilisation, it has the disadvantages of a more complex nature, limited adaptability, and lengthy recovery times that are required. The purpose of MPLS rapid reroute in connection security is to pre-process exchange ways in order to deal with double connection failures, and the advantages of doing so are becoming increasingly astounding. Because a first connection disappointment may have an impact on the reinforcement way of a second connection, the pre-processed reinforcement ways for each connection would need to account for every potential combination of disappointments from various connections in order to be effective.

Using this paper [13], the authors describe the most effective method for developing perfect sets of trees for weighted coordinated charts. Divides occurrence edges to any hub into "insurance charts," which look similar to one of the options available after a disappointment: the first disappointment is managed by assurance diagrams, and the second by disjoint trees. Considers the problem of finding the largest possible arrangement of preconfigured FRR reinforcement routes in the context of the following situation. Pretend a second disappointment, e2, arises in the reinforcement way of a first fizzled edge, e1, and is fixed by utilising the reinforcement way of e2 to fix it. At that time, this reinforcement method should be excluded from consideration. There is a heuristic provided.

III. Conclusion

The study presented here is a review of existing literature and researches conducted in the area of traffic engineering. Some of the methods are applicable for traditional network structure where as some are related to the techniques developed for SDN. The challenges related to the implementation and future enhancement required for the up gradation of the systems are also discussed. Software Defined Networking (SDN) is a promising approach in networking paradigm. It distinguishes the control plane of the network from the plane which is used for data forwarding. It enables and provides the solution for many problems in the traditional network architecture. It reduces the complexity in network management by managing the network centrally. It also presents the network programmability and providing a global view of a network and its state.

IV. REFERENCES

[1]. T. Elhourani, A. Gopalan, and S. Ramasubramanian, “Ip fast rerouting for multi-link failures,” in IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, April 2014, pp. 2148–2156.

[2]. Q. She, X. Huang, and J. P. Jue, “Survivable routing for segment protection under multiple failures,” in OFC/NFOEC 2007, March 2007, pp. 1–3.

[3]. H. Kim, M. Schlansker, J. R. Santos, J. Tourrilhes, Y. Turner, and N. Feamster, “Coronet: Fault tolerance for software defined networks,” in ICNP ’12, Oct 2012, pp. 1–2.

[4]. B. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, “A survey of software-defined networking: Past, present, and future of programmable networks”, IEEE Commun. Surv. & Tutor., vol. 16, no. 3, pp. 1617–1634, 2014.

[5]. Anmin Xu, Jun Bi, Baobao Zhang, Tianran Xu, Jianping Wu, "USTR: A High-performance Traffic Engineering Approach for the Failed Link", 38th International Conference on Distributed Computing Systems, IEEE 2018.

[6]. Theodore Elhourani, Abishek Gopalan, Srinivasan Ramasubramanian, “IP Fast Rerouting for Multi-Link Failures”, IEEE/ACM Transactions on Networking Volume: 24, Issue: 5, October 2016.

[7]. Mahesh Bhor, Deepak Chatrabhuj Karia, “Network recovery using IP fast rerouting for multi link failures”, International Conference on Intelligent Computing and Control (I2C2), IEEE Xplore: March 2018.

[8]. Rakesh K. Sinha, Funda Ergun, Kostas N. Oikonomou, K. K. Ramakrishnan, “Network Design for Tolerating Multiple Link Failures Using Fast Re-Route (FRR)”, IEEE , 2014.

[9]. Ajay Todimala, K. K. Ramakrishnan and Rakesh K. Sinha, “Cross-layer Reconfiguration for Surviving Multiple-link Failures in Backbone Networks”, IEEE, 2009.

[10]. Rozita Yunos, Siti Arpah Ahmad, Noorhayati Mohamed Noor, Raihana Md Saidi, Zarina Zaino, “Analysis of Routing Protocols of VoIP VPN over MPLS Network”, 2013 IEEE Conference on Systems, Process & Control (ICSPC2013), 13 - 15 December 2013

[11]. Cezary ˙ Zukowski, Artur Tomaszewski, Michał Pióro, David Hock, Matthias Hartmann and Michael Menth, “Compact node-link formulations for the optimal single path MPLS Fast Reroute layout”, ADVANCES IN ELECTRONICS AND TELECOMMUNICATIONS, VOL. 2, NO. 3, SEPTEMBER 2011

[12]. Maria Hadjiona, Chryssis Georgiou and Vasos Vassiliou, “A Hybrid Fault-Tolerant Algorithm for MPLS Networks”, Department of Computer Science University of Cyprus.

[13]. Suksant Sae Lor, Redouane Ali, Raul Landa, and Miguel Rio, “Recursive Loop- Free Alternates for Full Protection Against Transient Link Failures, IEEE, 2010.

Cite this Article

Pragati Gandhi, Neetu Gyanchandani, Gayatri Bhoyar, "A Study on Node Failure Detection Techniques In Software Defined Networks", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 6, pp.01-06, January-February-2022.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Implementation of Machine Learning Model in Digital Forensic Investigation

Alisha Sonwane, Rajat Sontakke, Rohini Badole, Kuldeep Kapgate, Sushant Seware, Rohan Kokate
Department of Computer Science and Engineering, J.D College of Engineering and Management, Nagpur, Maharashtra, India

ABSTRACT

Now a days visual data are massively increasing due to popularity of a smart devices and low cost surveillance system, that data is utilized in investigation of digital forensic. Whenever crime occurs for finding criminal, evidences a digital videos have been hugely utilized as a main source of evidence. By using digital videos police are able to identify, analyze, present and report evidences. Here key objective is to develop enhanced forensic video analysis technique for helping process of forensic investigation. For that forensic video examination framework need to propose which will act as an efficient video improving algorithm for examination of low quality footage. For enhancing the CCTV footage quality introduced an adaptive video enhancement algorithm depends on a CLAHE. And for helping the video based forensic investigation Convolution neural network (CNN) algorithm proposed that can identify and recognize suspects, tools used from footage. CNN utilized for detecting knife, blood and gun to prediction whether crime has occurred.

Keywords :— Forensics Investigation, Forensic Video Analysis, Video/Image Enhancement, Convolution Neural Network.

I. INTRODUCTION

crime scene prediction from a camera is very crucial task while working on a computer vision. In modern technology, people setup surveillance cameras in numerous areas to get rid of crime or protect from criminal, thief, unknown peoples and stokers. Still, it cannot help people as quick as people want to respond but help to cops after crime occurs. Usually after occurring a crime scene, law enforcement agencies come to this place and collect the footage from the video that was recorded at the time of crime scene. Then, law enforcement agencies examine the video and take required evidence of crime scene from footage if it is helpful. We believe this is very slow process to act on a crime scene. For this reason, we wanted to make a system that can quickly act on a crime scene to detect the criminal.

Moreover, there are a number of cameras being installed in various areas by law enforcement agencies or by any company. They have to monitor all the cameras at a time with human being. If a computer system can detect the threatening objects and give alert to the authority just after detection of threatening objects, the proper authority can quickly take action to stop the potential criminal before he commits any crime. Hence such system can prevent crime to occur. Some dangerous incident helped us to think more deeply to make a system that can be learned to identify threatening objects. Here for

detecting revolver, machine gun, shot gun, blood and knife utilized convolutional neural network.

To implement this utilized a convolutional neural network. Because a simple neural network cannot give desired result. Therefore, utilized convolutional neural network to get better result.

The section I explains the Introduction. Section II presents the literature review of existing systems and Section III present proposed system architecture Section VI concludes our proposed system. While at the end list of references paper are presented.

II. Literature Review

M. F. E. M. Senan, S. N. H. S. Abdullah, W. M. Kharudin et al [1] utilized Closed-circuit television (CCTV) for surveillance recordings and it act as digital device for collecting digital evidence. In forensic analysis CCTV recording utilized for examining the footage with target is extracted from CCTV. Because of numerous reasons quality of this recording is poor these reason consist of type of camera and its configuration and location where it is installed. Hence the face recognition in forensic analysis is based on CCTV recording quality. If quality of recording is poor then it would decrease confidence in criminal detection and hence it affect in evidence collection and presentation in court. Here author divide research task in two parts. First part consist of CCTV evidence testing task where the experiment was done depends on various types of CCTV cameras using distinct resolutions, and distances among the subject and the camera. In the second part, comparison between the face of the subjects and the face taken during the enrolment task takes place. The score generated from the forensic face recognition system would be totally depends on the camera resolutions, types of camera, distance among them, and also on the changes of ranking score after applying the enhancement process like Bicubic to the facial images.

G. Gilboa, N. Sochen, and Y. Y. Zeevi, et al [2] present image enhancement and denoising by utilizing complex diffusion processes.

S. Park, S. Yu, M. Kim, K. Park, and J. Paik et al [3] presents a model of dual autoencoder network which is depends on the retinex theory to perform the low-light enhancement and noise reduction and is done by combining the stacked and convolutional autoencoders. This method calculate illumination component utilizing a stacked autoencoder and then utilized convolutional auto encoder which deals with 2-D image information for reducing noise in brightness enhancement process.

W. Fan, K. Wang, F. Cayre, and Z. Xiong et al. [4] proposed an image variational de-convolution framework for quality enhancement and anti-forensics of median filtered (MF) images. The proposed optimization based framework contains a convolution term, a fidelity term w.r.t the MF image, and prior term. Median filtering utilized by anti-forensic researchers for distinguishing traces. The proposed method act as MF image quality enhancement technique.

C. Li, J. Guo, R. Cong, Y. Pang, and B. Wang et al [5] proposed method known as a systematic underwater image enhancement, this method consist of underwater image dehazing algorithm and contrast enhancement algorithm. Images clicked under water are normally degraded because of effects of scattering and absorption. For mitigating the limitations of underwater images author proposed image enhancement method. Dehazing algorithm is proposed for restoration of the color visibility and appearance of underwater images and contrast

enhancement algorithm is proposed for enhancing the brightness and contrast of underwater images.

S. Mandal, X. L. Deán-Ben, and D. Razansky, et al[6] proposed active contour segmentation priors for enhancing Visual quality in optoacoustic tomography. Segmentation is very essential task in biomedical images and also it is helpful in study of anatomical structures.

H. Walker and A. Tough et al [7] studied investigation process by using CCTV footage, it is commonly utilized in court for presenting crime and t help to identify criminal. It is difficult to identify the criminal because quality of images produced by surveillance cameras. The objective of this research is to determine the task of recognizing the offender in CCTV footage was one which a jury should be proficient to do or whether expert evidence would be beneficial in such cases. Here online survey is taken and role of jury is performed by participant.

E. Verolme and A. Mieremet et al [8] studied applications of forensic image analysis in accident investigations. Forensic investigations are mainly for collecting objective answers that can be utilized for criminal prosecution. Accident analysis are generally done to gain knowledge from similar events and utilized to prevent occurring similar incident in future. The use in accident inquiry means that more evidence can be generated from the present information than when utilized in criminal investigations, hence the latter need a higher evidence level. Here author studied cases of same field for accident investigation. The information is gathered from CCTV footage utilizing forensic image analysis techniques. This gathered information act as very crucial in detecting events. Hence this technique learn from accident and preventing future accidents.

III. SYSTEM ARCHITECTURE

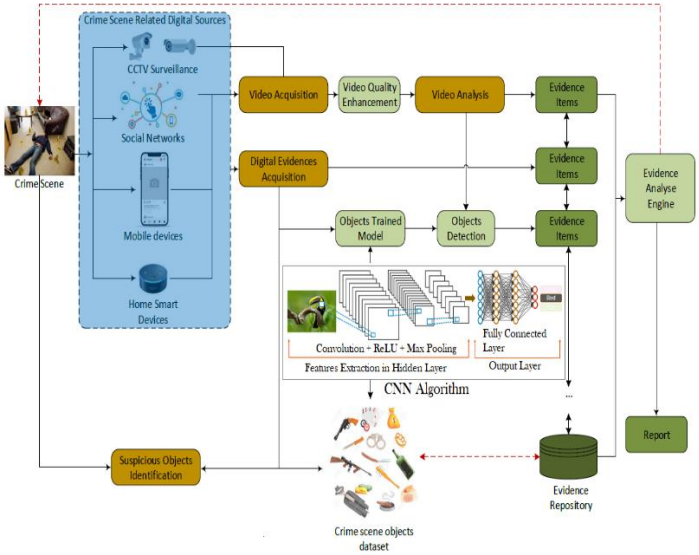


Fig 1. System Architecture

Following Fig. 1 Shows the proposed system architecture. First digital source related to crime scene are find and collected information from that sources. These digital sources consist of CCTV surveillance, mobile devices and smart devices. Then acquisition of evidences from these sources takes place in the form of video or digital. Then quality of video is enhanced using enhancement algorithm. Then evidence are collected and objects are identified using CNN algorithm.

Convolutional Neural Networks

CNN is a type of profound, feed-forward neural artificial network used to achieve exact output in computer vision tasks, such as image classification and detection [5]. Unlike the traditional neural network, CNNs are also deeper in layers. It has weights, distortions and results by non-linear activation. The CNN's neurons are organized in a volumetric manner including height, width and depth.

A fig. 2 displays CNN architecture, it consists of a convolutionary, pooling and fully connected layer. Convolutionary layer and pooling layer are usually

altered, and from left to right, the depth of each filter is increased while output size (height and width) is reduced. The fully linked layer is the last step close to traditional neural networks.

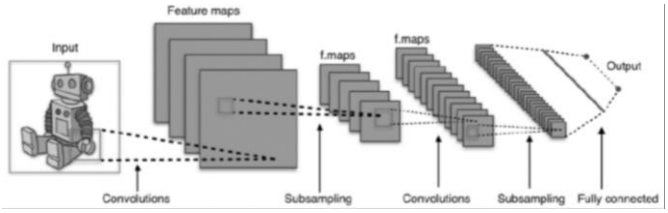


Figure 2. CNN Architecture

The input is an image containing pixels. The three-dimensional model is [50 x 50 x 3], such as width, height and depth (RGB channels) [13]. The convolutionary layer measures the output of neurons attached to the input local areas. The layer parameters are composed of a series of learning filters (or kernels), which covers the width and height of the input volume that extends across the depth of the layer. This produces a two-dimensional activation map of the filter, so the network learns to activate filters when it detects certain features in a certain space position in the input. The function called Rectified Linear Unit (ReLU) layer will perform element wise activation function. ReLU is defined in (1),

$$f(x)=max(0,x) \quad \text{.....(1)}$$

For negative values, this function is no and grows for positive values on a linear basis. The volume size is not affected. The layer of pooling produces the maximum activation in a region. This shows spatial dimensions like height and width. The output layer is a fully attached layer close to the neural network final layer. The softmax activation is used for the distribution of probability over the number of output classes in this layer.

Mathematical Formulation

System S is represented as

S = {ID, P, F, T, CNN, M}

1. Input Dataset

ID = {i1, i2, i3…in}

Where ID is the input image dataset and i1, i2…in are the number of images.

2. Preprocessing

PR = {pr1, pr2, pr3}

PR is preprocessing and pr1, pr2 and pr3 are the steps to be carried out during preprocessing.

pr1 be the reading of input dataset

pr2 be the enhancement of image input and

pr3 be the removal of hair from image.

3. Feature Extraction

F= {f1, f2, f3…fn}

Where F is the set of features extracted from the image and f1, f2, f3… fn are the extracted features such as border, thickness, color, etc.

4. Training and Testing file generation

T = {T1, T2}

Where T is the set of Training and Testing file and T1 is Training file and T2 is Testing file both the files contains various extracted features values while training file contains class of each image as 0 or 1.

5. Convolutional Neural Network (CNN).

CNN = {C, RL, PO, FC, LS}

Where CNN is algorithm consisting of various stages as

C is convolutional operation

RL be the ReLU activation layer

PO be the Pooling layer

FC be the Full Connection layer and

LS be the Loss function.

6. Object Detection

O= {0,1}

O is the set of Class having value 0 or 1

0 be the absent of object and

1 be the present of object

IV. Result Analysis

The picture. The performance analysis graph is shown in 3 and 4. Figure 3 shows the accurate graph that can be found to be the most accurate, while the current mechanism provides a lower percentage, while the

proposed CNN algorithm is more exact compared to the other algorithms in terms of accuracy. Different classification algorithms appear on the following graphs while the y- axis shows the percentage.

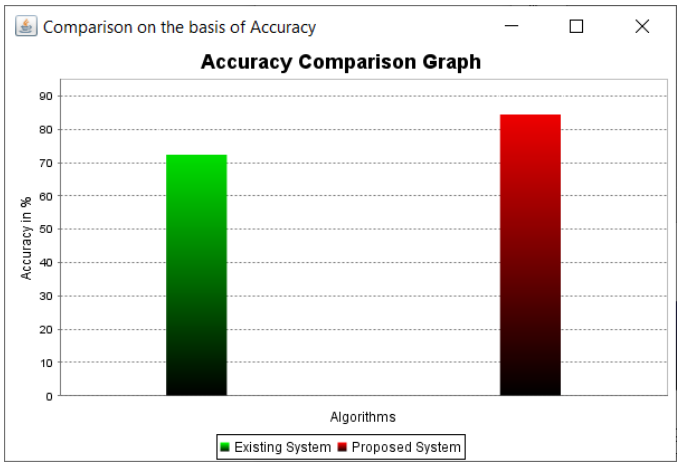


Figure 3. Accuracy Graph

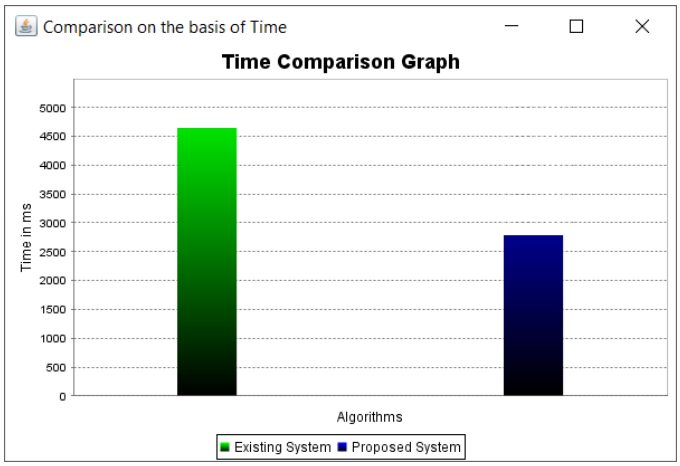


Figure 4. Time Efficiency Graph

V. Conclusion

Enhanced forensic analysis video technology to support the forensic investigation process was discussed here. Low quality CCTV film has an effect on the process of collecting evidence. CCTV film is used to collect criminal records. An adaptive video improvement algorithm is presented here to improve the quality of CCTV footage based on CLAHE. CNN is proposed as an algorithm for promoting forensic video-based investigations that are able to recognize and track offenders, methods used in the perpetration of film crime. CNN used knife, blood and weapon to detect whether or not a crime occurred.

VI. REFERENCES

[1]. M. F. E. M. Senan, S. N. H. S. Abdullah, W. M. Kharudin, and N. A. M. Saupi, "Cctv quality assessment for forensics facial recognition analysis," in 2017 7th International Conference on Cloud Computing, Data Science Engineering - Confluence, Jan 2017, pp. 649–655.

[2]. G. Gilboa, N. Sochen, and Y. Y. Zeevi, "Image enhancement and denoising by complex diffusion processes," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 26, no. 8, pp. 1020–1036, Aug 2004.

[3]. S. Park, S. Yu, M. Kim, K. Park, and J. Paik, "Dual autoencoder network for retinex-based low-light image enhancement," IEEE Access, vol. 6, pp. 22 084–22 093, 2018.

[4]. W. Fan, K. Wang, F. Cayre, and Z. Xiong, "Median filtered image quality enhancement and anti-forensics via variational deconvolution," IEEE Transactions on Information Forensics and Security, vol. 10, no. 5, pp. 1076–1091, May 2015.

[5]. C. Li, J. Guo, R. Cong, Y. Pang, and B. Wang, "Underwater image enhancement by dehazing with minimum information loss and histogram distribution prior," IEEE Transactions on Image Processing, vol. 25, no. 12, pp. 5664–5677, Dec 2016.

[6]. S. Mandal, X. L. Deán-Ben, and D. Razansky, "Visual quality enhancement in optoacoustic tomography using active contour segmentation priors," IEEE Transactions on Medical Imaging, vol. 35, no. 10, pp. 2209– 2217, Oct 2016.

[7]. H. Walker and A. Tough, "Facial comparison from cctv footage: The competence and confidence of the jury," Science & Justice, vol.

55, no. 6, pp. 487 – 498, 2015. Online]. Available:http://www.sciencedirect.com/science/article/pii/S1355030615000635

[8]. E. Verolme and A. Mieremet, "Application of forensic image analysis in accident investigations," Forensic Science International, vol. 278, pp. 137 – 147, 2017. Online]. Available: http://www.sciencedirect.com/science/article/pii/S0379073817302463

[9]. S. Kim, W. Kang, E. Lee, and J. Paik, "Wavelet-domain color image enhancement using filtered directional bases and frequency-adaptive shrinkage," IEEE Transactions on Consumer Electronics, vol. 56, no. 2, pp. 1063–1070, May 2010.

[10]. G. Tzanidou, I. Zafar, and E. A. Edirisinghe, "Carried object detection in videos using color information," IEEE Transactions on Information Forensics and Security, vol. 8, no. 10, pp. 1620–1631, Oct 2013.

[11]. D. Seckiner, X. Mallett, C. Roux, D. Meuwly, and P. Maynard, "Forensic image analysis – cctv distortion and artefacts," Forensic Science International, vol. 285, pp. 77 – 85, 2018. Online]. Available: http://www.sciencedirect.com/science/article/pii/S0379073818300380

[12]. J. Jasmine and S. Annadurai, "Real time video image enhancement approach using particle swarm optimisation technique with adaptive cumulative distribution function based histogram equalization," Measurement, 2019. Online]. Available:http://www.sciencedirect.com/science/article/pii/S0263224118312508

[13]. T. Ayyavoo and J. John Suseela, "Illumination pre-processing method for face recognition using 2d dwt and clahe," IET Biometrics, vol. 7, no. 4, pp. 380–390, 2018.

[14]. A. Hendrawan and S. Asmiatun, "Identification of picnosis cells using contrast-limited adaptive histogram equalization (clahe) and k-means algorithm," in 2018 1st International Conference on Computer Applications Information Security (ICCAIS), April 2018, pp. 1–3.

[15]. R. C. Pandey, S. K. Singh, and K. K. Shukla, "Passive forensics in image and video using noise features: A review," Digital Investigation, vol. 19, pp. 1 – 28, 2016. Online]. Available:http://www.sciencedirect.com/science/article/pii/S1742287616300809

[16]. L. J. G. Villalba, A. L. S. Orozco, R. R. López, and J. H. Castro, "Identification of smartphone brand and model via forensic video analysis," Expert Systems with Applications, vol. 55, pp. 59 – 69, 2016. Online]. Available:http://www.sciencedirect.com/science/article/pii/S095741741600035X

[17]. J. Kamenicky, M. Bartos, J. Flusser, B. Mahdian, J. Kotera, A. Novozamsky, S. Saic, F. Sroubek, M. Sorel, A. Zita, B. Zitova, Z. Sima, P. Svarc, and J. Horinek, "Pizzaro: Forensic analysis and restoration of image and video data," Forensic Science International, vol. 264, pp. 153 – 166, 2016, special Issue on the 7th European Academy of Forensic Science Conference. Online]. Available: http://www.sciencedirect.com/science/article/pii/S0379073816301827

[18]. S. Li, Q. Sun, and X. Xu, "Forensic analysis of digital images over smart devices and online social networks," in 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), June 2018, pp. 1015–1021.

[19]. S. Saikia, E. Fidalgo, E. Alegre, and L. Fernández-Robles, "Object detection for crime scene evidence analysis using deep learning," in Image Analysis and Processing - ICIAP 2017, S. Battiato, G. Gallo, R. Schettini, and F. Stanco, Eds. Cham: Springer International Publishing, 2017, pp. 14–24.

[20]. X. Liu, W. Lu, Q. Zhang, J. Huang, and Y. Shi, "Downscaling factor estimation on pre-jpeg compressed images," IEEE Transactions on Circuits and Systems for Video Technology, pp. 1–1, 2019

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

To Develop Robust Algorithm for Security in Black box Using Explainable Artificial Intelligence (XAI)

Shruti Ajaykumar Yelne[1], Dr. A. N. Thakare[2]

[1]P. G. Student, Department of Computer Engineering, Bapurao Deshmukh College of Engineering, Sevagram Wardha, Maharashtra, India

[2]Professor, Department of Computer Engineering, Bapurao Deshmukh College of Engineering, Sevagram, Wardha, Maharashtra, India

ABSTRACT

Artificial Intelligence based systems is that they often lack transparency. Indeed, the black-box nature of these systems allows powerful predictions, but it cannot be directly explained. This issue has triggered a new debate on explainable AI (XAI). AI to continue making steady progress without disruption.

Explainable Artificial Intelligence (XAI) is a branch of AI that advocates a set of tools, strategies, and algorithms for generating high-quality interpretable, intuitive, and human-understandable explanations of AI judgments. This paper gives mathematical summaries of seminal work in addition to offering a holistic assessment of the present XAI landscape in deep learning. We begin by establishing a taxonomy and categorising XAI strategies based on the scope of explanations, algorithmic methodology, and level of explanation or application, all of which aid in the development of reliable, interpretable, and self-explanatory deep learning models. The key ideas employed in XAI research are then described, and a timeline of significant XAI studies from 2007 to 2020 is shown. We evaluate the explanation maps created by XAI algorithms using image data, highlight the limitations of this methodology, and suggest potential future routes to improve XAI assessment after thoroughly discussing each category of methods and methodologies.

Keywords : Explainable XAI, Interpretable Deep Learning, Machine Learning, Computer Vision, Neural Network, Black-box Model

I. INTRODUCTION

For many years, artificial intelligence (AI) was mostly a theoretical field with few applications with real-world significance. This has fundamentally altered during the last decade, as breakthroughs in Machine Learning (ML) have been enabled by a combination of more powerful machines, improved learning algorithms, and better access to enormous amounts of data, resulting in widespread industrial adoption [1]. Deep Learning approaches [2] began to dominate accuracy benchmarks around 2012, hitting superhuman performances and continuing to improve over time. As a result, machine learning models are now being used

to solve a wide range of real-world problems in a variety of areas, ranging from retail and finance [3, 4] to medicine and healthcare.

Increased model complexity, on the other hand, is frequently used to obtain higher predicted accuracy. The deep learning paradigm, which is at the heart of most cutting-edge machine learning systems, is an excellent example. It enables machines to explore, learn, and extract the hierarchical data representations required for detection and classification tasks automatically. This hierarchy of increasing complexity, combined with the fact that large volumes of data are utilised to train and construct such sophisticated systems, although boosting the systems' predictive power in most circumstances, reduces their ability to explain their inner workings and methods naturally. As a result, the reasoning behind their actions becomes more difficult to comprehend, making their projections more difficult to interpret.

There is a clear trade-off between a machine learning model's ability to deliver explainable and interpretable predictions and its performance. On the one hand, there are "black-box" models such as deep learning [2] and ensembles. The so-called white-box or glass-box models, on the other hand, yield simply explainable results— common examples are linear [11] and decision tree- based [12] models. The later models, while more explainable and interpretable, are not as powerful as the former and fail to achieve state-of-theart performance when compared to the former. Their poor performance, as well as their capacity to be simply comprehended and explained, stem from the same source: their cost-cutting design.

It is difficult to trust systems whose conclusions are difficult to explain, especially in fields like healthcare or self-driving cars, where moral and justice questions have inevitably arisen. The need for trustworthy, fair, robust, high-performing models for real-world applications prompted the resurgence of the field of explainable Artificial Intelligence (XAI) [13]—a field devoted to the understanding and interpretation of AI system

behaviour that had languished in the scientific community in the years prior to its resurgence, with most research focusing on the predictive p Figure 1 shows the evolution of the popularity of the search phrase "Explainable AI" over time, as measured by Google Trends. The substantial growth in recent years, reflecting the field's regeneration, is mirrored in the increasing research output during the same time period.

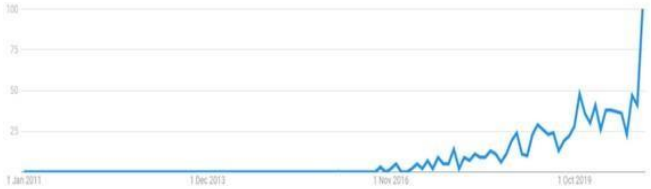


Figure 1. Google Trends Popularity Index (Max value is 100) of the term “Explainable AI” over the last ten years (2011–2020).

Attacks on XAI Methods

Recently, some research [14] has begun to investigate adversarial robustness by examining the range of classification accuracy and network interpretability. Zhang et al. describe a family of white-box attacks that generate adversarial inputs that deceive target deep learning classifiers as well as their associated interpretation models [15]. They put the proposed strategy to the test using four distinct types of explainers. An unnoticeable adversarial perturbation to fool classifiers can result in a large change in a classspecific network interpretability map, as demonstrated in [14]. The sensitivity of explanation maps to tiny disturbances in the picture domain has been illustrated in [16]. In the area of picture categorization, there has been some recent study on modifying explanations. In [17], the authors demonstrate how to change inputs in a way that is

unnoticeable to humans demonstrated that post-hoc explanations are unreliable, presenting merely correlations between the underlying computations. LIME and SHAP explanations are not intuitive in the

case of structured data, as demonstrated by [13]. Dylan et al. [14] developed a unique approach for efficiently hiding discriminating biases in any black-box classifier and fooling post-hoc explanation approaches such as LIME and SHAP in a recent paper. Our research focuses on two types of adversaries and black box focused attacks against them. The first tries to threaten the integrity of the underlying classifier and explainer, whereas the second tries to attack only the explainer without affecting the classifier's prediction, i.e. modify the explanation map given a natural sample.

Adadi and Berrada [18] did an exhaustive literature analysis, collecting and assessing 381 distinct scientific papers between 2004 and 2018. They arranged all of the scientific work in the field of explainable AI along four primary axes and underlined the need for more formalism to be introduced in the field of XAI and for more interaction between people and machines. After underlining the trend of the community to study explainability exclusively in terms of models, they advocated embracing explainability in other elements of machine learning. Finally, they identified a prospective research route that would go towards the composition of existing explainability methodologies.
Another survey that sought to categorise the available explain ability methodologies is this of Guidotti et al. [19]. Firstly, the authors established four categories for each approach depending on the sort of problem that they were created to answer. One category for discussing black-box models, one for inspecting them, one for explaining their results, and, ultimately, one for developing transparent black box models. Subsequently, they provided a taxonomy that takes into account the sort of underlying explanation model (explanator), the type of data utilised as input, the difficulty the technique confronts, as well as the black box model that was “opened”. As with works previously discussed, the lack of formality and need for a definition of metrics for

evaluating the performance of interpretability methods was highlighted once again, while the incapacity of most black-box explain ability methods to interpret models that make decisions based on unknown or latent features was also raised. Lastly, the lack of interpretability techniques in the field of recommender systems is noted and a strategy according to which models might be trained directly from explanations is presented.

Upon noting the lack of formality and means to test the success of interpretability approaches, Murdoch et al.
[20] published a study in 2019, in which they built an interpretability framework in the expectation that it would help to overcome the aforementioned gap in the area. The Prediction, Descriptive, Relevant (PDR) framework presented three types of metrics for grading the interpretability approaches, predictive accuracy, descriptive accuracy, and relevancy. To conclude, they dealt with transparent models and post-hoc interpretation, as they believed that post-hoc interpretability could be used to elevate the predictive accuracy of a model and that transparent models could increase their use cases by increasing predictive accuracy—making clear, that, in some cases, the combination of the two methods is ideal.

A more recent study carried out by Arrieta et al. [21] offered a different style of organisation that initially distinguished transparent and post-hoc approaches and subsequently formed sub-categories. An alternate taxonomy exclusively for the deep learning interpretability approaches, due to their huge volume, was devised. Four categories were proposed under this taxonomy: one for explaining deep network

processing, one for explaining deep network representation, one for explaining producing systems, and one for explaining hybrids of deep network processing, representation, and production systems.

Procedures that are transparent and methods that are black-box finally, the authors discussed the concept of Responsible Artificial Intelligence, which is a technique that introduces a set of criteria for integrating AI in businesses.

II. PROPOSED METHODOLOGY

The main focus of the proposed system is on three key areas:

- The defense mechanisms against the attack proposed;
- Extend the proposed method to compromise the privacy and confidentiality properties of explainable methods, and
- Examine the security robustness of other XAI with different neural network architectures.

In the context of the security domain, we divide the ex- plainability space into - (a) explanations of predictions/data itself X-PLAIN ; (b) explanations covering security and privacy properties of predictions/data XSP PLAIN ; (c) explanations covering threat model of predictions/data under consideration XT PLAIN .

1) X-PLAIN: This space covers the following type of explanations:

- Static vs. interactive changes in explanations seen by user in response to feedback. • Local vs. global explanations.
- In-model vs. post-hoc model explanations that cover models, which are transparent by their nature vs. use of an auxiliary method to explain a model after it has been trained.

- Surrogate model is a second, usually directly interpretable model that approximates a more complex model, while a visualization of a model may focus on parts of it and is not itself a fullfledged model.

2) XSP-PLAIN: The XSP-PLAIN explanations include: Confidentiality properties of data and model e.g. which features of the data are protected by system owner. Integrity properties of data and model e.g. when and how the data was collected and model was trained to accommodate domain shifts etc. Fairness property can be part of model integrity in which explanations can help expose fairness violations by providing insights into possible biases in a model.
Privacy properties of data and model in the explanations
e.g. which part of the data/predictions is exposed to whom. For the publicly released training data and models, have noise added to them so that data rights or model privacy are not compromised? Global explainability methods need to investigate ways to provide explanations about the model without providing details on model weights (directly or via feature importance scores).
3) XT-PLAIN: This space captures the properties of threat models considered at the time of training and deployment. e. g. data poisoning protection, thresholds used, etc. Below we list some of the properties of XAI methods that are relevant to threat modelling in the security domain.

- Correctness: Correctness evaluates the ability of an ex- plainer to correctly identify components of the input that contribute most to the prediction of the classifier.
- Consistency: It is the measure of the explainer's ability to capture the relevant components under

various transformation to the input. More specifically, if the classifier predicts the same class for both the original and transformed inputs, consistency attempts to measure whether the generated explanation for the transformed input is similar to the one generated for the original input modulo the transformation.

- Transferability: Explainability is an advocate for transferability, since it may ease the task of elucidating the boundaries that might affect a model, allowing for a bet- ter understanding and implementation. Similarly, the mere understanding of the inner relations taking place within a model facilitates the ability of a user/attacker to reuse this knowledge craft an attack.
- Confidence: as a generalization of robustness and stability, confidence should always be assessed on a model in which reliability is expected. As stated in [23]–[25], stability is a must-have when drawing interpretations from a certain model. Trustworthy interpretations should not be produced by models that are not stable. Hence, an explainable model should contain information about the confidence of its working regime.
- Fairness: From a social standpoint, explainability can be considered as the capacity to reach and guarantee fairness in ML models. One of the objectives of XAI is highlighting bias in the data a model was exposed to [5], [22]. The support of algorithms and models is growing fast in fields that involve human lives, hence explainability should be considered as a bridge to avoid the unfair or unethical use of the algorithm's outputs.
- Privacy: One of the by-products enabled by explainability in ML models is its ability to assess privacy. ML models may have complex representations of their learned patterns. Not being able to understand what has been captured by the model [6] and stored in its internal representation may entail a privacy breach. Contrarily, the ability to explain the inner relations of a trained model by non-authorized third parties may also compromise the differential privacy of the data origin.

Ideally, XAI should be able to explain the knowledge within a model and it should be able to reason about what the model acts upon. However, the information revealed by XAI techniques can be used both to generate more effective attacks in adversarial contexts aimed at confusing the model, at the same time as to develop techniques to better protect against private content exposure by using such information.

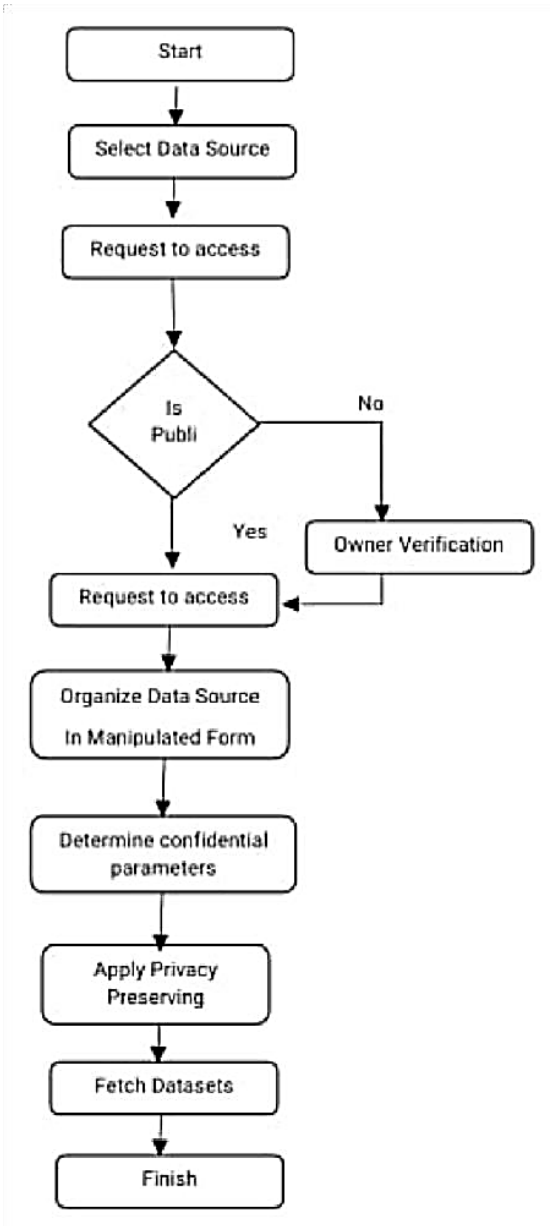


Figure 1. Flowchart for proposed system.

III. SYSTEM REQUIREMENT

- Software Requirement Eclipse IDE , JDK 7.0 , MYSQL
- Hardware Requirement RAM:4 GB , Processor:i3(6th Gen)

IV. CONCLUSION

Findings showed that XAI is not just a research field, its impact is spanning in a large range of application domains. However, we have seen evidence throughout this work for the lack of formalism in terms of problem formulation and clear unambiguous definitions. Further more, it has been noted that the human's role is not sufficiently studied in existing explainability approaches. In essence, attention is devoted to interpreting ML models letting other promising AI system explainability under-explored. It has then been concluded that considerable effort will be required in the future to tackle the challenges and open issues with XAI.

XAI is indeed a key area of multidisciplinary AI research. This document offers a full background on this subject in the spirit of holism. Inspired by our way of understanding new issues, we concentrated on the five components of wisdom and how to cover all the factors associated to XAI. What, Who, Who, Why, Where and How. This poll also examined a portfolio of explanations from a variety of angles for the aim of mapping the wide terrain around XAI research.

Findings have shown that XAI is not only a laboratory field but has an impact on a wide variety of application fields. In the course of this effort, however, we have found evidence that problem formulation and clear, precise definitions have not been formalised. In addition, it was found that the function of the human person in present methods to explainability is not thoroughly studied. Basically, the focus is on the interpretation of the ML models which under-explore the explainability of another promising AI system. In the future, great effort has been concluded in order to confront XAI problems and open problems.

V. REFERENCES

[1]. International Data Corporation IDC. (2018). Worldwide Semiannual Cognitive Artificial Intelligence Systems Spending Guide. Accessed: Jun. 6, 2018. OnlineAvailable: https://www.idc.com/getdoc.jsp?containerId=prUS4 3662418

[2]. Statista. (2018). Revenues From the Artificial Intelligence (AI) Market Worldwide From 2016 to 2025. Accessed: Jun. 6, 2018. OnlineAvailable: https://www.statista.com/statistics/607716/worldwide-artificialintelligence-market-revenues/

[3]. Gartner. (2017). Top 10 Strategic Technology Trends for 2018. Accessed: Jun. 6, 2018. OnlineAvailable: https://www.gartner.com/doc/3811368?srcId=1-6595640781

[4]. S. Barocas, S. Friedler, M. Hardt, J. Kroll, S. VenkaTasubramanian, and H. Wallach. The FAT-ML Workshop Series on Fairness, Accountability, and Transparency in Machine Learning. Accessed: Jun. 6, 2018. OnlineAvailable: http://www.fatml.org/

[5]. B. Kim, K. R. Varshney, and A. Weller. 2018 Workshop on Human Interpretability in Machine Learning (WHI). OnlineAvailable: https://sites.google.com/view/whi2018/

[6]. A. G. Wilson, B. Kim, and W. Herlands. (2016). Proceedings of NIPS 2016 Workshop on Interpretable Machine Learning for Complex Systems. OnlineAvailable: https://arxiv.org/abs/1611.09139

[7]. D. W. Aha, T. Darrell, M. Pazzani, D. Reid, C. Sammut, and P. Stone, in Proc. Workshop Explainable AI (XAI) IJCAI, 2017.

[8]. M. P. Farina and C. Reed, in Proc. XCI, Explainable Comput. Intell. Workshop, 2017.

[9]. I. Guyon et al., in Proc. IJCNN Explainability Learn. Mach., 2017.

[10]. A. Chander et al., in Proc. MAKE-Explainable AI, 2018.

[11]. S. Biundo, P. Langley, D. Magazzeni, and D. Smith, in Proc. ICAPS Workshop, EXplainable AI Planning, 2018.

[12]. M. Graaf, B. Malle, A. Dragan, and T. Ziemke, in Proc. HRI Workshop, Explainable Robot. Syst., 2018.

[13]. T. Komatsu and A. Said, in Proc. ACM Intell. Interfaces (IUI) Workshop, Explainable Smart Syst. (EXSS), 2018.

[14]. Xu K. et al. (2018), Structured adversarial attack: Towards general implementation and better interpretability, arXiv preprint arXiv:1808.01664

[15]. Zhang X. et al. (2018), Interpretable Deep Learning under Fire, arXiv preprint arXiv:1812.00891,2018

[16]. Ghorbani A.,Abubakar A., Zou J. (2019), Interpretation of neural networks is fragile, Proceedings of the AAAI Conference on Artificial Intelligence, 2019

[17]. Dombrowski A.-K. et al. (2019), Explanations can be manipulated and geometry is to blame, arXiv preprint arXiv:1906.07983 2019

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

An Improved Mechanism for Privacy Preservation and Multi-Keyword Search in Cloud Environment

Minakshi Nirmal, Suhani Bansod, Sneha Barsagade, Shradha Adikane, Moiz Mirza Baig
Department of Computer Science & Engineering, J. D. College of Engineering and Management, Nagpur, Maharashtra, India

ABSTRACT

In Information Networks, proprietors can store their documents over passed on different servers. It urging customers to store and get to their information in and from various servers by settling down wherever and on any device. It is an amazingly troublesome task to give beneficial look for on dispersed records also give the privacy on proprietor's documents. The present system gives one possible game plan that is privacy safeguarding indexing (PPI). In this system, records are dispersed over different private servers which are all things considered controlled by cloud/open server. Exactly when customer require a couple of reports, they request to open cloud, which at that point restores the confident summary that is private server once-over to customers. In the wake of getting summary, customer can look for the records on specific private server however in this structure; reports are secured fit as a fiddle on private server that is privacy is bartered. Regardless, proposed structure enhances this present system to influence it more too secure and capable. To begin with records are secured in encoded outline on the private servers and after that use Key Distribution Center (KDC) for allowing deciphering of information got from private server, at client side. The proposed structure moreover executes TF-IDF, which gives the situating of results to customers.

Keywords : Information Network, Private Server, Public Cloud, Distributed Databases, Ranking Results

I. INTRODUCTION

In Information Networks, proprietors can store their chronicles over passed on different servers. It urging customers to store and get to their information in and from various servers by settling down wherever and on any device. It is an amazingly troublesome task to give gainful look for on dispersed records moreover give the privacy on proprietors chronicles. The present system gives one possible course of action that is privacy saving indexing (PPI). In this structure, records are dispersed over different private servers which are all things considered controlled by cloud/open server. Right when customer require a couple of reports, they request to open cloud, which at that point restores the cheerful once-over that is private server rundowaIn the season of distributed figuring, information customers, while valuing countless from the public server (e.g. incurred significant damage reasonability and information openness), are at the same time reluctant or even adaptable to use the fogs, as they lose information control. The ebb and flow research and mechanical undertakings towards returning information control back to public server customers have delivered a combination of multi-space public server stages, most extraordinarily creating information frameworks. In an information framework, an information proprietor

can hold the full control of her information by having the ability to investigate an assortment of authority associations one that she can evidently trust or even have the ability to dispatch an individual server administrated clearly without any other individual. The information sort out does not require shared trusts between servers, that is, a proprietor simply needs to believe her own particular server and nothing more.

Information frameworks create in a collection of use areas. For a case, in the endeavor intranet (e.g. IBM YouServ structure [1], [2]), delegates can store and manage their own specific records on eventually administrated machines. While the agents have their own privacy concerns and could set up get the opportunity to control courses of action on the close-by records, they may be required by the corporate level organization gathering to share certain information for propelling potential joint endeavors [2]. For another representation, a couple of flowed casual groups e.g. Diaspora [3], Status [4] and Persona [5]) starting late ascent and end up being dynamically outstanding, which rely upon the arrangement of decoupling the limit of social information and long range casual correspondence helpfulness. Not in the least like the united strong long range casual correspondence (e.g. Facebook and LinkedIn), the appropriated relational associations allow an ordinary social customer to dispatch an individual server for securing her own specific social information and executing self-portrayed get the chance to control rules for privacy-careful information sharing [6]. Diverse instances of information frameworks fuse electronic Healthcare over the overall public Internet (e.g. the open-source NHIN Direct wander [7]), distributed record giving to get to controls [8] and others. In each one of these frameworks, an information proprietor can have a select zone for association of physical resources (e.g., a virtual machine) and information organization of individual information under the full customer control. Spaces arranged inside various servers are withdrawn and addressed between each other.1 Information sharing and exchanges over a zone constrain are appealing for various application needs.

For privacy-careful request and information sharing in the information sorts out, a candidate course of action is a privacy protecting document on get to controlled circled records [9], [10], [11], or PPI for short. In Fig. 1, a PPI is an index advantage encouraged in a third-social occasion substance (e.g. an open cloud) that serves the overall information to different information clients or searchers. To find reports of interest, a searcher would partake in a two-mastermind look system: First she speaks to a request of noteworthy catchphrases against the PPI server, which gives back an once-over of candidate proprietors (e.g. p0 and p1) in the framework.

n to customers. In the wake of getting summary, customer can look for the records on specific private server however in this system; reports are secured fit as a fiddle on private server that is privacy is haggled. Regardless, proposed system enhances this present structure to influence it more to secure and capable. To begin with records are secured in encoded outline on the private servers and after that use Key Distribution Center (KDC) for allowing interpreting of information got from private server, at client side. The proposed system furthermore executes TF-IDF, which gives the situating of results to customers.

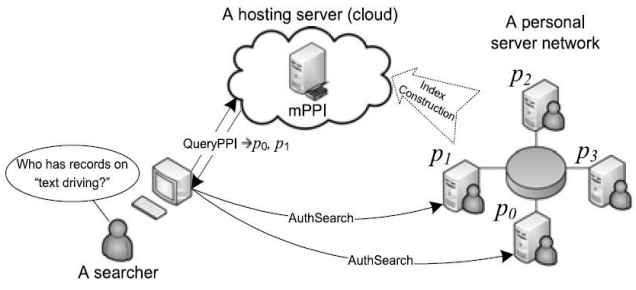


Fig. 1 PPI system

By then for each cheerful proprietor in the once-over, the searcher contacts its server and requesting for customer affirmation and endorsement before looking for locally there. Observe that the affirmation and endorsement simply occur inside the information orchestrate, yet not on the PPI server.

Appearing differently in relation to existing work on secure information serving in the cloud [12], [13], [14], the PPI design is unprecedented as in 1) Data is secured in plain-content (i.e. without encryption) in the PPI server, which makes it achievable for capable and versatile information giving rich handiness. Without use of encryption, PPI stick customer privacy by adding uproars to cloud the delicate ground truth information. 2) Only coarse-grained information (e.g. the responsibility for looked for articulation by a proprietor) is secured in the PPI server, while the principal substance which is private is as yet kept up and guaranteed in the individual servers, under the customer decided get the opportunity to control rules.

In the PPI structure, it is appealing to give isolated privacy assurance as for different search inquiries and proprietors. The information exhibits used as a piece of a PPI structure and an information framework is that each server has diverse records, each containing various terms. What is regarded private and should be secured by a PPI is the possession information as "whether a proprietor has no short of what one record noteworthy to a multi-term express." Under this model, the significance of isolated privacy protection is of two folds: 1) Different (single) terms are not considered ascent to as far as how delicate they seem to be. For example, in an eHealthcare sort out, it is typical for a woman to think about her as helpful record of an "untimely birth" task to be significantly more fragile than that of a "hack" treatment. 2) A multi-term state, as a semantic unit, can be an awesome arrangement progressively (or less) fragile than a single term contained in the articulation. For instance, "substance" and "driving" are two terms that may be respected non-fragile in their solitary appearances; however a record of "content driving" can be seen as more unstable.

The current PPI work [9], [10], [11], while proposed to guarantee privacy, isn't prepared to isolate privacy preservation on different terms. In light of the quality-pragmatist procedures used for building up these PPIs, they can't pass on a quantitative confirmation for privacy protecting for request of a single term, also that of a multi-watchword express.

In this paper, we propose ϵ-MPPI, another PPI pondering which can quantitatively control the privacy spillage for multi-watchword record look. In the ϵ-MPPI structure, unmistakable articulations, be it either a single term or a multi-term articulation, can be outlined with a proposed degree on privacy, implied by ϵ. ϵ can be of any a motivator from 0 to 1; Value 0 addresses negligible stress on privacy preservation, while regard 1 goes for the best privacy protecting (possibly to the disservice of extra request overheads). By this suggests, an attacker, looking for a multi-term state on ϵ-MPPI, can simply have the sureness of mounting viable strikes restricted by what the articulation's privacy degree licenses.

Building a ϵ-MPPI from an information framework is attempting from the purposes of both the estimation and system plots. Computationally, the ϵ-MPPI improvement requires careful arrangement to honestly incorporate false positives (i.e. a proprietor who does not have a term or an articulation wrongly claims to have it) with the goal that a honest to goodness positive proprietor can be concealed among the false positive ones, in this way safeguarding privacy.

As to traces, in a honest to goodness information sort out which needs shared trusts between self-rulingly

worked servers; it is fundamental and alluring to create ϵ-MPPI securely without a place stock in master. The task of scattered secure improvement would be to a great degree testing. On one hand, creating ϵ-MPPI to meet the stringent privacy goals under different multi-term looks while constraining extra chase costs can be essentially shown as an improvement issue, handling which requires complex computations, for instance, a non-straight programming or NLP.

On the other hand, while the fundamental insight for secure estimations (as required by the safe ϵ-MPPI improvement) is to use a multi-party count (MPC) framework or MPC [15], [16], [17], [18] which guarantees input information privacy, the current MPC methodologies can work for all intents and purposes well just with an essential workload in a little framework. For example, FairplayMP [16], an operator valuable MPC organize, "needs around 10 seconds to survey (amazingly direct) limits" [19] which ought to for the most part be conceivable inside milliseconds by the reliable non-secure estimation. Direct applying the MPC methodology to the ϵ-MPPI advancement issue which incorporates a brain boggling estimation and a significant number of individual servers could incite to a cost that is truly breathtaking and in every practical sense unacceptable. To address the troubles of capable secure ϵ-MPPI advancement, our center idea is to draw a line between the protected part and non-secure part in the figuring appear. We confine the protected figuring part however much as could sensibly be normal by researching diverse techniques (e.g. count reordering).

By thusly, we have viably disengaged the baffling NLP count from the MPC part to such a degree, to the point that the expensive MPC in our ϵ-MPPI advancement tradition just applies to a to a great degree clear computational errand, in this manner propelling general structure execution.

The contribution of this paper can be abridged as taking after.

- We proposed ϵ-MPPI to address the necessities of isolated privacy security of multi-term communicates in a PPI structure. To best of our understanding, ϵ-MPPI is the key wear down the issue. ϵ-MPPI guarantees the quantitative privacy protection by means of correctly controlling the false promising focuses in a PPI and in this way effectively compelling an attacker's assurance.
- We proposed a suite of sensible ϵ-MPPI improvement traditions material to the arrangement of normally untrusted singular servers. We especially thought to be both the single-term and multi-term state cases, and enhanced the execution of the safe ϵ-MPPI improvement from the two edges of estimation model and system design by researching the considerations of reworking the ensured figuring endeavors however much as could be normal while without surrendering the idea of privacy protecting.
- We executed a working model for ϵ-MPPI, in light of which a trial consider certifies the execution ideal position of our rundown improvement tradition.

II. MODULES AND METHODOLOGY

Structure includes open cloud server, various private servers and diverse customers. The proprietors files are store on private servers in scatter way. The records are secured in mixed design. AES count is used for information encryption. Each private server influenced its document to record of information. Watching structure accumulates all records and consolidating them. This united record is then put at open cloud. By and by, if client needs some record from server, it speaks to a request to open cloud. In returns, open cloud gives the solidified record got from

watching structure. By and by from this last union rundown, client having the summary of private server at which question related information is secured. By then to get to the information at server, client sends the affirmation requests with customer name and watchword.

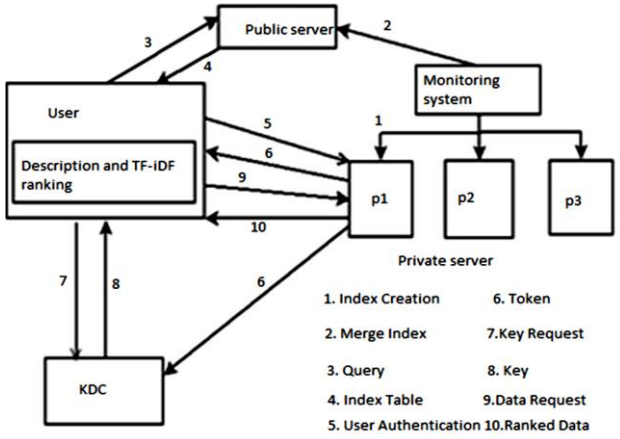


Fig. 2: System Architecture

Private server affirms this unobtrusive components store in its database. After productive check, private server makes the token and sends it to client and Key Distribution Center (KDC). In the wake of getting these token, customers request to KDC for a key. KDC affirm this token with its token which is starting at now getting from private server. After check, KDC gives encryption key to the client. By then client send information request to private server in returns server gives all planning mixed reports. Using key client can unscramble the information. Finally apply the TF-IDF situating estimation, to get all results in situating design.

System consisting of following modules:

- **System Deployment**

Registration And Login with Database, Client and Server with attachment programming and information exchange AES Encryption and Decryption with Client side GUI.

- **MPPI Index creation algorithm**

MPPI calculation is utilized for making list of all private servers. List speaks to the detail portrayal of information store at private server.

- **Index combining and Upload on Public Server**

Checking framework is in charge of joining list of every private server and transfers this last consolidation file record on open cloud.

- **Input Query and Response From Public Server**

Client represents an inquiry to cloud server for receiving specific information from private server consequently open cloud gives consolidate file.

- **Client Authentication and token generation**

Subsequent to getting file, client needs to associate with private server to get the outcomes. Client login to the server and in the wake of finishing effective validation, private server create and disseminate the token to client and KDC.

- **Key Distribution and File Decryption**

After check of tokens, KDC give the way to client to decoding of results got from private server.

- **TF IDF Ranking Results**

After confirmation, client gets the outcomes from private server in scrambled organization. These scrambled outcomes are then unscrambled utilizing key acquired from KDC. At long last create the positioning of comes about by utilizing TF IDF.

I. MATHEMATICAL MODEL FOR PROPOSED WORK

Let S be a System.

S= {I, P, O}

Where,

- Input I: The input for the system is multi word query from the user.
- Output O: Ranking results.
- Process P:

(a) Single-term publication

$$\varepsilon_j = \frac{(1-\sigma_j).\beta_j(t_j)}{(1-\sigma_j).\beta_j+\sigma_j}$$

$$\beta_j = [(\sigma_j^{-1}-1)(\varepsilon_j^{-1}-1)]^{-1}$$

Where, β_j is number of probability values produces by source analytical computation for term.

(b) False Positive Rate:

FP (0; 1) = F (0; 1)

$$FP(0,1) = \frac{F(0,1)}{F(0,1)+\sigma_0\sigma_1}$$

Where, FP (0, 1) is the false positive values, β_0; β_1 are the probability at which a non-positive owner publishes data as a positive owner.

(c) Index Generation

I= {I1, I2... In}

Where I is the set of all index of all private servers

(d) Merge and upload index at private server.

MI= {MI1, MI2... Min}

Where MI is the set of all merge indexes collected from monitoring system.

(e) User Query to public server

Q= {Q1, Q2... Qn}

Where, Q is the set of all queries poses to public cloud.

(f) User Authentication at private server

U= {U1, U2... Un}

Where U is the set of all authenticated users of private server.

(g) Token Generation and distribution

T= {T1, T2... Tn}

Where T is the set of all tokens generated by private server for its authenticated users.

(h) Key Generation at KDC

G= {G1, G2... Gn}

Where G is the set of all keys stored at KDC, used for decryption of data at user side.

(i) Data decryption and TF IDF ranking

D= {D1, D2... Dn}

Where D is the set of all ranked results for particular input query.

III. Algorithms

A) Advanced Encryption Standard (AES) Algorithm:

AES is a block cipher with a square length of 128 bits. AES licenses for three differing key lengths: 128, 192, or 256 bits. The encryption procedure utilizes an arrangement of especially inferred keys called round keys. AES is an iterative as opposed to Feistel figure. AES utilizes 10 rounds for 128-piece keys, 12 rounds for 192-piece keys and 14 rounds for 256-piece keys. The piece to be encoded is only an arrangement of 128 bits. Each round of handling contains one single-byte based substitution step, a line savvy stage step, a segment insightful blending step, and the expansion of the round key. The request in which these four stages are executed is diverse for encryption and decryption.

Encryption Steps:-

(a) Byte Substitution (SubBytes)

(b) Shift rows

(c) Mix Columns

(d) Add round key

Decryption Steps:-

(a) Add round key

(b) Mix columns

(c) Shift rows

(d) Byte substitution

B) TF-IDF:

The term frequency inverse document frequency (TF IDF), is a numerical statistic that is proposed to reflect how significant a word is to a document in a corpus or collection. The TF-IDF value increases proportionally to the number of times a word appears in the document, but is equalizing by the frequency of the word in the corpus, which assist to regulate for the information that some words appear more frequently in general.

TF: Term Frequency, which measures how frequently a term occurs in a document. Since every document is different in length, it is possible that a term would appear much more times in long documents than shorter ones.

TF (t) = (Number of times term t appears in a document) / (Total number of terms in the document).

After calculating the TF values for the entire terms top 5 terms will be selected for generating the index. A table will be creating a table and the keyword obtained for index generation will be inserted. The generated table will contain the filename, keywords i.e., the

word which will be used for index generation server Id and the size of the file. In further processing this table will be uploaded and sent to monitoring server for further processing.

IDF: Inverse Document Frequency, which measures how important a term is. While computing TF, all terms are considered equally important. However it is known that certain terms, such as "is", "of", and "that", may appear a lot of times but have little importance. Thus we need to weigh down the frequent terms while scale up the rare ones, by computing the following:

IDF (t) = log_e (Total number of documents) / (Number of documents with term t in it).

C) Iterative-Publish (Owner Pi, set β_0 (r_k))

a) for all k ϵ [0; l -1] do β'(rk) is topologically sorted
b) if match(cur-memvec, getStartingState(rk)) then Bcur memvec is the current membership vector
c) cur-memvec publish (cur-memvec, β'(rk))
d) end if
e) end for

To publish data with multiple probabilities for overlapping phrases, we propose to use the IBeta approach. Algorithm illustrates how the index publication approach iteratively runs, phrase by phrase.

IV. CONCLUSIONS

The proposed system is tied in with interfacing between neighborhood server and cloud server for information sharing among the customers. Some approval is required to get to specific information or information. This approval is managed through encryption structure. For sensible execution of secure counts, it proposes Associate in Nursing MPC reducing framework supported the traditionalist usage of secret sharing designs. Thusly, through the proposed system customer can get a passageway to required information in situated organize using PPI and encryption strategy.

V. REFERENCES

[1]. Yuzhe Tang and Ling Liu,"Privacy-Preserving Multi-Keyword Searching Information Networks", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 27, NO. 9, SEPTEMBER 2015

[2]. R. J. Bayardo Jr, R. Agrawal, D. Gruhl, and A. Somani, "Youserv: A web-hosting and content sharing tool for the masses," in Proc. 11th Int. Conf. World Wide Web, 2002, pp. 345–354.

[3]. M. Bawa, R. J. Bayardo Jr, S. Rajagopalan, and E. J. Shekita, "Make it fresh, make it quick: Searching a network of personal webservers," in Proc. 12th Int. Conf. World Wide Web, 2003, pp. 577–586.

[4]. [Online]. Available: Diaspora: https://joindiaspora.com/, 2014.

[5]. [Online]. Available: Status, http://status.net, 2014.

[6]. R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: An online social network with user-defined privacy," in SIGCOMM Conf. Data Commun., 2009, pp. 135–146.

[7]. H. L€ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proc. 1st ACM Int. Health Informat. Symp., 2010, pp. 220–229.

[8]. [Online]. Available: Nhin direct, http://directproject.org/, 2014.

[9]. R. Geambasu, M. Balazinska, S. D. Gribble, and H. M. Levy,

[10]. "Homeviews: Peer-to-peer middleware for personal data sharing applications," in Proc. SIGMOD Conf., 2007, pp. 235–246.

[11]. M. Bawa, R. J. Bayardo Jr, and R. Agrawal, "Privacy-preserving

[12]. indexing of documents on the network," in Proc. VLDB Conf.,

[13]. 2003, pp. 922–933.

[14]. Y. Tang, T. Wang, and L. Liu, "Privacy preserving indexing for ehealth information networks," in Proc. 20th ACM Int. Conf. Inf. Knowl. Manage., 2011, pp. 905–914.

[15]. M. Bawa, R. J. Bayardo, Jr, R. Agrawal, and J. Vaidya, "Privacy preserving indexing of documents on the network," VLDB J., vol. 18, no. 4, pp. 837–856, 2009.

[16]. R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting confidentiality with encrypted query processing," in Proc. 23rd ACM Symp. Operating Syst. Principles, 2011, pp. 85–100.

[17]. C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. 41st Annu. ACM Symp. Theory Comput., 2009, pp. 169–178.

[18]. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in Proc. IEEE INFOCOM, 2011, pp. 829–837.

[19]. D. Malkhi, N. Nisan, B. Pinkas, and Y. Sella, "Fairplay—Secure two-party computation system," in Proc. 13th Conf. USENIX Security Symp., 2004, pp. 287–302.

[20]. Ben-David, N. Nisan, and B. Pinkas, "Fairplaymp: A system for secure multi-party computation," in Proc. ACM Conf. Comput. Commun. Security, 2008, pp. 257–266.

[21]. W. Henecka, S. K€ogl, A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, "TASTY: Tool for automating secure two-party computations," in Proc. 17th ACM Conf. Comput. Commun. Security, 2010, pp. 451–462.

[22]. Damga rd, M. Geisler, M. Krøigaard, and J. B. Nielsen, "Asynchronous multiparty computation: Theory and implementation," in Proc. 12th Int. Conf. Practice Theory Public Key Cryptography, 2009, pp. 160–179.

[23]. Narayan and A. Haeberlen, "DJoin: Differentially private join queries over distributed databases," in Proc. 10th USENIX Conf. Operating Syst. Des. Implementation, Oct. 2012, pp. 149–162.

[24]. J. Hsu, M. Gaboardi, A. Haeberlen, S. Khanna, A. Narayan, B. C. Pierce, and A. Roth. (2014). Differential privacy: An economic method for choosing epsilon, CoRR [Online]. abs/1402.3329 Available: http://arxiv.org/abs/1402.3329

[25]. Y. Tang and L. Liu, "Multi-keyword privacy-preserving search in information networks," Tech. Rep. 2014 [Online]. Available: http://tristartom.github.io/docs/tr-mppi.pdf, 2014.

[26]. Y. Tang, L. Liu, A. Iyengar, K. Lee, and Q. Zhang, "e-PPI: Locator service in information networks with personalized privacy preservation," in Proc. IEEE 34th Int. Conf. Distrib. Comput. Syst., Madrid, Spain, Jun. 30–Jul. 3, 2014, pp. 186–197.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Sentiment Classification of Movie Review using Machine Learning Approach

Ashish Lahase, Sachin N. Deskmukh
Department of Computer Science & IT, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India

ABSTRACT
The quality of a movie might be determined by recent researchers' opinions or reviews. This review classification divides opinions into two categories: positive and negative. It defines the expressing of sentiments, such as negative or good feelings concerning the existence of anything. Data analysis may make use of a variety of sources, including healthcare, media platforms, news, and movie reviews. We employed POS tagging, Stopword removal, and tokenization for preprocessing (NLTK library). For feature selection, principal component analysis was utilized based on the relevance of the work in relation to the overall movie review. Our analysis outlines that Support vector machine achieves better accuracy 81.70% shows higher recall compared to the K Nearest neighborhood 65.15%.

Keywords— Sentiment Analysis; PCA; SVM; KNN; BOW; TF-IDF

I. INTRODUCTION

The internet makes it simpler for individuals to connect. They use the internet to express themselves through social media, blog posts, movie reviews, product review sites, and so on. Every day, users create massive volumes of data. Movies are perhaps the finest form of entertainment for humans, and it is typical for individuals to watch them and then voice their ideas on social networking sites. By examining movie review data, we may learn about a movie's strong and weak points, as well as whether or not the movie matches the user's expectations. When a person decides to see a movie, he first looks at the movie's review and rating. Sentiment analysis (SA) aids in acquiring a movie review [1].

One of the issues with sentiment analysis is that an opinion term that is regarded as favorable in one scenario may be judged bad in another. Second, people's ways of expressing themselves in a given scenario differ. Traditional text processing believes that a little alteration between two bits of text does not affect the meaning. However, in sentiment analysis, "the picture is nice" differs from "the picture is bad." The majority of statements include both positive and negative sentiments. It is processed by the algorithm one sentence at a time. Blogs and Twitter, on the other hand, feature more casual messages that are easily understood by the user rather than the system. "That movie was as good as its last movie," for example, is dependent on another thing

whose description is unavailable [2].

Every day, a massive volume of text data relating to customer views regarding products and services is created throughout the world. However, manually analyzing the sentiment of such a large number of messages is not practicable. As a result, an automated approach must be used to mine this text data and accurately assess the sentiment, as organizations need to use these massive volumes of data to enhance their operations through more effective marketing analysis, product evaluations, public relations, and so on[3]. Sentiment analysis is the technique of computationally recognizing attitudes represented in a text, particularly to assess if the writer's opinion toward a specific topic or product is good, negative, or neutral. For sentiment analysis, many natural language processing or text analysis approaches are used [4].

Researchers use publicly available datasets such as Amazon Reviews, IMDB Movie Reviews, Yelp Reviews, and others to examine sentiment analysis approaches. Previously, numerous feature engineering-based techniques for sentiment analysis were used. However, these techniques need handmade features, which are prone to mistake. With the growth of Machine Learning and Deep Learning, new state-of-the-art outcomes are being produced by a variety of models [5]. Machine Learning and Deep Learning-based sentiment analysis models were tested on the IMDB review dataset. For sentiment analysis, we used four different algorithms. Long Short-Term Memory Model (LSTM) and Gated Recurrent Unit (GRU) are neural network-based algorithms, whereas Multinomial Nave Bayes and Support Vector Machine are non-neural network-based techniques. To assess their performance, we used Binary Classification on the IMDB movie review dataset [6].

II. RELATED WORK

In recent years, a substantial number of studies on the subject of sentiment analysis have been done.

Previously, numerous rule-based techniques were utilized for sentiment analysis. Developed a simple rule-based model for generic sentiment analysis and discovered that it outperformed the benchmarks utilized in their study. However, the performance of their suggested model was not compared to alternatives based on neural networks. Twitter, a popular social media website, has also been utilized for sentiment analysis [7]. By incorporating Parts of Speech (POS) characteristics, we investigated sentiment analysis on Twitter data. Studied the efficacy of linguistic characteristics for identifying sentiment in Twitter messages and discovered that part-of-speech features are ineffective for sentiment analysis in the micro blogging arena [8].

Introduced a novel technique to phrase-level sentiment analysis that first evaluated whether an expression was neutral or polar before disambiguating the polarity of the polar expressions[9]. Throughout history, a variety of methodologies have been utilized for opinion mining activities. This method is represented by the works listed below. utilizes review data from vehicles, banks, movies, and tourism places He divided the words into two categories (positive and negative) and calculated an overall positive or negative score for the text. If the document has more positive than negative phrases, it is deemed to be positive; otherwise, it is considered negative. Document and phrase-level categories are used in these classifications. These classifications are beneficial and increase the efficacy of sentiment classification, but they cannot determine what each characteristic was liked and hated by the opinion holder [10]

Many studies employ machine learning and lexical pattern extraction approaches to obtain views. The findings of review categorization were introduced by examining the algebraic sum of the orientation of words about the orientation of the documents. He calculated the similarity of two terms by counting the number of online

search results returned. The association between a polarity unknown word and a collection of manually picked seeds was utilized to categorise the polarity unknown word as positive or negative [11].

Used movie review, customer feedback review, and product review data. They employ a variety of statistical feature selection approaches as well as machine learning techniques. These findings indicate that machine learning algorithms are only marginally effective in sentiment categorization. They demonstrate that the presence or absence of a term appears to be more informative of its substance than its frequency [12]. used the data of customer feedback review and product review. They use the Decision learning method for sentiment classification. Decision tree learning is a method for approximating discrete-valued target functions, in which the learned function is represented by a decision tree. Learned trees can also be re-represented assets of if-then rules to improve human readability. These learning methods are among the most popular inductive inference algorithms and have been successfully applied to a broad range of tasks from learning to diagnose medical cases to learning to assess the credit risk of loan applicants [13].

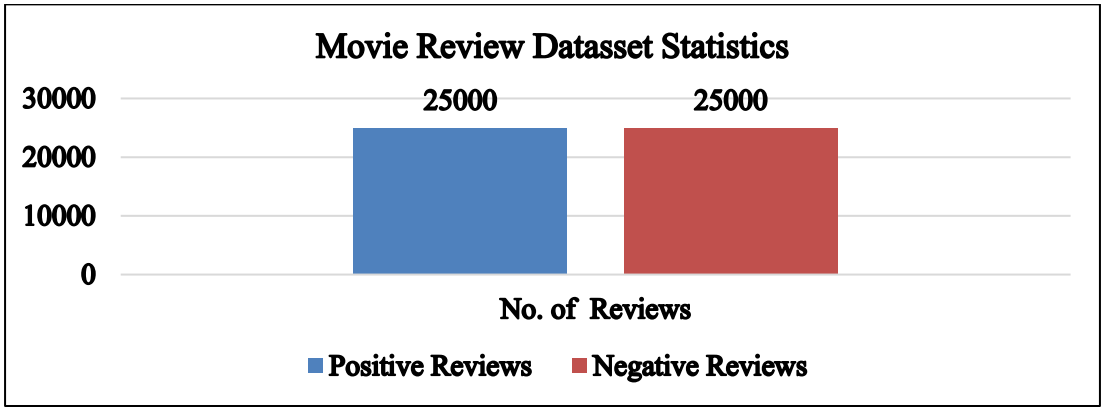
III. DATA & DATA SOURCE

feedback is a useful source of data that can be used to enhance the quality of service provided. Blogs, review sites, and microblogs are examples of venues where users may share their ideas. Movie reviews are taken into account when doing the research. The database may be found at https://ai.stanford.edu/amaas/data/sentiment/. The Large Movie Review Dataset contains far more data than prior datasets for binary sentiment categorization. They supply a set of 25,000 highly polar movie reviews for training and another set of 25,000 for testing. There are also unlabeled data available for usage [14].

TABLE I. STATISTICS OF MOVIE REVIEW DATASET

Sr. No.	Movie Reviews	No. of Reviews
01	Positive Reviews	25000
02	Negative Reviews	25000

MOVIE REVIEW DATASET STATISTICS



IV. METHODOLOGY

Sentiment analysis may be performed at document level. In this work, we used supervised machine learning models to classify the sentiment of movie reviews using Support vector machines and KNearest Neighbor.
We utilised a bag of words to collect all of the words in each movie review, then counted the number of times each word appeared. The phrase refers to the frequency of occurrence of a word w in a document (text) d. It is equal to the number of occurrences of word w in document d divided by the total number of words in document d, and Inverse Document Frequency (IDF) provides a numerical value of a word's relevance.

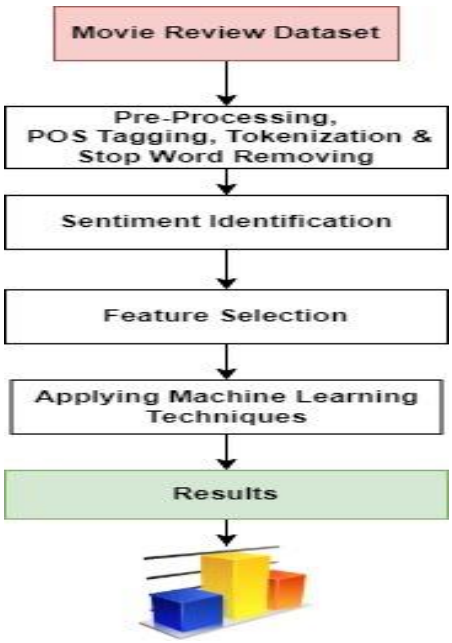


Figure 1. Proposed Method

A. Support Vector Machine

The support vector machine is a non-probabilistic technique that is used to split data into linear and nonlinear segments. Here, dataset D = Xi, yi, where Xi is a set of tuples and yi is a tuple's associated class label. For the no and yes categories, the class labels are -1 and +1, respectively. The purpose of SVM is to identify an n-1 hyperplane to differentiate negative and positive training examples. In linear data, a Quadratic Programming (QP) issue must be addressed [15]. The Lagrange Multipliers theory is used to convert this issue, and optimal Lagrange coefficient sets are found. A separating hyperplane is denoted by:

$W^*X + b = 0$

where W = w1, w2,..., wn, w n is the weight vector of n characteristics and b is the bias The distance between the separating hyperplane and any point on H1 is 1/|W|, and the distance between the separating hyperplane and any point on H2 is 1/|W|, therefore the maximum margin is 2/|W|. Input vectors that just touch the boundary of the margin (street) – circled below, there are 3 of them (or, rather, the 'tips' of the vectors

$w_0{}^T\mathbf{x} + b_0 = 1$

or

$w_0{}^T\mathbf{x} + b_0 = -1$

Where TX is the test tuple, I and b0 are numeric parameters, and y I is the support vector Xi's class label. As a result, if the sign of the MMH equation is positive, TX falls into the positive group. Define the hyperplanes H such that:

w•xi+b ≥ +1 when yi =+1

w•xi+b ≤ -1 when yi = –1

H1 and H2 are the planes:

H1: w•xi+b = +1

H2: w•xi+b = –1

The points on the planes H1 and H2 are the tips of the Support Vectors. The plane H0 is the median in between, where w•xi+b =0.

d+ = the shortest distance to the closest positive point

d- = the shortest distance to the closest negative point

The margin (gutter) of a separating hyperplane is d+ + d–.

B. K Nearest Neighbourhood

KNN may be used to solve classification and regression difficulty. It outperforms the majority of the other classifiers on smaller datasets. KNN implementation entails the following two key steps:

- Identifying a group of k items that are closest to the test object, and
- Assigning a label based on the preponderance of a class in the test object's neighborhood.

The first step is to compute the distance between the test item and each of the training objects. Distance can be defined as Euclidian distance, Cosine similarity, and so forth. The Euclidian distance is determined as follows:

$d = \sqrt{[(x_2 - x_1)^2 + (y_2 - y_1)^2]}$

The second step is to sort the vector after computing the distance between the training items and selecting the first k values. The label assigned to a test item is determined by the dominance of a class. Option for k value: There is no straightforward method for calculating the best value of k. It is entirely dependent on the task at hand and the dataset. One easy method for determining the ideal k value is to experiment with several k values and select the one with the highest accuracy %. Furthermore, the value of k should not be too big, since this may cause the model to overfit.

C. Principal Components Analysis(PCA)

When the dimensions of the inputs are large and the components are highly correlated, PCA is used to reduce the dimensions of the inputs. PCA selects a smaller collection of generated variables to reflect the variance of a set of observed variables. The computed artificial variables are referred to as main components. In other analyses, these major components are employed as predictor or criterion variables. The PCA orthogonalizes the variables, and the principal components with the greatest variation are picked, while the components with the least variance are removed from the dataset [16].

V. EXPREIMENT RESULT

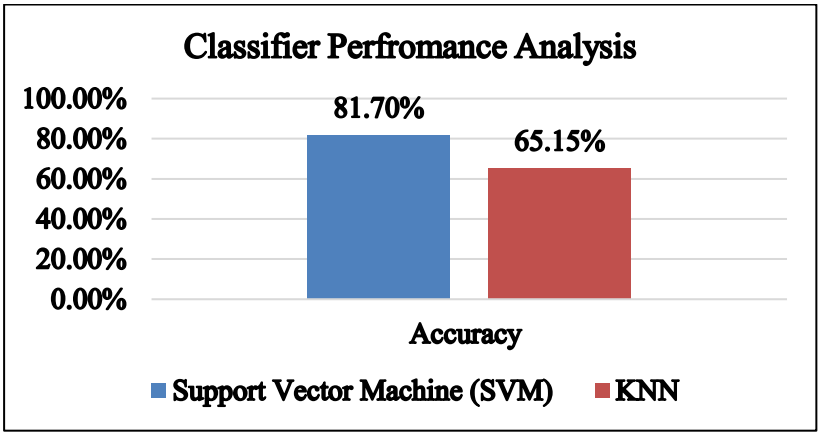
In this study, two types of machine learning classifiers are used: Support Vector Machine and k-Nearest Neighbours, and the analysis is done at the sentence level. For a data set obtained from Unigram and Bigrams,

the processes of separating the data set into two halves were examined. The characteristics were reduced using Principal Component Analysis (PCA). Table 2 displays the Dataset Distribution Statistics for Training/Validation/Testing Machine Learning Models, and the graph below depicts the classifier performance analysis, with Support Vector Machine scoring 81.70 % and k-Nearest Neighbours scoring 65.15 %.

TABLE II. DATASET DISTRIBUTION STATISTICS FOR TRAINING/VALIDATION/TESTING MACHINE LEARNING MODEL

Sr. No.	Movie Reviews	No. of Reviews
01	Training Dataset	30000
02	Validation Dataset	10000
03	Testing Dataset	10000

CLASSIFIER PERFORMANCE ANALYSIS



VI. CONCLUSION

The data set from HTTPS://AI.STANFORD.EDU/amaas/data/senti ment/ is used in this research (Large Movie Review Dataset). Machine Learning methods (Support Vector Machine and K Nearest Neighbours) are used to train the data set, analyse the reviews, and forecast the sentiment of the reviews, which might be positive or negative, with high accuracy. An effective and efficient approach for collecting movie reviews has been automated, allowing the anatomization to be carried out quickly in such a way that the consequence of the evaluation may be employed effectively previously its utility has been superannuated. Support Vector Machine may be utilized very effectively and correctly to execute sentiment analysis on movie reviews in order to understand the consumer's emotions and behavioral preferences in order to give a better customer experience. The next step is to see if a hybrid strategy may be utilized to improve accuracy by combining the permutations and combinations of the above-mentioned classifiers.

VII. REFERENCES

[1]. Appel, G., Grewal, L., Hadi, R., & Stephen, A. T. (2020). The future of social media in marketing. Journal of the Academy of Marketing Science, 48(1), 79-95.
[2]. Medhat, W., Hassan, A., & Korashy, H. (2014). Sentiment analysis algorithms and applications: A survey. Ain Shams engineering journal, 5(4), 1093-1113.
[3]. Liu, B., & Zhang, L. (2012). A survey of opinion mining and sentiment analysis. In Mining text data (pp. 415-463). Springer, Boston, MA.
[4]. Ruiz Martínez, N. (2021). The Use of Linguistic Knowledge in Sentiment Analysis Tools.
[5]. Rajput, Q., Haider, S., & Ghani, S. (2016). Lexicon-based sentiment analysis of teachers' evaluation. Applied computational intelligence and soft computing, 2016.
[6]. Rani, S., & Kumar, P. (2019). Deep learning based sentiment analysis using convolution neural network. Arabian Journal for Science and Engineering, 44(4), 3305-3314.
[7]. Montoyo, A., Martínez-Barco, P., & Balahur, A. (2012). Subjectivity and sentiment analysis: An overview of the current state of the area and envisaged developments. Decision Support Systems, 53(4), 675-679.
[8]. Pak, A., & Paroubek, P. (2010, May). Twitter as a corpus for sentiment analysis and opinion mining. In Proceedings of the Seventh International Conference on Language Resources and Evaluation (LREC'10).
[9]. Wilson, T., Wiebe, J., & Hoffmann, P. (2009). Recognizing contextual polarity: An exploration of features for phrase-level sentiment analysis. Computational linguistics, 35(3), 399-433.
[10]. Las Johansen, B. C. (2018). Deciphering west philippine sea: A plutchik and vader algorithm sentiment analysis. Indian Journal of Science and Technology, 11, 47.
[11]. Pradhan, V. M., Vala, J., & Balani, P. (2016). A survey on sentiment analysis algorithms for opinion mining. International Journal of Computer Applications, 133(9), 7-11.
[12]. Brahimi, B., Touahria, M., & Tari, A. (2021). Improving sentiment analysis in Arabic: A combined approach. Journal of King Saud University-Computer and Information Sciences, 33(10), 1242-1250.
[13]. Du, W., & Zhan, Z. (2002). Building decision tree classifier on private data.
[14]. Andrew L. Maas, Raymond E. Daly, Peter T. Pham, Dan Huang, Andrew Y. Ng, and Christopher Potts. (2011). Learning Word Vectors for Sentiment Analysis. The 49th Annual Meeting of the Association for Computational Linguistics (ACL 2011).
[15]. Berwick, R. (2003). An Idiot's guide to Support vector machines (SVMs). Retrieved on October, 21, 2011.
[16]. Jolliffe, I. T., & Cadima, J. (2016). Principal component analysis: a review and recent developments. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374(2065), 20150202.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

A Comparative Study of Automatic Visual Speech Recognition Techniques

Kiran Suryawanshi[1], Dr. Charansing N. Kayte[2]
[1]Department of Computer Science & IT, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India
[2]Government Institute of Forensic Science, Aurangabad, Maharashtra, India

ABSTRACT
This study argues that speech is the most crucial instrument for human connection. This has prompted academics to conduct more research on Automatic Visual Speech Recognition and to create a computer system capable of integrating and comprehending human speech. Much of this research has only been conducted in their specific platform. Audio-Visual Speech Recognition is advancement in ASR technology that integrates audio and facial expressions to record the voice of a narrator. The purpose of this study is to explain AVSR architecture, including front-end processes, audio-visual data corpus utilized, current developments, and estimating methodologies.

Keywords— AVSR, MFCC, Feature Extraction, DTW, DCT, PCA, BLSTM, CNN

I. INTRODUCTION

Voice is the most suitable, ordinary, and easy to use interface to numerous types of devices, automatic speech recognition (ASR) has sparked a lot of attention. However, speech recognition acquired in actual noisy scenarios often heavily polluted, and ASR systems that use the tainted speech signal perform much worse owing to a misalignment between both the training and test sets conditions [1].

A common audio-visual speech recognition system uses hidden Markov models (HMMs) to represent words, with each state matching to a phoneme. The emission probability of each state is represented by a Gaussian mixture trained using the expectation-maximization technique (EM). However, because the EM technique is designed to simulate the probability distribution rather than providing the best discriminative representation, it cannot guarantee ideal recognition rates. When the Gaussian mixture is replaced with more discriminative classifiers, hybrid systems with higher recognition rates result [2].

Traditional audiovisual fusion systems are divided into two stages: feature extraction from picture and audio data and feature combining for joint categorization. Several deep learning techniques for audiovisual fusion have recently been published, with deep bottleneck topologies aiming to replace the feature extraction stage. Typically, a transform, such as principal component analysis, is performed to the mouth ROI and spectrograms

or concatenated MFCC, and a deep auto encoder is trained to identify bottlenecks features. Lip reading is divided into two stages: feature extraction and identification. A crucial aspect of this work is feature extraction, which entails detecting significant locations on the lip contour. Many work reports on feature extraction have been published in recent years [3].

According to the International Phonetic Alphabet, After Mandarin, Spanish, and English, Hindi is the fourth most commonly spoken language among native speakers. Because the Hindi language has recently grown in popularity throughout the world, most speeches allow technologies are developing a Hindi speech interface system. The number of phone sets in Hindi is more than the number of phone sets in English [4].

Image-based speech recognition VSR's steps for predicting spoken utterance include lip detection, lip feature extraction, and visual speech classification. Appearance-based features and geometric-shape-based features are the two types of features. Pixel intensities or their alteration by recording spatial frequencies are used as feature vectors in appearance-based features. The second type of feature is geometrical, and it refers to the shape of the lips. The most crucial components of lip reading are described by the shape of the speaker's mouth. Before establishing the feature vectors, the fractal patterns feature extraction approach identifies the lip shape and numerous crucial spots on the lips. Model-based features, which include parameters from the lip model, or high-level mouth properties, such as mouth height, width, area, perimeter, and so on, are examples of feature vectors [5].

Visems are used to transcribe visual speech. It represents the lip shape or lip motions associated with a speech in the visual domain. A temporal pattern of lip geometry or fluctuation in lip geometric properties can be used to represent a visem. After the lips have been identified from video frames containing face images, benchmark marks on the lips were defined in order to establish geometric form attributes such as height, width, area, and so on, which describe the lip shape. A typical VSR is seen in Figure 1. (Lip-reading system). Recognize a human face in video frames is the first step. The second phase is lip localization, which is accompanied by visual extracting features and lip-reading, or classification of spoken words. Correct lip identification and also the durability of the obtained features are critical to the accuracy of a VSR system [6].

The approaches for face identification, lip alignment, and extracted features are all thoroughly studied. Among the several options available.

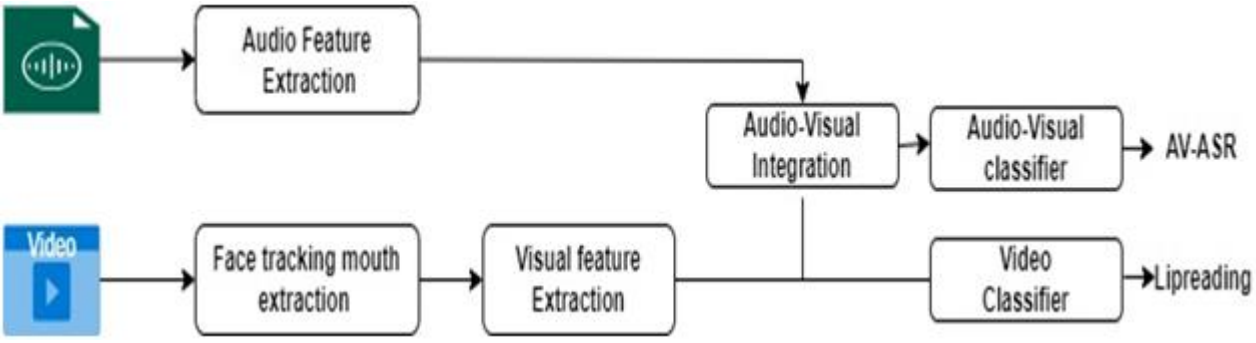


Figure 1. Visual Speech Recognition System [6]

II. RELATED WORK

lip-voice (MFCC acoustic vectors) feature vectors comprised of Mel-cepstral coefficients, eigenlips, and lip area measurements, experiments with the multi-modal VidTIMIT database achieve liveness verification equal-error rates of less than 1%. [7].

Russian and Czech feature vector geometric shape-based features are used, as well as DCT and PCA pixel-based visual parameterization and feature vector concatenation and multi-stream models. compiled an audio-visual database of automobile driver utterances for audio-visual recognition tests[8].

MFCC's are used to obtain acoustic features, and 48 features, 39; audio features, and 9 visual elements are used to assess the AVASR accuracy. Two-Dimensional Discrete Cosine Transform (2D-DCT), Principal Component Analysis (PCA) and Two-Dimensional Discrete Wavelet Transform followed by PCA (2D-DWT-PCA) are used to create four sets of visual characteristics [9].

Speech recordings with limited non-ideal visual circumstances, notably fixed known positions and natural lighting, are stored in a database. The movies were shot with two high-definition cameras, CANON VIXIA HG20, among a resolution of 1920*1080 pixels at 25 frames for every second, and featured the speaker's head and shoulders. The MFCC approach was employed for the feature vector and the DCT technique. The HTK toolkit is used to create three-state phoneme HMMs using three Gaussian mixtures per state. The same number of states and Gaussian distributions are employed in multi-stream HMMs as in single-stream HMMs [10].

The visual / voice encodings are concatenated in the TM-CTC model, and the output is propagated through the same stack of self-attention / feedforward modules used in the encoders. The database made use of BBC shows ranging from Dragon's Den to Top Gear and Countryfile. When decoded using a language model, TM-seq2seq yields a WER of 48:3 percent on LRS2-BBC [11].

The 3D Feature Pyramid Attention (3D-FPA) model was utilised for sentence-level lip-reading, while LipNet was employed for Robust Visual Speech Recognition[12].

They used RNN-T architecture to make a massive audio-visual dataset of segmented utterances taken from YouTube community videos (YTDEV18), 31k hours of audio-visual training, and a large audio-visual (A/V) dataset of segmented utterances taken from YouTube public videos (YTDEV18) [13].

For that AVSpeech dataset, we developed a novel Attention-based Residual Speech Portrait Model (AR-SPM) and innovatively established a tri-item loss function, which is a biased linear grouping of the L2-norm, L1-norm, and negative cosine loss, to train model by comparing the final face feature and true face feature[14].

Self-supervised AVSR framework based on Audio-Visual HuBERT (AV-HuBERT), a cutting-edge audio-visual speech representation learning model for the LRS3 AVSR benchmark dataset [15].

The Audio-Visual TIMIT (AV-TIMIT) video corpus, as well as an audio-visual integration technique based on segment-constrained Hidden Markov Models, were collected in this paper HMMs. Visual features were extracted using DCT, PCA, LDA, and the AVCSR Toolkit [16].

In response to a video question, the dual cross-modality (DCM) attention technique uses both audio/video context vector. We employed CTC loss throughout combination with our attention-based approach to enforce the monotonic alignments required in AVSR. The DCM attention scheme and the hybrid CTC/attention architecture both scored at least 7.3 percent on the LRS2-BBC and LRS3-TED datasets [17].

Lip geometric shape parameters, video frames of speakers saying Marathi digits एक, दोन, and तीन, and a DTW-based approach for identifying Marathi number utterances using visual speech recognition Geometric shape

parameters utilised for categorisation include changes in lip height, breadth, area, and height-to-width ratio in subsequent frames. Width has a 63 %, whereas area has a 46 % [18].

TABLE I. OPEN ACCESS DATABASE FOR VISUAL AUDIO RECOGNITION

Sr. No.	Database	Year	Feature Extraction Technique & Classification	Task	Result	Ref
1	LUNA-V	2014	HSV colour filter + border following + convex hull technique – MFCC, HMM	Digit recognition	92.5 % (Visual only)	[19]
2	CUAVE	2015	MFCC HMM	Digit recognition	94 %	[20]
3	RAVDESS	2018	CNN-14 and biLSTM- GuidedST HMM	Emotional Recognition	80.08%	[21]
4	China Audio Visual Equipment	2015	ERANN-0-4 HMM	Emotional Recognition	74.8	[22]
5	AVSpeech: Large-scale Audio-Visual Speech	2020	AR-SPM , MFCC	Speech to Face Generation	94.7%	[23]
6	Laboratory Conditions Czech Audio-Visual Speech Corpus	2008	DCT and PCA, MFCC	Czech language AV	96.36 %	[24]
7	VidTIMIT Audio-Video	2017	DET, MFCC		99.99%	[25]
8	The Grid Audio-Visual Lombard Speech Corpus	2019	BLSTM, CNN		97.02%	[26]
9	VoxCeleb	2019	CNN, MFCC, GMM-UBM		93.88%	[27]
10	Audio/Video Australian English Speech Data Corpus	2012	MFCC, BLSTM, CNN		97.30%	[28]

III. FEATURE EXTRACTION TECHNIQUE

A. Residual Networks and LSTMs for Lipreading

ResNets & LSTMs, respectively, are game-changers in computer vision and natural language processing. In this study, the authors tried to include the advantages of spatiotemporal convolutional, residual, and bidirectional Long Short-Term Memory networks. They proposed a word-level visual speech recognition end-to-end deep learning framework that is trained and evaluated on the Lip-reading Wild dataset.

The authors claim that the suggested network has achieved word accuracy of 83.0, representing a 6.8 absolute increase over the existing state-of-the-art, without employing word boundary information during training or testing [29].

B. LRW-1000

In this paper, the researchers present LRW-1000, a widely dispersed large-scale standard for lip-reading in the wild. It includes 1,000 classes and 718,018 samples from more than 2,000 distinct speakers. Every class defines one or maybe more Chinese characters that make up the syllables of a Mandarin sentence. In terms of the quantity of samples in each class, video resolution, illumination variations, speakers' posture, age, gender, and other factors, this experiment demonstrated a considerable difference in the benchmark. Investigated a number of various lip-reading methods and did a thorough analysis of the data from various of viewpoints [30].

C. Deep Word Embeddings

While suppressing other kinds of variability such as speaker, location, and illumination, this study summarises the embeddings of the mouth area that are critical to the problem of word identification. A spatiotemporal conv layer, a Residual Network, and Bi-LSTMs make up the system, which was trained using the Lipreading in-the-wild database. The results show a promising 11.92 percent error rate on a vocabulary of 500 words. In order to execute low-shot learning, PLDA was utilised to model embeddings on words that were not encountered during training. Even when the target words aren't in the training set, the experiments indicated that word-level visual voice recognition is feasible [31].

D. Read Speech Beyond Lips

In this paper, the researchers investigate one of the most understudied aspects of VSR research: reading of the excisional facial landmarks, i.e. far beyond lips. Experiments were conducted on objectives with varied features at the word and sentence levels. The testing indicated improvements above previous methods that just employed the lip area as an input. The efficiency of this approach revealed that integrating data from extraoral facial regions, such as the face, increased VSR performance on a regular basis [32].

E. Identifying Audio/Visual Speech Recognition Adversarial Attacks

Adversarial assaults have lately emerged as one of the most actively investigated issues in the deep learning domain. Because of the drawbacks that these assaults have shown, researchers are on the watch for similar anomalies even in reinforcement learning. In a similar vein, a detection approach based on the temporal correlation of audio and video streams is presented in this study. The notion here is that because of the additional hostile noise, the correlation between audio and video in adversarial samples will be lower than in

benign examples. This is the first study to look at detecting adversarial assaults on audio-visual speech recognition algorithms. According to the findings of the experiments, the authors have proved that the proposed technique is an effective way of identifying such assaults [33].

IV. CONCLUSION

A comprehensive review of the extant literature on Audio-Visual Speech Recognition. We addressed the exciting feature extraction (MFCC) and techniques like HMM, GMM, ResNets, LSTMs, LRW-1000 in the comparative research study. It will be beneficial to examine how Audio-Visual Speech Recognition for low-resource languages may be developed in the future.

V. REFERENCES

[1]. Ali, M. H., Jaber, M. M., Abd, S. K., Rehman, A., Awan, M. J., Vitkutė-Adžgauskienė, D., ... & Bahaj, S. A. (2022). Harris Hawks Sparse Auto-Encoder Networks for Automatic Speech Recognition System. Applied Sciences, 12(3), 1091.

[2]. Gurban, M., & Thiran, J. P. (2005, September). Audio-visual speech recognition with a hybrid SVM-HMM system. In 2005 13th European Signal Processing Conference (pp. 1-4). IEEE.

[3]. Hao, M., Mamut, M., Yadikar, N., Aysa, A., & Ubul, K. (2020). A Survey of Research on Lipreading Technology. IEEE Access.

[4]. Malviya, S., Mishra, R., & Tiwary, U. S. (2016, October). Structural analysis of Hindi phonetics and a method for extraction of phonetically rich sentences from a very large Hindi text corpus. In 2016 Conference of The Oriental Chapter of International Committee for Coordination and Standardization of Speech Databases and Assessment Techniques (O-COCOSDA) (pp. 188-193). IEEE.

[5]. Isobe, S., Tamura, S., Hayamizu, S., Gotoh, Y., & Nose, M. (2021). Multi-angle lipreading with angle classification-based feature extraction and its application to audio-visual speech recognition. Future Internet, 13(7), 182.

[6]. Werda, S., Mahdi, W., & Hamadou, A. B. (2013). Lip localization and viseme classification for visual speech recognition. arXiv preprint arXiv:1301.4558.

[7]. Chetty, G., & Wagner, M. (2004, December). Liveness verification in audio-video speaker authentication. In in Proc. 10th ASSTA conference.

[8]. Císař, P., Zelinka, J., Železný, M., Karpov, A., & Ronzhin, A. (2006, June). Audio-Visual speech recognition for Slavonic languages (Czech and Russian). In Proc. of 11-th International Conference SPECOM-2006, St. Petersburg:—Anatoliya.

[9]. Anderson, S. J. (2012). Lip reading from thermal cameras (Doctoral dissertation, Auckland University of Technology).

[10]. Young, S. J., & Young, S. (1993). The HTK hidden Markov model toolkit: Design and philosophy.

[11]. Afouras, T., Chung, J. S., Senior, A., Vinyals, O., & Zisserman, A. (2018). Deep audio-visual speech recognition. IEEE transactions on pattern analysis and machine intelligence.

[12]. Xiao, J. (2018). 3D Feature Pyramid Attention Module for Robust Visual Speech Recognition. arXiv preprint arXiv:1810.06178.

[13]. Makino, T., Liao, H., Assael, Y., Shillingford, B., Garcia, B., Braga, O., & Siohan, O. (2019, December). Recurrent neural network transducer for audio-visual speech recognition. In 2019 IEEE automatic speech recognition and understanding workshop (ASRU) (pp. 905-912). IEEE.

[14]. Wang, J., Hu, X., Liu, L., Liu, W., Yu, M., & Xu, T. (2020). Attention-based Residual Speech Portrait Model for Speech to Face Generation. arXiv preprint arXiv:2007.04536.

[15]. Shi, B., Hsu, W. N., & Mohamed, A. (2022). Robust Self-Supervised Audio-Visual Speech Recognition. arXiv preprint arXiv:2201.01763.

[16]. Hershey, J. R., & Casey, M. (2001, January). Audio-Visual Sound Separation Via Hidden Markov Models. In NIPS (pp. 1173-1180).

[17]. Lee, Y. H., Jang, D. W., Kim, J. B., Park, R. H., & Park, H. M. (2020). Audio–visual speech recognition based on dual cross-modality attentions with the transformer model. Applied Sciences, 10(20), 7263.

[18]. Brahme, A., & Bhadade, U. (2017, November). Marathi digit recognition using lip geometric shape features and dynamic time warping. In TENCON 2017-2017 IEEE Region 10 Conference (pp. 974-979). IEEE.

[19]. Seong, T. W., Ibrahim, M. Z., & Mulvaney, D. (2019). WADA-W: A modified WADA SNR estimator for audio-visual speech recognition.

[20]. Patterson, E. K., Gurbuz, S., Tufekci, Z., & Gowdy, J. N. (2002, May). CUAVE: A new audio-visual database for multimodal human-computer interface research. In 2002 IEEE International conference on acoustics, speech, and signal processing (Vol. 2, pp. II-2017). IEEE.

[21]. Luna-Jiménez, C., Griol, D., Callejas, Z., Kleinlein, R., Montero, J. M., & Fernández-Martínez, F. (2021). Multimodal Emotion Recognition on RAVDESS Dataset Using Transfer Learning. Sensors, 21(22), 7665.

[22]. Issa, D., Demirci, M. F., & Yazici, A. (2020). Speech emotion recognition with deep convolutional neural networks. Biomedical Signal Processing and Control, 59, 101894.

[23]. Wang, J., Hu, X., Liu, L., Liu, W., Yu, M., & Xu, T. (2020). Attention-based Residual Speech Portrait Model for Speech to Face Generation. arXiv preprint arXiv:2007.04536.

[24]. Císař, P., Zelinka, J., Železný, M., Karpov, A., & Ronzhin, A. (2006, June). Audio-Visual speech recognition for Slavonic languages (Czech and Russian). In Proc. of 11-th International Conference SPECOM-2006, St. Petersburg:—Anatoliya.

[25]. Chetty, G., & Wagner, M. (2004, December). Liveness verification in audio-video speaker authentication. In in Proc. 10th ASSTA conference.

[26]. Morrone, G., Bergamaschi, S., Pasa, L., Fadiga, L., Tikhanoff, V., & Badino, L. (2019, May). Face landmark-based speaker-independent audio-visual speech enhancement in multi-talker environments. In ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 6900-6904). IEEE.

[27]. Nagrani, A., Chung, J. S., Xie, W., & Zisserman, A. (2020). Voxceleb: Large-scale speaker verification in the wild. Computer Speech & Language, 60, 101027.

[28]. Goecke, R., & Millar, J. B. (2004, October). The audio-video Australian English speech data corpus AVOZES. In Proceedings of the 8th International Conference on Spoken Language Processing INTERSPEECH (pp. 2525-2528).

[29]. Zhou, X., Liu, Z., Wang, F., Xie, Y., & Zhang, X. (2020). Using deep learning to forecast maritime vessel flows. Sensors, 20(6), 1761.

[30]. Yang, S., Zhang, Y., Feng, D., Yang, M., Wang, C., Xiao, J., ... & Chen, X. (2019, May). LRW-1000: A naturally-distributed large-scale benchmark for lip reading in the wild. In 2019 14th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2019) (pp. 1-8). IEEE.

[31]. Stafylakis, T., & Tzimiropoulos, G. (2018, April). Deep word embeddings for visual speech recognition. In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 4974-4978). IEEE.

[32]. Zhang, Y., Yang, S., Xiao, J., Shan, S., & Chen, X. (2020, November). Can we read speech beyond the lips? rethinking roi selection for deep visual speech recognition. In 2020 15th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2020) (pp. 356-363). IEEE.

[33]. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Survey on Handwritten English Character Recognition Methods

Amey Pachpande, Vishv Shah, Karishma Shah, Omkar Vaidya, Srushti Variya, Dr. C.H. Patil
School of Computer Science, MIT World Peace University, Pune, Maharashtra, India

ABSTRACT
Handwritten character Recognition plays an important role in various fields of automation. It is applicable in areas of Bank, medicine prescriptions etc. Handwritten characters are much more difficult to recognize than printed characters. For handwritten character recognition deep learning techniques such as Convolutional Neural Networks is used as they are better than other conventional methods.

Keywords— Directed Acyclic Graph (DAG), Convolutional Neural Network (CNN), Rectified Linear Unit (ReLu), Handwritten Character Recognition (HCR), Optical Character Recognition (OCR), Generative Adversarial Networks (GAN), Generalized Chain Code (GCC), Hidden Markov Model's (HMM), Recurrent Neural Network (RNN), Character precision rate (CAR), Support Vector Machine (SVM), Handwritten English Character Recognition (HECR).

I. INTRODUCTION

Typing data manually into computer is a tedious and time-consuming job. Since 1870, many advancements are made in character recognition. In the middle of 1950 Optical Character Recognition (OCR) machines became popular. OCR methods can be classified into deep learning and conventional methods. Conventional methods are based on handcrafted features whereas deep learning methods include various Neural Network models.

II. PROPOSED SYSTEMS

A. Directed Acyclic Graph Technique

Deep learning techniques play a vital role in OCR. It comes under kingdom of Artificial Intelligence (AI) [10]. This method incorporates tracking machines that have a large amount of data and have high accuracy and flexibility. When using Convolutional Neural Networks (CNN) for cursive alphabets there are chances that alphabets are misclassified. In order to avoid this, DAG is applied to basic CNN. The proposed system has various modules like data acquisition, dataset augmentation, partitioning of training and testing data etc. Directed Acyclic Graph (DAG) is multi-scale Convolutional Neural Network which can be subdivided into several paths [10]. DAG is not a linear structure. It's can have multiple inputs and outputs. Multiple connection to each layer allows every

layer to be connected to final classifier directly, skipping connections. Since we r taking features from low, mid and high level there will be over fitting. This can be avoided using Greedy Forward selection strategy [10]. DAG is suitable solution as it incorporates features from every layer. Advantage is that most features will be available free as they are already processed by some layers. Then features will be extracted at each layer then after normal average pooling operation, output will be given to SoftMax module for classification and accuracy prediction.

B. Generative Adversarial Network Technique

Many historical documents have English cursive handwriting which is hard to recognize using automated English cursive recognition. This is due to difficulty in segmentation of connected characters in words. This issue can be resolved using Generative Adversarial Networks (GAN) [6]. GAN is a type of deep learning method for image stylization, recognition and classification. It includes one neural network that generates results according to samples of databases and one discriminates that generated image from samples within that same database. The model used in these papers can be stated as multilayer perceptron. Most important difference of GAN and other neural networks is adversarial nature of GAN [6]. We are using Content GAN (MC GAN) for font transfer with great results and is also able to generate scripts with different fonts. For recognizing English cursive an intermediate font is used between original script and final output. File transfer from original script to intermediate font is done by GAN and result is obtained by using conventional OCR algorithm. Disadvantage of GAN here is that it generates one-to-one results. That means it generates different outputs for different inputs. Other GAN methods are also of great use in image morphing, image style transfer and other areas of this field [6]. This method is also used for other languages' scripts.

C. Optical Character Recognition

This idea is for identification of English and Tamil letters. Neural Networks are used to provide algorithm to recognize letters. Many old documents having old scripts which are difficult to recognize can be solved by converting handwritten data to machine readable by using this method.[11] The major problem with Optical Character Recognition (OCR) is that caused due to different styles and sizes of writing. But it can be solved using Artificial Intelligence (AI) and Machine Learning. The process is carried out as input is given to machine and after processing it is finally compared to trained algorithms like SVM and CNN classifier algorithms to classify letters and provide output [11]. This approach is based on Neural Network to determine each set of characters. Another method deals with MATLAB that contains neural system to identify letters by images. This new concept is Feature Extraction which is used to improve identification rates. To optimize handwritten data with accuracy we have proposed a method. Methods such as- Pre-processing, classification, Feature Release,[11] Editing and Visibility are used for character recognition in this approach.

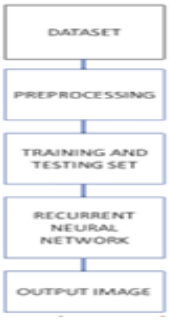


Fig. 1 Flowchart of proposed approach [11]

- To reduce noise parameters from given image, pre-processing technique is used. Techniques like noise filtering, Smoothing & sharpening, Normalization, Binarization are used.
- In segmentation the image is partitioned into separate image. Line segmentation technique is used in this method.
- Most important process in the method is feature extraction. Datasets based on geometric character and gradient method of character are trained for given image in this method.
- Classification and recognition methods are used for classification of input images. This technique is used to determine patterns that exactly matches to input image.
- By feature extraction, image is classified, and exact output is recognized

Without changes in the sizes and styles, this method is effective to generate handwritten text images. Advantage of this method is, that accuracy depends upon handwritten text. MATLAB platform is used here with help of neural trained datasets.

D. Hidden Markov Model and Deep Learning Technique

The Writing of any individual can be recognized by tracing and image transfer and on the basis of freehand simulation. There are many systems developed for English character recognition but due to some flaws it does not provide that much accuracy, so more research works are being carried out in recognition works and automatic detection through computer techniques, feature extraction, classification accuracy comparison, performance evaluation and pattern recognition. Various characteristics are taken into consideration to differentiate the handwritten characters, they are height, width and size of characters, beginning and ending strokes, unusual letter formation, pen pressure. Many external features can also affect the handwriting because of pen tip type, smoothness and material of paper, types and colors of ink and the speed of writing.

An electronic pen of high sensitivity is used as a tool to write on electronic surface in order to have a higher detection accuracy. The input given by the electronic pen are basically raw and to retrieve the qualitative data it needs to be filtered. The Hidden Markov model (HMM) is used to extract the data from the sequence of features by using three components of recognition such as multidimensional LSTM, multidimensional recurrent neural network and the hierarchical structure. To recognize the scanned characters or written text characters online, optical character recognition is also used. Its approach is that in order to detect the characters/letters properly before learning different languages it must be familiar with the particular language.[8] After that advanced version of OCR came into existence known as Intelligent Character Recognition (ICR) which showed better performance i.e., extracting the text from poor-quality image and used more optimized algorithms than OCR.

There are two methods associated with deep learning first one is data collection where raw data is collected and tested on a different pixel environment and the second one is pre-processing where the raw data is filtered and then finalized as an acceptable data.[8] An experiment was conducted for a group of 25 people which showed how the number of pixels influence the character detection. This experiment was done on 5 * 7-pixel environment. The characters taken into consideration were straight stroke characters (‘V’, ‘X’, ‘Y’) and curve stroke characters (‘C’, ‘O’, ‘S’) which increases the difficulty level in the detection because these characters are having similar writing patterns and thus creates the confusion for character detection. Throughout the experiment the successful recognition rate for straight stroke characters was 35.92% to 44.00% and for the curve stroke characters it was 64.00% to 61.44%.[8] The successful recognition rate changes based on different pixel

environments. There are some characters which are misrecognized repeatedly from a selected group of characters in which the highest misrecognized character was 'Y' and 'W' and the lowest misrecognized character was 'C'.

Table 1(a): Result of Stroke character detection [8]

5x7 Pixel Environment		35x33 Pixel Environment
Character	Success Recognition Rate (%)	Success Recognition Rate (%)
V	35.92	85.40
X	53.32	82.84
Y	44.00	81.48

Table 1(b): Result of Curve Character detection [8]

5x7 Pixel Environment		35x33 Pixel Environment
Character	Success Recognition Rate (%)	Success Recognition Rate (%)
C	64.00	92.08
O	60.04	84.12
S	61.44	82.84

E. Fuzzy Logic Technique

During the last two decades significant work has done in the field of handwritten characters recognition. The process of recognition based on fuzzy logic approaches pre-processing of characters covering characters for translation invariance and normalization of characters for changes in size.[14] In the process of normalization all extracted character bitmaps are identified in order to match isolated character patterns against database-characters using features such as junction points and distance between points. There are many types of normalization with regard to size, position, skew, line and width of the character.

Every person has their own style of writing and for that reason variability in a character is seen and this variability is shown in difference in size, translation and rotation. To invariant the translation from the text, each individual character is isolated into a box. It is very hard to eliminate the rotation variant through end points, junction points, and number of branches and angles, to end this difficulty fuzzy logic-based approach is used.[14] Here in this approach normalized angles which are connected with section of character are used moreover to classify the character into group different points are located. Each pixel is delegated a direction code. These direction codes are computed with associated angles and normalized angles.

Variability is also seen in the feature data. To deal with this variability cluster for mean and variance is formed. Gaussian fuzzification function is used to find out mean and variance for large number of samples. At the recognition stage character is searched then computed with associated normalized angles. After that membership function of each normalized angle of input character is determined, using this function fuzzy distance is calculated. The character is recognized to be that reference character which produces the least fuzzy distance.[14] Special points are detected through scanning and storing the skeleton in matrix. Skeletonization method is used to define and examine all the branches. When all the branches are formed into skeleton, they are vectorized. Vectorization means assigning a direction code to every pixel of branch

F. A Chain Coding Approach

The novel's method of coding is proposed in real time English handwritten recognition online characters. New version of generalized chain code (GCC) proposed for non-missing coding for diversity-spaces handwritten data points naturally generated by tablet writing electronically due to fixed sample size once flexible writing speed. Different features for each the character are then extracted based on segments standard aggregate GCC values and adjectives of structure.[12] The test was shown successfully real-time recognition of one handwritten online small English letter on PC class 486 Coding is a way of dividing the space, to enter the curve code, one must find the nearest vector node: cross curve in the center of the square text instead of the previous encoding. Chain codes are common are a special class of chain codes that use multiplication embedded code rings. For maximum efficiency, number of the ring sizes that can be used are limited, and such it is usually predetermined to allocate a unique binary code for all vector nodes.

The proposed GCC system was used for coding alone Online English handwriting letters and l NGCC values are inclusive produced by each character.[12] Recognition system used on 486 class PC connected to electronic tablet. The author was asked to write one character while using tablet and real time: recognition had been made. Medium visibility more than 90% is achieved with letters in small capital letters English letters. The whole process is inclusive pre-processing, GCC coding, feature extraction and more recognition was made in less than 1 second [12].

The novel's method of coding has been suggested unencrypting technique for handwritten data taken from the tablet and real-time recognition of one handwritten online character are created in the PC platform area.

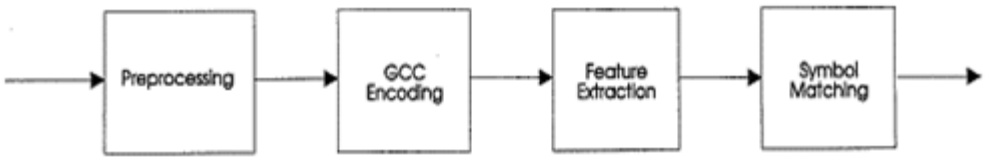


Fig 2. Block diagram of the recognition system [12]

Through the proposed GCC system, most of these characters can be divided into three parts or less. Quick recognition can be done directly based on different NGCC combined pattern patterns to other characters. Fig 2 shows the total block diagram of the awareness system.

G. Using On-line Character Writing Information

Identification of character patterns disabled in variety is an important theme for offline handwriting recognition. Adequate recognition functionality of actual use has not been achieved despite reports that many ways to be aware.[1] Simple pattern compatibility methods, matching patterns based on guiding elements methods, methods of Neural Network and Hidden Markov Model methods (HMM) are represented as standard methods of recognition. A simple pattern corresponding to the character the recognition and recognition methods of HMM characters are used in our proposed way to evaluate the proposal a common stretch method using an online character writing information.

This study proposes a method of recognition using online writing information that includes typing information. Our proposed method is used online information as an image measurement filter in a pre-processing phase.[1]

The proposed approach sees the closest recognition performance in pattern matching based on direction of how to use using only 1/20 of calculation time for comparison.

H. Using Character Bigram Match Vextors Technique

This paper describes the level of the word variable, which is partial, it depends on the author, the system of recognizing handwriting that uses English n-gram arithmetic language. The program benefits from the language material very few pairs of English words share exactly the same set of capital letters.[4] This building is used for delivery language context up to the recognition stage. I recognition is based, measuring the probability that major events between words. Previous testing using absurd features and limited training sets indicate that the system can detect more than 60% words. I have never seen it before in a handwritten way. System has only a few trained parameters. In addition, increasing training is mathematically costly. The recognition system is based on to find features of matching between words. The program uses a dictionary and a reference set. A lexicon is a set of label names from which is the system that selects the effect of recognition [4]. Here reference set is a set of handwritten words, represented internally another feature of the space, which has corresponding word labels. Receives major events from feature level representation, used to paraphrase words includes some of the benefits of character level as well word level recognition. As a character-based recognition, the dictionary expands, and recognition does not end their words with clear samples in the training set. As widely used Hidden Markov methods, based on feature bigram discovery brings context to the recognition stage instead of returning it to its configuration.[4] Unlike HMMs, neural networks and other machine learning methods, the system requires an average of only a few parameters. The proposed method is best suited to the author recognition.

I. Athena Model Technique

The Athena model uses a neural for handwriting recognition. The neural net used for handwriting recognition are based on same model. The Athena model has several layers and then need to be presented parallel one by one layer.[3] Here the training goes from the root to the leaves and in a binary tree format based on neurons. This helps to make the learning time a little bit less and it dynamically decides the leaning process. As handwriting recognition involves many processing phases, so the main aspect of this model is on the classifier. The model learns by recognizing more and more patterns. In this process no information is lost and the net does not forget any pattern [3]. As the Athena model is simple and fast with the training and its dynamic net expands during the process it is best suited as incremental learning. It has a good level of success. The Rum 86 or Rumelhart is the purest form of neural net which consist of the neurons present in a multilayer architecture [3]. The Athena model was developed at research at cast western where it consists of a multilevel tree.

The four stages in this approach are -

- Vision Stage
- Object Detector
- Preprocessor
- Feature extractor
- Classifier

The main research work emphasis on the Classifier and its learning abilities as it supports incremental learning abilities.

J. Feed Forward Back Propagation Neural Network Technique

Character Recognition System consist of pre-processing, segmentation, classification & post-processing stages.[2] First of all, acquired handwritten image through scanner or any other digital input device in any specific format. Then that image firstly converted from grey scale to binary image using global thresh holding technique followed by dilation of edge in the binarized image using Sobel technique and then after filling the holes present in the image, we will get the processed image for the segmentation.[2] In segmentation, image is decomposed into isolated individual characters by assigning number to each character using labelling process and each individual character resized into 30x20 pixels. Classification is decision making part of the recognition system. Feed Forward Back Propagation Neural Network is used in this recognizing system. 600 pixels derived from resized characters in segmentation stage from input to the classifier. Neural network consists of Two Hidden Layers between input and output layers. Two hidden layers use log sigmoid activation function where output layer is a competitive layer as one of the characters is required to be identified at any point in the time. Total number of neurons in output is 26 because of English alphabets. In post-processing stage, it prints character in structured format (Computerized). Proposed system has been implemented using mat lab(v.7.1). 7 different neural network architecture were chosen & each was trained with 50 data sets for a target MSE of 10e-8. Each hidden layers having 100 neurons so that its highest recognition accuracy is 90.19% [2]. The proposed system will be a little more complicated compared to offline methods using feature removal techniques. Rather than using several neural network architectures, using one neural network architecture having two hidden layers having 100 neurons each has been found highest recognition memory.

K. Recurrent Neural Network Technique

Optical Character Recognition System consist of Datasets, pre-processing, Training and Testing, Recurrent Neural Network, Output Image. [7] Firstly, scan the handwritten characters as dataset and then crop each character physically & label each separately as image then it is used for character recognition. After that resize all pictures & convert to grey scale structure. Alter pixels force. Include cushioning of 2 pixels all sides it is a grey scale of size 128x32. It will be resized until it either has a width of 128 or a tallness of 32. Duplicate of the image into objective picture of 128x32. Information increase can without much of a stretch be coordinated by duplicated image to irregular situation as opposed to adjusting it to one side or by arbitrarily resizing the picture. Then in the training and testing stage, first split the data into training and testing set. All the characters are adjusted at their positions. This activity is without division and couldn't care less about outright positions. Its clear name, the content can undoubtedly be decoded and finally OCR has effectively distinguished the characters from the picture [7]. In this system, there is a need to recollect the past words. Accordingly, RNN appeared, which comprehended this issue with the assistance of hidden layer. Input layer will hold the pixel estimation of the picture. RNN yield succession is mapped to a network of size 32x80. Finally, the output image is given as formal printed text. Word exactness rate level of words with all characters effectively recognized [7]. Character precision rate (CAR) normal Level stein separation standardized by the length of the longest word and subtracted from 1. In this framework, the handwritten English Document are scanned and recognized optically. by using RNN. Output is got as printed text with 90% accuracy.[7] In addition, need to examine the issue further for discovering better arrangement by planning a totally new engineering.

L. Using Database

Today's website is even more important for research. They are important for development, testing and comparison. In recognition of handwriting many programs are designed for individual letters. In every word in the text a tag is used.[13] On this site is the Lancaster-Oslo / Bergen corpus (LOB), a collection of 500 English texts, each with about 2,000 words in use. The text is then divided into choruses into 3 to 6 sentence pieces with at least 50 words each. The sentences are then taken out of each text piece and a document containing the text and form structure is created. The next three digits indicate which sentence the text begins with. [13] In the second part of the form the people who are asked to write it are published. Each form was completely scanned, including printed and handwritten text. Data labelling is a requirement for recognition testing because data labelling is expensive, time consuming and prone to error, we decided to do it automatically as much as possible. Once the left and right end of the first horizontal dividing line is found, the skew angle is used to adjust the skew of the entire document. After all, with three horizontal lines found, we are able to extract part of the form containing the manuscript. After the handwriting was divided into individual lines, the printed section labels were copied and the line feeds were completed by hand. In some cases, corrections are needed because the handwriting does not fit exactly with the printed text. The website can serve as a research base for handwriting recognition. A few processes of analysis and classification have been developed along with the website. [13] Their main purpose was to assist in the automatic labeling of websites, but they can be integrated into any recognition system.

M. Mobile Application for handwritten character recognition

The proposed app will offer an offline handwriting recognition system that can be used as a teaching aid for low level students. [5] The whole system works in the following ways:

- The handwritten character is stored in bitmap type for processing.
- Then the characters are separated using a display method, first the input image is processed in advance by lowering the font.
- Secondly each connected component is labeled.
- Separation of the third projection on each item is done.

The distinctive end points are used to extract each character from the input image. Image familiarity is applied to each character with categories. After the classification is done for each character that has categories.[5] To perform the character separation using the Tensor Flow Lite model. Different types of partitions are designed for specific tasks. The reason for creating a separate separator is to match the type of split with academic content that has a high degree of separation. Tests performed on handwritten data are collected from low-level students. The result of the separation and the number of characters will be displayed on the screen for accuracy [5]. Sometimes, there are similarities between digits and letters such as '0' (digit) and 'o' (lower case), '1' (digit) and 'l '(lower case) and so on. Therefore, a separator can sometimes distinguish between these same characters. Overall, the system test results are promising and have a good recognition value for all class dividers.

N. Convolutional Neural Network Technique

There have been many HECR studies, but most of them are done with online information or pure offline information [9]. The CNN model used in this paper has been replaced by LeNet-5. They are experimenting with various modes based on the basic structure of LeNet-5 in order to find the trade between the time costs and the

performance of the recognition. First, change the number of neurons in each CNN layer. This may validate different feature maps in layer C4 to obtain different sets of features from layer C2. First, CNN parameters may be updated at different levels. Second, from layer C2 to layer C4, some feature maps will receive less information than others. It is important to make the photos more natural [9]. In our experiment, we expand the pixels of a three-dimensional image: 20×20, 28×28 and 32×32, where the left-hand parts of the input are combined with the background value.

During CNN training, it usually encounters two problems. First, compared to the traditional backpropagation (BPN) distribution network, CNN training is time consuming, because CNN has tens of thousands of parameters to review. One reason the sample-errors in the training set may be too low is that they could create significant impacts on CNN [9]. The test is based on section 1b (uppercase) and 1c (lower case) of the UNIPEN Train-R01 / V07 website. These two categories consist of 28069 capital letters and 61351 lowercase capital letters, respectively. LeNet-5 results are set with debug codes; thus LeNet-5 had the ability to reject illegal samples in its research in order to recognize printed characters. Rejection should be more meaningful in recognizing a handwritten character, where many samples are of an unrestricted, or illegal, style. CNN output is set by EC codes, thus CNN, has the power to refuse recognition. Comparison with other high-quality alternatives, CNN has provided an efficient and accurate way for HECR solution

III. CONCLUSION

Handwritten Character Recognition is very important now a days. These methods can be used in areas like medicine prescriptions, tax returns, old historic documents etc. The main challenge we face in these techniques is that there is a huge variability and ambiguity in the handwriting of each person which varies time to time and is also inconsistent.

Best method for alternative of conventional handcrafted features is to use deep learning and neural networks. Convolutional neural networks have better accuracy rates than other methods as it has the ability to reject the recognized character because the CNN output is set by EC codes. We would like to find more efficient and accurate techniques of detection irrespective of the quality, handwriting, strokes of the English character

IV. REFERENCES

[1]. Off-line Character Recognition using On-line Character Writing Information by Hiromitsu NISHIMURA and Takehiko TIMIKAWA Dept. of Information and Computer Sciences, Kanagawa Institute of Technology 1030 Shimo-ogino, Atsugi, Kanagawa, Japan {nisimura, tomikawa}@ic.kanagawa-it.ac.jp

[2]. Neural Network based Handwritten Character Recognition system without feature extraction J.Pradeep# , E.Srinivasan# , S.Himavathi* # Department of ECE, Pondicherry Engineering College, Pondicherry, India E-mail id: jayabala.pradeep@pec.edu# , esrinivasan@pec.edu# * Department of EEE, Pondicherry Engineering College, Pondicherry, India E-mail id: himavathi@pec.edu

[3]. Handwritten Character Recognition with the ATHENA Model by Anders Abrahamsson Linkoping Institute of Technology Linkoping, Sweden Cris Koutsougeras Computer Science Department Tulane University New Orleans, Louisiana 701 18 Christos A. Papachristou Computer Engineering and Science Department Center of Automation and Intelligent Systems Research Case Western Reserve University Cleveland, Ohio 44106

[4]. On-Line Handwriting Recognition Using Character Bigram Match Vectors by Adnan El-Nasan Rensselaer Polytechnic Institute Troy, NY USA elnasan@rpi.edu, Michael Perrone IBM T.J. Watson Research Center Yorktown Heights, NY USA mpp@us.ibm.com

[5]. A Mobile Application for Offline Handwritten Character Recognition Thi Thi Zin, Moe Zet Pwint, Shin Thant Graduate School of Engineering University of Miyazaki Miyazaki, Japan.

[6]. Recognizing English Cursive Using Generative Adversarial Networks Xinrui Yu and Jafar Saniie Embedded Computing and Signal Processing Research Laboratory (http://ecasp.ece.iit.edu/) Department of Electrical and Computer Engineering Illinois Institute of Technology, Chicago, IL, U.S.A.

[7]. Optical Character Recognition for English Handwritten Text Using Recurrent Neural Network R.Parthiban1,R.Ezhilarasi2 ,D.Saravanan3 Associate Professor1,3, Department of CSE, IFET College of Engineering, Villupuram1,3 Final Year Students2 ,Department of CSE, IFET College of Engineering, Villupuram2

[8]. Handwriting Detection and Recognition Improvements Based on Hidden Markov Model and Deep Learning by Mohammed Hazim Alkawaz Faculty of Information Sciences & Engineering Management and Science University Shah Alam, Selangor, Malaysia , Cheng Chun Seong School of Graduates Studies Management and Science University Shah Alam, Selangor, Malaysia, Husniza Razalli Faculty of Information Sciences & Engineering Management and Science University Shah Alam, Selangor, Malaysia

[9]. Offline Handwritten English Character Recognition based on Convolutional Neural Network Aiquan Yuan, Gang Bai, Lijing Jiao, Yajie Liu College of Information Technical Science Nankai University Tianjin City, China

[10].A Proposed Framework for Recognition of Handwritten Cursive English Characters using DAG-CNN by Bhagyasree P V Department of Computer Science and Engineering, Govt.Engineering College Thrissur,Kerala, Ajay James Assistant Professor, Department of Computer Science and Engineering, Govt.Engineering College Thrissur,Kerala, Chandran Saravanan Associate Professor, Department of Computer Science and Engineering, National Institute of Technology Durgapur, West Bengal.

[11].Recognition Of Cursive English Handwritten Characters by Pritam Dhande Department of Computer Engineering Pimpri Chinchwad College of Engineering,Pune,India , Reena Kharat Department of Computer Engineering Pimpri Chinchwad College of Engineering,Pune,India

[12].A Chain Coding Approach for Real-Time Recognition of On-line Handwritten Characters by Hung Yuen Department of Electronic Engineering The Hong Kong Polytechnic University, Hong Kong

[13].A full English sentence database for off-line handwriting recognition by U.-V. Marti and H. Bunke Institute of Informatics and Applied Mathematics University of Bern, Neubr¨uckstrasse 10, CH-3012 Bern, Switzerland

[14].Fuzzy Logic Based Handwritten Character Recognition by M. HANMANDLU Dept. of Electrical Engg. I.I.T, Delhi New Delhi-1 10 016 INDIA, K. R. MURAL1 MOHAN Dept. of Computer Engg, Delhi College of Engg. Kashmere Gate Delhi-110 006, VIVEK GUPTA All India Radio Akash Vani Bhavan Parliament Street New Delhi- 110001.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

AI Based Smart Agriculture System

Chinmay Anand[1], Soumya Bajpai[1], Varsha A Shukre[2]
[1]Student, School of Computer Science, Faculty of Science, MIT-WPU, Pune, Maharashtra, India
[2]Assistant Professor, School of Computer Science, Faculty of Science, MIT-WPU, Pune, Maharashtra, India

ABSTRACT
Indian agriculture history dates back to Indus valley civilization era and even earlier to that somewhere in southern India. Agriculture sector comes forward as one of the foundational industries in the Indian economy. This suggests that it also holds a large proportion of employment in India. Looking at the stats as per February 14,2022, about 60% of the Indian population works in agriculture contributing around 18% in India's GDP. Unfortunately, this share is lowering with each passing year because of the development in other sectors. Farmers in India face so many distinct issues that they are forced to switch to other sectors. In-spite of Covid-19 pandemic, agriculture has sustained to be a major employer and GDP contributor in India. Though the government of India has introduced several new schemes and initiatives to supports Indian farmers. Still the basic common difficulties which the farmers have on face on ground-level is somehow far from the vision of the government. Hence, we have come up with an idea of "AI-based smart agriculture system" which will leave a great impact in agriculture sector by not only assisting farmers to solve their daily challenges but will also be their best companion to answer all their doubts with facts and figure, in their suitable language.

Keywords: Agriculture, Fertilizers, Recommendation, Soil health parameters, Real-time analysis

I. INTRODUCTION

The increasing number in country population leads to a higher demand in food [4]. Soil nutrients and various seasons have a straight forward impact on the crop growth and yield. Any nutrient whether deficient or in excess can cause toxicity to the crops [5]. Hence, the importance of fertilizer rises. Fertilizers are substances containing chemical elements such as manure or mixture of nitrogen, phosphorus and potassium that improves the growth of plants [7]. Soil plays a vital role in agriculture and the nutrients on the soil has a direct impact on quality of crops growing on it [6].
This system simplifies farming for farmers. From soil analysis to fertilizer recommendation, this system reduces many hassles all at a single place. Different crops require different nutrients at different growth periods [4]. The proposed system will assist individual farmers for obtaining soil health parameters of agricultural fields to recommend suitable crop and the dose of fertilizers for that particular crop. The system will use real time soil

analysis data for fertilizer recommendation. And hence, it will assist farmers in better cultivation and fertilization of the crop.

The existing systems measure soil parameters and changes across India using methodologies like Conductivity Measurement Technique, Electrochemical Method and Optical Method. Further, farmers especially in India are so far dependent on the traditional Manual Chemical method to find soil composition. This method not only takes too much time but also does not provide accurate results.

The proposed system performs real-time soil analysis using highly accurate automated sensors to determine NPK value along with other parameters. It then gives crop recommendation along with the fertilizer recommendation for the particular soil type. The proposed system ensures higher accuracy with efficient results. It attains this precision with the implementation of high accuracy algorithms using real-time data. It comes forward as an Affordable system with comparatively efficient pricing model.

II. RELATED WORK

Many students and researchers have contributed their work in national and international research papers, thesis to understand the objective, types of algorithms they have used and various techniques for pre-processing and suggesting solutions for farming challenges.

Varsha A. Shukr, Supriya S. Patil under “Comparative Study of Different Methodologies used for Measuring Soil Parameters: A Review” proposed sensing technologies with references and merits/ demerits [1].

Liming Chen, Liming Xu, Yanlong Hou in “A Control System for the Mechanism of Fertilizer Proportioning and Mixing Based on the Nitrogen, Phosphate and Potassium Fertilizer”, concluded that the precision agriculture’s key technology is the rational use of fertilizers. They attempted to come up with a system for fertilizer proportioning and mixing on the grounds of Nitrogen, Phosphate and potassium-based fertilizers [2].

Hema Pallevada, Siva parvathiPotu, Teja Venkata Kumar Munnangi, Bharath ChandhraRayapudi, Sai Raghava Gadde, Mukesh Chinta in “Real-time Soil Nutrient detection and Analysis”, tested various soil types to determine nutrients, pH and overall analysis and suggested the deficient nutrient [3].

Izuddin Zainal Abidin1, Faizal Ahmad Fadzil, Yen Shin, under “Micro-controller Based Fertilizer Dispenser Control System”, presented a user-friendly platform to keep a check on the soil condition and fertilization process [4].

JenskieJerlin I. Haban, John Carlo V. Puno, Argel A. Bandala, Robert KerwinBillones, Elmer P. Dadios, Edwin Sybingco, in “Soil Fertilizer Recommendation System using Fuzzy Logic” used fuzzy logic system to develop a fertilizer recommender [5].

Z. Ren and X. Lu, in "Design of fertilization recommendation knowledge base and application," focused on decomposition of the model by method of object-oriented concept in order to comply with the requirements of C++ programming [6].

III. RESEARCH DETAILS AND OBJECTIVES

A. Project Details

- A system that simplifies farming for farmers. From soil analysis to fertilizer recommendation, this system reduces many hassles all at a single place.

- This system will assist individual farmers in obtaining soil health parameters of agricultural fields to recommend suitable crops and the dose of fertilizers for that particular crop.

B. Objective

The system will provide real-time soil analysis data for fertilizer recommendation and also it will assist farmers in better cultivation and fertilization of the crop.

C. Technical Stack:

- Database – Firebase
- Programming Language – Dart
- Framework - Flutter, Android Studio, and Java SDK

D. Methodology

- Collection of raw soil data (NPK) values via. Sensors.
- Storing it in our database/cloud.
- Processing the data for analysis of soil factors.
- NPK values and Fertilizer recommendation on the basis of processed data.
- Crop and fertilizer store recommendation.

E. Resources required

- NPK Sensor OUTPUT RS485
- Raspberry Pi Pico
- RS485 Auto Direction Module
- 12 V DC Adapter
- DC jack connector

F. Detailed Project Description

- T The proposed system performs real time soil analysis.
- It uses accurate automated sensors to determine NPK value along with other parameters.
- It then gives crop recommendations along with the fertilizer recommendation for the particular soil type.

G. Strength

- Higher accuracy
- Precise implementation of high accuracy algorithms
- Uses real-time data
- Affordable system
- flexibility via updates

H. Weakness

- Higher cost compared to other alternatives.

I. Opportunities

- Enhanced accuracy
- Reduced overall cost over time for both sensors and microcontroller
- Compact design
- One time investment

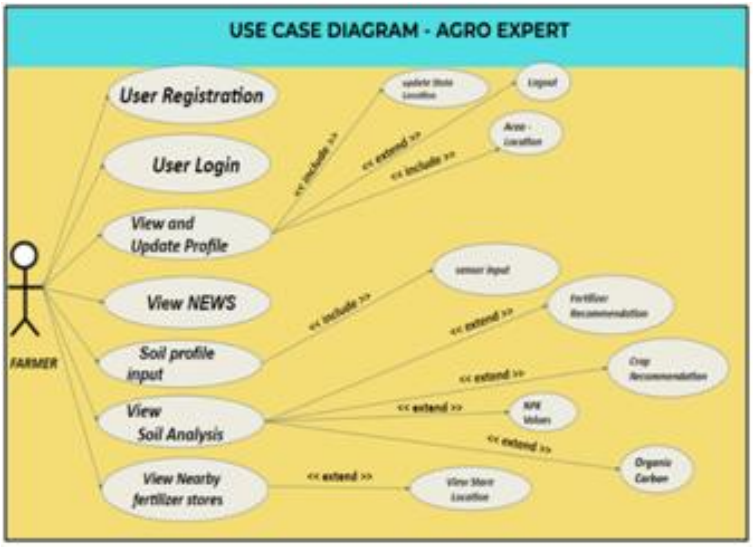
J. Threats

- Rise in price of the sensor due to lack of availability in the market

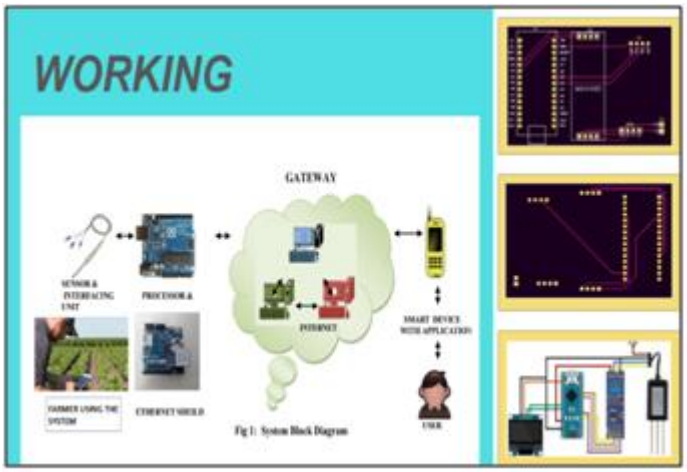
K. Market survey

IIT-Kanpur professor Jayant Singh, along with three students, has developed a mobile app named BhuParikshak to test nutrients like nitrogen, phosphorus, and more in the soil, alongside a low-cost and portable device.

L. Use Case Diagram



M. Block diagram (working)



IV. RESULT AND DISCUSSION

In this research we have considered real-time soil analysis data with the help of highly accurate automated sensors. We use this data to compare with our database and apply AI algorithms to perform the data analysis. This analysis after running through the algorithm will yield the recommendation for the particular soil type. This recommendation will include the suitable crop recommendation, fertilizer and it's required dosage for the soil on which analysis is performed.

Such type of system will assist and guide farmers to decide which crop to growth and which fertilizer to use for their respective field.It will also reduce the loses which farmers face due to issues like wrong fertilizer usage/ wrong crop chosen/ or incorrect dosage of fertilizers used.Such analysis is crucial part of planning before starting with the farming season.

To predict the crop yield, selected Machine Learning algorithms such as Support Vector Machine (SVM), Artificial Neural Network (ANN), Random Forest (RF), Multivariate Linear Regression (MLR), and K-Nearest Neighbour (KNN) are used [8].

V. CONCLUSION

After the detailed research, we propose a system that comes forward as a one stop solution for farmer's all day-to-day challenges. It performs real-time soil analysis. It uses accurate automated sensors to determine NPK value along with other parameters. It then gives crop recommendation along with the fertilizer recommendation for the particular soil type.

VI. ACKNOWLEDGEMENT

We are thankful to our research guide Dr. Varsha Sontakke, School of Computer Science, for consistence motivation, support and valuable guidance.

I am also obliged to our Associate Dean Dr. Shubhalaxmi Joshi for their valuable support and guidance

VII. REFERENCES

[1]. Varsha A. Shukr, Supriya S. Patil, "Comparative Study of Different Methodologies used for Measuring Soil Parameters: A Review",International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Published by, www.ijert.org, ICSITS - 2020 Conference Proceedings.

[2]. Liming Chen, Liming Xu, Yanlong Hou, "A Control System for the Mechanism of Fertilizer Proportioning and Mixing Based on the Nitrogen, Phosphate and Potassium Fertilizer", 978-1-4244-9577-1/11/$26.00 ©2011 IEEE.

[3]. HemaPallevada, Siva parvathiPotu, Teja Venkata Kumar Munnangi, Bharath ChandhraRayapudi, Sai Raghava Gadde, Mukesh Chinta, "Real-time Soil Nutrient detection and Analysis", 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) Department of Electrical & Electronics Engineering, Galgotias College of Engineering and Technology, Gr. Noida, India.

[4]. Izuddin Zainal Abidin1, Faizal Ahmad Fadzil, Yen Shin Peh, “Micro-controller Based Fertilizer Dispenser Control System”, 2018 IEEE Conference on Wireless Sensors (ICWiSe).

[5]. JenskieJerlin I. Haban, John Carlo V. Puno, Argel A. Bandala, Robert KerwinBillones, Elmer P. Dadios, Edwin Sybingco, “Soil Fertilizer Recommendation System using Fuzzy Logic”,2020 IEEE REGION 10 CONFERENCE (TENCON) Osaka, Japan, November 16-19, 2020.

[6]. M. Sindelar, "Soils Support Agriculture," 2015.

[7]. P. Heffer, “Assessment of fertilizer use by crop at the global level,” International Fertilizer Industry Association, Paris, 2009.

[8]. Shilpa Mangesh Pande, Prem Kumar Ramesh, Anmol Anmol, B. R Aishwarya, Karuna Rohilla, Kumar Shaurya, "Crop Recommender System Using Machine Learning Approach," 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), 2021, pp. 1066-1071, doi: 10.1109/ICCMC51019.2021.9418351.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Drug Recommendation Based on DDI Using Machine Learning

Akshay Bhorde, Mithilesh Dave, Devyani Kamble, Tanmay Borde
M.Sc. Department of Computer Science, MIT WPU, Pune, Maharashtra, India

ABSTRACT
As indicated by the World Health Organization, over 42% of drug mistakes are brought about by specialists since specialists compose the solution as per their very restricted encounters. With the headway of innovation and information science methods like information mining and recommender frameworks, it is possible to investigate possible information from analysis history records and assist specialists with endorsing drugs accurately. A suggestion of the right medication dependent on determination can target mending and diminishing experimentation when recommending drugs. This can additionally diminish unfortunate medication incidental effects. Thus, in this undertaking, we created a recommender framework that can give a clinical suggestion of a drug by diagnosing the patient by considering not just symptoms but his/her Medical history, ongoing medication and medicinal allergies or side effects as well. These axioms make our framework unique and novel when compared to other existing drug recommendation systems. It also makes the drug recommendation more accurate, precise and best suited for the patient.

Keywords— Drug-Drug Interaction, Machine Learning, Neural Network, DDI Dataset, Medicine Dataset

I. INTRODUCTION

Incorrect or partial diagnosis and Drug Prescription is the biggest and most unfortunate problem in the world today. According to WHO's 2019 report, annually there are 138 million deaths worldwide caused due to wrong drug prescription. 42% of the mistakes are made by specialists as their solution or recommendation is mainly composed of factors like: Existing encounters, knowledge, gathered data, diagnosis and Human Error. These axioms are limited and not always reliable. Consequently, the drug / medicine being recommended is not always best suited and sometimes can be fatal. We are in 2022 where technologies like AI / ML can outperform human intelligence in terms of data crunching and computation. Therefore, there is a dire need of a recommender framework of AI / ML which can solve this problem and assist the doctors to improve the quality, accuracy and precision of medical practice and save lives of millions. Combination of Human experience and computed diagnosis is the ultimate solution and we are going to discuss this in the presentation.

State of the art ML models for drug recommendation are mostly based on sentiment analysis and reviews of the patients for the drug as ordinal data type. The problem with these models is that most of the time the accuracy is very low and the suitability of the recommended drug is subjective. The dataset used for these models doesn't consider the medical history of the patient which plays a very vital role while recommending any drug both by the automated systems like ML models or by human doctors or pharmacists. Due to false medicine recommendations, many people have lost their lives and some have suffered severe long term damage. Another drawback of the existing systems is not considering the ongoing medication of the patient. Many drugs are not supposed to be given to the patient if the patient is already on another specific medication, this may cause negative side effects and can even be fatal. Considering a layman example, suppose the existing model recommends the drug 'Zaroxolyn' to the patient, based on the current symptoms of kidney disorder. The model suggests this drug based on the current symptoms but if the patient is diabetic, then consuming this drug can cause side effects and in some cases can also be fatal. These are some of the reasons why considering the medical history and current medication of the patient is vital before recommending any drug. Consequently, there is a dire need for an accurate ML model which recommends the drug or medicine considering the following:

Medical History of the patient.

Existing medication of the patient.

Medicinal allergies or side effects.

Current symptoms of the patient.

II. EASE OF USE

A. GUI Based Application

Since The Software has user engagement for diagnosis, it is designed to be a user friendly GUI which is suitable for a wide range of compatible devices like kiosk, computer, Mobile phone etc.

B. Cloud Computing

Machine Learning and other computations can be executed on the cloud using open APIs. This will ensure cross platform support.

C. Abbreviations and Acronyms

DDI: Drug-Drug Interaction.

ML: Machine Learning.

NDD: Neural Network based DDI Prediction.

D. Requirements

The ML model can be deployed on any compatible computing device or the cloud as well. An input device is required for registering the inputs from the end-users. An output device is required for delivering the output results to the end-user.

The system comprises multiple datasets and respective ML models to accomplish the inferences in sequence, leading up to the desired results at the end. The system initially performs some diagnoses by asking basic questions. This helps the system to split and narrow down the data which is as user-specific as possible. This may include splitting the data based on gender, age group etc. These parameters can be variable.

Symptoms Dataset: Next, the system takes the symptoms as input and registers them in the user's dataset. Now the ML model of this dataset comes into the picture which tries to predict the ailment. The system then splits down the similar features ailments and asks counter questions to validate and filter down the exact symptoms to one or more ailments. Once the ailment is confirmed, the system proceeds further.

Drugs Dataset: This ML model takes the confirmed ailment as input and searches for the best suitable drugs or medicines for the concerned ailment and filters down along with alternative or similar drugs. It then checks for the side effects and forbidden drugs of the selected drug and asks counter questions to the end-user to ensure that the selected drug is not forbidden for the end-user and does not clash with his/her existing medication. For this, the drugs dataset helps to backtrack and trace the side effects and list of forbidden drugs to frame counter questions and register any existing illness or ailment or ongoing medication of the end-user. If the selected drug is clashing or is forbidden for the end-user due to medical history or current medication, then the system searches for an alternative drug that is not forbidden and has properties least or not at all affected for the user. Once the best suitable drug is traced, then the system proceeds further.

DDI dataset: This dataset is not easily available. It contains the information of drugs that are reactive towards other drugs. And this dataset is specifically designed to support pharmaceutical scientists. Using this dataset in our recommendation system is very important. DDI is a drug-drug interaction dataset.

If a patient is under some medication or drug, say X, this X drug will be compared with the drug Y recommended by the forbidden drug search algorithm and check for side effects and if found it will further recommend an alternative non-reactive drug Z for the same.

III. COMPARISON TO SIMILAR FRAMEWORKS

Sentiment analysis and surveys of the patients for the medication as ordinal information type is used to recommend the drug. The issue with these models is that more often than not the precision is exceptionally low and the appropriateness of the suggested drug is abstracted. But taking into consideration, if the patient is already under medication we need to consider his/her medical history. Many medications are not expected to be given to the patient if the patient is now on another particular drug, this might cause negative incidental effects and can even be deadly.

Drug Recommendation Based on Medical History of Patients and Sentiment is a perfect blend and can generate more accurate results that will be more reliable and effective, and at the same time unobjectionable. But for this, we require new datasets that will help us to conclude which drugs are interactive and are harmful together. Here we need Drug-Drug Interaction (DDI) prediction. NDD uses the neural organization model alongside likeness determination and combination strategies to exploit nonlinear examination and expert component extraction to further develop the DDI forecast exactness. NDD is a multi-step pipeline. In the initial step, it gets data of different medication likenesses (substance, target-based, Gene Ontology (GO), incidental effect, off-mark incidental effect, pathway, Anatomical Therapeutic Chemical (ATC), ligand, carrier, sign, and Gaussian Interaction Profile (GIP) similitudes) and their communication information from various datasets. Then, at that point, it chooses the most useful and less repetitive subset of closeness types by a heuristic interaction proposed by Olayan et al.25. In the following stage, the choice comparability types are coordinated by a non-straight similitude combination technique called SNF26. At long last, the incorporated likeness framework, notwithstanding the communication information, is utilized for preparing the neural organization.

NDD can give a precise system for foreseeing new DDIs. NDD uses past strategies in closeness determination and similitude combination, however, the design of the neural organization is novel and exceptionally tuned for this issue.

And another dataset wherein to keep the records of the medical history of the patient. This new dataset will consist of 2 major fields: disease and medication/drugs. And a comparison of the drugs that are being consumed by the patient and the drug prescribed by the sentimental drug recommendation can be compared with the drugs in the DDI dataset. Henceforth, predicting the drug that will be best suitable to the patient keeping in mind the medical history of the patient.

The given data set contains the information about medicine, its expiry date, reviews, ratings and conditions in which they found out. This data set helps in predicting how much users found the medicine useful. Here we tried to figure out how many medicines have ratings and how many medicine users found out useful. We can furthermore study each rated medicine.

IV. FUTURE ENHANCEMENTS

We can further make it simpler by adding AI natural language processing to respond to the input given by the patient using voice commands and further process the data by collecting the terms that match the sentimental, medical history of the patient and Drug-Drug Interaction dataset to recommend the drug to the patient. Henceforth, avoiding human errors and considering more data and processing on the same to avoid any further mistakes in drug recommendation.

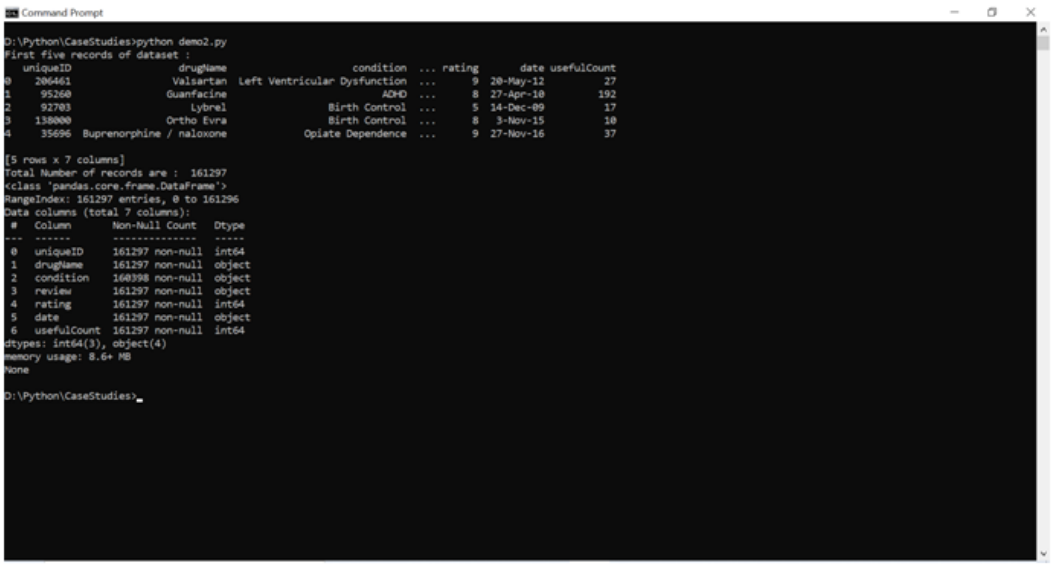
V. LIMITATIONS

The dataset for drug to drug interactions is not directly available in the public domain.

Users should be aware of their medication, inaccurate diagnosis can lead to fatal medicine recommendations.

VI. ACKNOWLEDGMENT

This research project would not have been possible without the help of our guide Ms. Devyani Kamle. We thank her for the support, guidance and knowledge. We also extend our gratitude towards the managing committee of MIT WPU who gave us this opportunity to complete this paper.


Command Prompt
D:\Python\CaseStudies>python demo2.py
First five records of dataset :
uniqueID drugName condition ... rating date usefulCount
0 206461 Valsartan Left Ventricular Dysfunction ... 9 20-May-12 27
1 95260 Guanfacine ADHD ... 8 27-Apr-10 192
2 92703 Lybrel Birth Control ... 5 14-Dec-09 17
3 138000 Ortho Evra Birth Control ... 8 3-Nov-15 10
4 35696 Buprenorphine / naloxone Opiate Dependence ... 9 27-Nov-16 37
[5 rows x 7 columns]
Total Number of records are : 161297
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 161297 entries, 0 to 161296
Data columns (total 7 columns):
Column Non-Null Count Dtype
0 uniqueID 161297 non-null int64
1 drugName 161297 non-null object
2 condition 160398 non-null object
3 review 161297 non-null object
4 rating 161297 non-null int64
5 date 161297 non-null object
6 usefulCount 161297 non-null int64
dtypes: int64(3), object(4)
memory usage: 8.6+ MB
None
D:\Python\CaseStudies>

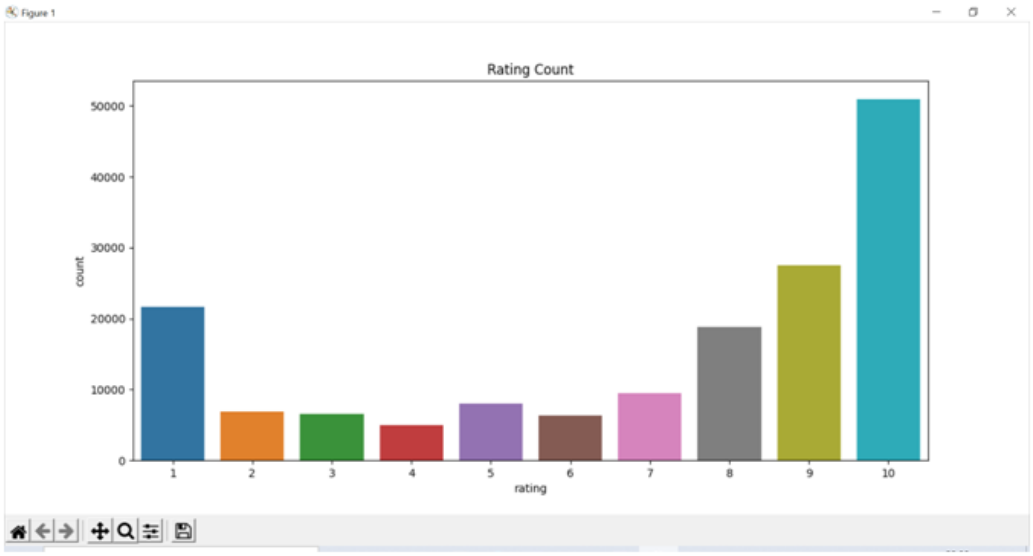


Figure 1
Rating Count
count
rating
0
10000
20000
30000
40000
50000
1
2
3
4
5
6
7
8
9
10

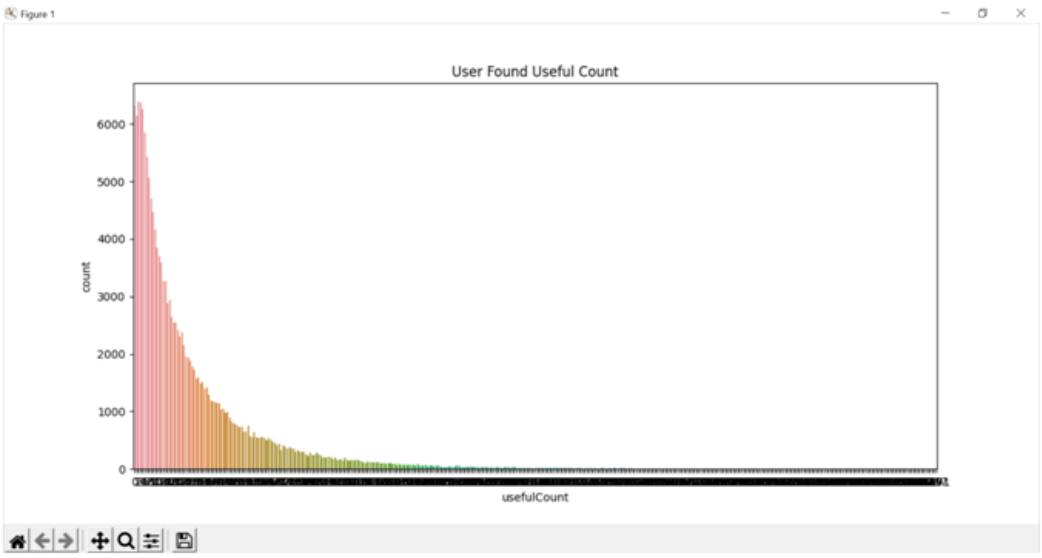
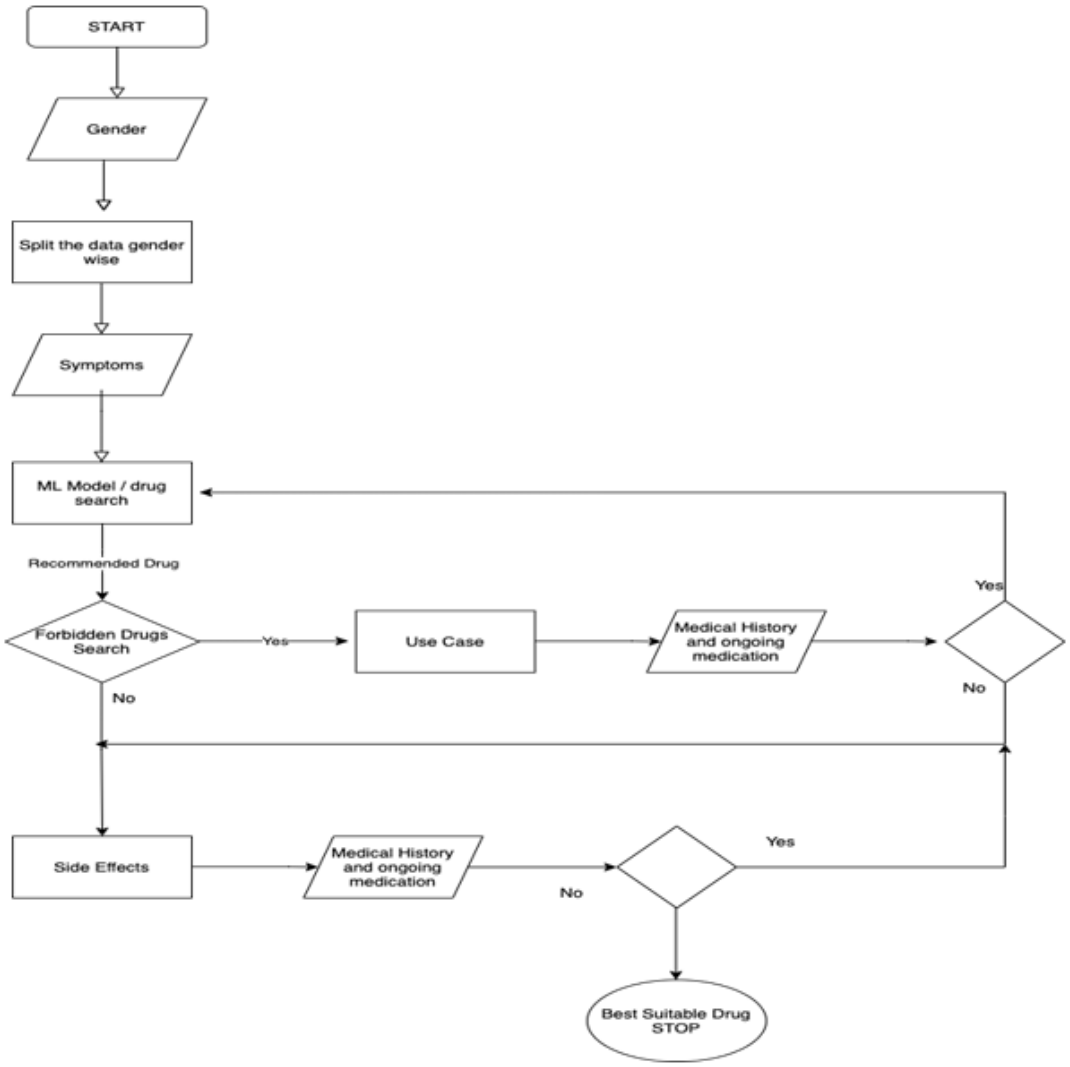


Figure 1
User Found Useful Count
count
usefulCount
0
1000
2000
3000
4000
5000
6000



VII. REFERENCES

[1]. S. Garg, "Drug Recommendation System based on Sentiment Analysis of Drug Reviews using Machine Learning," 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2021, pp. 175-181, doi: 10.1109/Confluence51648.2021.9377188.

[2]. Napa, Komal Kumar & Vigneswari, D.. (2020). A Drug Recommendation System for Multi-disease in Health Care Using Machine Learning. 10.1007/978-981-15-5341-7_1.

[3]. Stark, Benjamin, Constanze Knahl, Mert Aydin and Karim O. Elish. "A Literature Review on Medicine Recommender Systems." International Journal of Advanced Computer Science and Applications (2019): n. pag.

[4]. Tran, Thi Ngoc Trang, Alexander Felfernig and Nava Tintarev. "Humanized Recommender Systems: State-of-the-art and Research Issues." ACM Transactions on Interactive Intelligent Systems (TiiS) 11 (2021): 1 - 41.

[5]. Joshi, Shreehar and Eman Abdelfattah. "Multi-Class Text Classification Using Machine Learning Models for Online Drug Reviews." 2021 IEEE World AI IoT Congress (AIIoT) (2021): 0262-0267.

[6]. Banerjee, Madhurima. "RECOMMENDER SYSTEM – AN OVERVIEW." International Journal of Advanced Research in Computer Science 10 (2019): 21-23.

[7]. Rohani, N., Eslahchi, C. Drug-Drug Interaction Predicting by Neural Network Using Integrated Similarity. Sci Rep 9, 13645 (2019). https://doi.org/10.1038/s41598-019-50121-3

[8]. Zhang, Q., Guangquan Zhang, Jie Lu and Dianshuang Wu. "A Framework of Hybrid Recommender System for Personalized Clinical Prescription." 2015 10th International Conference on Intelligent Systems and Knowledge Engineering (ISKE) (2015): 189-195.

[9]. Bao, Youjun and Xiaohong Jiang. "An intelligent medicine recommender system framework." 2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA) (2016): 1383-1388.

[10]. Lafta, Raid, Ji Zhang, Xiaohui Tao, Yan Li and Vincent S. Tseng. "An Intelligent Recommender System Based on Short-Term Risk Prediction for Heart Disease Patients." 2015 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT) 3 (2015): 102-105.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Polarized Opinion Maker using Machine Learning

Aayushi Joshua, Tanmay Borde, Harshita Kansara, Devyani Kamble, Rajshree Patela
M.Sc., Department of Computer Science), MIT WPU, Pune, Maharashtra, India

ABSTRACT

Today's world is full of opinions due to freedom of speech but manipulating a fact or creating a bubble of favored facts to falsify opinions is contradictory to the rights itself of Democracy and Freedom of Speech. With the rise in usage and adoption of social media, the concern for people becoming adamant is ever increasing due to the algorithms of the social media platforms like Facebook, Instagram, etc. These platforms have humongous data and user engagement which now has the power to stir public sentiments, form inclined and biased opinions which result in chaotic and unsettling social situations in the world. These social media platforms use algorithms that typically create a bubble of favored feeds around the user depending on their Likes - Dislikes, interests, and inclinations. This results in users becoming vulnerable to targeted or biased ads and fake news. Therefore, the user never gets exposed to the counter view of the subject and s/he becomes adamant about their opinions which creates a lack of critical and rational thinking in public. This is the reason we can see riots, clashes, conflicts, and intolerance about any subject, and this will get worse with time, so there is a dire need to solve this problem.

This problem can be solved using Machine Learning where the user can enter the topic or subject s/he wants to explore. Then using sentiment analysis, we can determine the polarity of the news and classify the news in view and counter view columns (along with the link to the news article), according to the degree of polarity. This will help users to know both sides of the subject/topic and form a well thought and rational opinion.

Keywords— Web scraping, OpenAPI Tools, Natural Language Processing, Sentiment Analysis, Machine Learning.

I. INTRODUCTION

Technology is connecting and bringing people together like never before. It all started with enabling people across the globe to communicate with each other, but we have come a long way since then. Today people don't just communicate, but share or impose opinions, make propagandas, stir public sentiments, trolling people etc. Basically the virtual world of interconnectivity today, has become a powerful and vulnerable platform. On one hand, people can successfully do crowdfunding for a charity with the help of social media, and on the other hand, people can spread hate speech, fake news and cause distress in the society. The worst part is that this

fragile platform is being misused by powerful people, extremists, political parties and propagandists. People must know both sides of the coin, only then they can make rational opinions and make better decisions.

Today, Google is the de facto standard to search for some information. But this search engine is nothing but a Page Ranking Algorithm which just shows what's trending and not what is true. Media Manipulation is a growing concern and there is no such existing platform which helps in making rational decisions. We, being the students of computer science, feel that this is our prime responsibility to try and solve this problem.

Proposed Solution:

To solve this problem, we are going to make use of Machine Learning. Our project 'Unbiased Opinion Maker' is about providing information related to the keyword such as a unique personality that the user is going to provide. This project is basically going to use web scraping to get the related information from the top headlines from a reliable news source and then through sentiment analysis, opinion is going to be formed. The resultant opinion can be either positive, negative and neutral. This will be presented to the user and after seeing all the facts, an unbiased and true opinion can be formed. Currently, there is no such system that provides all the information about a particular subject/topic in one place. Existing systems have following issues:

1. Information can be biased or it can be affected by the mood of the person who uploaded it.
2. There can be a limitation in information (that means that only partial truth is being presented).
3. Information that is being presented is not from a reliable source (that is the information can be completely wrong).
4. Propagandist articles and hate speech.

As there is no such system that provides all the true information about a subject etc. at one place, it is crucial to create such a system. As this is the era of technology and the internet, many out there are using this opportunity to create chaos or to put wrong information in the media to create false opinions about particular things. Also, in order to give the opportunity to the user to create their own opinion after seeing all the facts about something, this project is being created.

A. Comparison to Similar Frameworks:

Summary of Existing Research Papers and systems is mentioned below:

[1] News can be good or bad, but it is seldom neutral. Although full comprehension of natural language text remains well beyond the power of machines, the statistical analysis of relatively simple sentiment cues can provide a surprisingly meaningful sense of how the latest news impacts important entities.

In this paper, we report on our development of a large-scale sentiment analysis system for news and blog entities built on top of the Lydia text analysis system .

Our sentiment index relies critically on tracking the reference frequencies of adjectives with positive and negative connotations. We present a method for expanding small candidate seed lists of positive and negative words into full sentiment lexicons using path-based analysis of synonym and antonym sets in WordNet. We use sentiment-alternation hop counts to determine the polarity strength of the candidate terms and eliminate the ambiguous terms. We present the detailed algorithm and performance results.

- Sentiment Index Formulation – There is considerable subtlety in constructing a statistical index which meaningfully reflects the significance of sentiment term juxtaposition.

[2] The approach taken in uses machine translation technology to develop a high precision sentiment analysis system for Japanese at a low cost. Sentiment unit polarity extraction precision of 89% is reported. propose a method of determining sentiment orientation of Chinese words using a bilingual lexicon and achieve precision and recall of 92%. argue that adverbs in combination with adjectives are more helpful for sentiment score assignment to individual sentiment units than adjectives alone.

B. The Lydia sentiment analysis system:

The Lydia system recognizes named entities in text and extracts their temporal and spatial distribution. As a preliminary step, the sentiment lexicon is constructed. Starting from sets of seed positive and negative adjectives, their polarity is propagated through WordNet synonym and antonym links, and every adjective is assigned a polarity score. Then, the top fraction of adjectives from both extremes of this curve are placed into positive and negative parts of the sentiment lexicon respectively.

The next step is entity sentiment calculation in a specific corpus. Using the existing sentiment lexicon, positive and negative word occurrences are marked up in the corpus. For every entity and every day i, the number of positive and negative sentiment words co-occurring with that entity in the same sentence are calculated. For every entity, its polarity score on a given day is then calculated as entity polarity.

II. METHODOLOGY

This section defines the procedure and order of execution of the proposed system. The execution is broken down into following steps:

- Live News Fetching: This step involves fetching news headlines using HTTP REST API based searching and retrieving.
- To avoid ambiguity and interrogation, headlines with typographical symbols will be discarded.
- The data fetched from the sources can be sorted in following orders:
- Relevance to the searched keyword.
- Popularity of the source.
- Date of the published news.
- The authentication is handled with an API key of NewsAPI.

The result generated from the searched keyword will consist of the authentic source of the news, author, title, description, url of the complete article, url of a related image, date and time of publish, and content of the news. Here we tried fetching the necessary components such as title of the article or we can say headline for further process. Here is an example : The output obtained by using the keyword “Barack Obama” :-

The idea behind taking headlines from some reliable news sources using the NewsAPI is to perform sentiment analysis on it. Using the API we extracted the headlines and using some basic python operations we generated a list of headlines i.e. title from each news which was extracted is placed inside a single list for NLP.

Natural Language Processing: This step involves tokenizing the headline, punctuation removal, stop word removal, pronoun ambiguity etc.

In natural language processing, human language is separated into fragments so that the grammatical structure of sentences and the meaning of words can be analyzed and understood in context. This helps computers read and understand spoken or written text in the same way as humans.

Here are a few fundamental NLP pre-processing tasks data scientists need to perform before NLP tools can make sense of human language:

Tokenization: breaks down text into smaller semantic units or single clauses

Part-of-speech-tagging: marking up words as nouns, verbs, adjectives, adverbs, pronouns, etc

Stemming and lemmatization: standardizing words by reducing them to their root forms

Stop word removal: filtering out common words that add little or no unique information, for example, prepositions and articles (at, to, a, the).

Only then can NLP tools transform text into something a machine can understand.

There are two main algorithms you can use to solve NLP problems:

A rule-based approach. Rule-based systems rely on hand-crafted grammatical rules that need to be created by experts in linguistics, or knowledge engineers. This was the earliest approach to crafting NLP algorithms, and it's still used today.

Machine learning algorithms. Machine learning models, on the other hand, are based on statistical methods and learn to perform tasks after being fed examples (training data).

The biggest advantage of machine learning algorithms is their ability to learn on their own. You don't need to define manual rules – instead machines learn from previous data to make predictions on their own, allowing for more flexibility. Here is the output of our NLP code.

Sentiment Analysis: The processed headlines are then analyzed. A headline is split into words, and analysis will be done on those words and an overall result will be generated showing that the headline is positive, negative or neutral.

Several NLP activities break human text and voice data in ways that help a computer make sense of what it is importing. Some of these activities include the following:

Speech recognition, also called speech-to-text, is the function of faithfully converting voice data into text data. Speech recognition is required for any app that follows voice commands or answers spoken questions. What makes speech recognition particularly challenging is how people speak — quickly, consistently, with emphasis and modulation, in a variety of pronunciations, and often using the wrong grammar.

The marking part of a speech, also called the marking of a language, is the process of determining the part of speech of a particular word or piece of text based on its use and context. Part of the expression refers to 'doing' as the verb 'I can make a paper airplane,' and as the noun 'What makes the car you own?'

Separating the meaning of a word is the choice of the meaning of a word that has multiple meanings through a semantic analysis process that determines a word that gives greater meaning to a given context. For example, separating the meaning of a word helps to separate the meaning of the verb 'do' from 'make distance' (gain) vs. 'make a bet' (place).

Named business recognition, or NEM, identifies names or phrases as useful businesses. NEM identifies 'Kentucky' as a locality or 'Fred' as a man's name.

The reference solution is a function of identifying whether and when two words refer to the same thing. The most common example of identifying a person or thing to whom a pronoun refers (eg, 'she' = 'Mary'), but may

also involve pointing to a metaphor or expression in a text (e.g., an event where 'bear' is not an animal but a furry adult).
Emotional analysis attempts to exclude thoughtful traits — attitudes, feelings, sarcasm, confusion, suspicion — from the text.
The production of natural language is sometimes described as contrary to the recognition of speech or spoken speech; it is the work of introducing formal information into human language.

III. RESULTS AND DISCUSSIONS

Currently the project is in the development phase and the progress made so far is mentioned below:
Proof of Concept: News Headline fetching using an open API tool is accomplished successfully and we are testing it. We are able to fetch the news headlines based on different parameters and do abstraction of the fetched response. The request parameters are passed along with the API Key and the response is returned in JSON format. Abstraction and further processing is done on the response. The News API is a simple JSON-based REST API for searching and downloading news across the web. By using this, one can download top stories that run on a news website or search for top stories on a particular topic (or keyword).
Stories can be retrieved based on some circumstances. It says the title (keyword) to be searched is 'Geeksforgeeks' or it may be concerned about a particular channel. Everything can be done, but an API key is needed to get started.
Ideation: The NLP and Sentiment analysis part of the proposed system is still in the ideation phase. We are in the cycle of research and testing NLP for our use case. Since the accuracy of the Sentiment Analysis model has direct consequences on the output, we are testing different Models and trying to find the fine tuned Sentiment Analysis model for this application.

IV. FUTURE ENHANCEMENTS

The project has a wide scope for future enhancements including:-
Fact Check: We can add a fact checking feature in the pipeline. This will double check that the news fetched from the web or manually requested by the user is legit and not a fake news.
Summarisation: Currently, the scope of the project is limited to only news headlines and not news summary. For future enhancements, we can add this feature to extend the scope.
Categorized Opinion Making: If a user wants to know the two sided opinions of the public, s/he can search for polarized opinions based on categories of the subject / topic.
Opinion Making about Political Leader/Party: A dedicated polarized political news showing category feature.
Enable Public API: Enabling a public API of our application for other platforms to use.
Including more languages: adding support for different languages.

V. LIMITATIONS

The news fetching depends on the source of news. The source of news needs to be unbiased.

VI. ACKNOWLEDGMENT

This research project would not have been possible without the help of our guide Ms. Devyani Kamle. We thank her for the support, guidance and knowledge. We also extend our gratitude towards the managing committee of MIT WPU who gave us this opportunity to complete this paper.

VII. REFERENCES

[1]. Godbole, Namrata &Srinivasaiah, Manjunath &Skiena, Steven. (2007). Large-Scale Sentiment Analysis for News and Blogs. ICWSM 2007 - International Conference on Weblogs and Social Media.

[2]. Bautin, Mikhail &Vijayarenu, Lohit&Skiena, Steven. (2008). International Sentiment Analysis for News and Blogs.. ICWSM 2008 - Proceedings of the 2nd International Conference on Weblogs and Social Media.

[3]. Chaima Messaoudi, ZahiaGuessoum, Lotfi Ben Romdhane. (2022) Opinion mining in online social media: a survey. Social Network Analysis and Mining 12:1.Online publication date: 11-Jan-2022.

[4]. Chaudhary, Jashubhai& Paulose, Joy. (2019). Opinion mining on newspaper headlines using SVM and NLP. International Journal of Electrical and Computer Engineering. 9. 2152. 10.11591/ijece.v9i3.pp2152-2163.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Person Identification Based on offline Signature Using Deep learning

Krishna K. Shinde[1], Sumegh S. Tharewal[2], Dr. Charansing N. Kayte[3]
[1]Department of Computer Science & IT, Dr. B. A. M. University Aurangabad, Maharashtra, India
[2]School of Computer Science, Dr, V.K. MIT World Peace University Pune, Maharashtra, India
[3]Department of Digital & Cyber Forensic, (Government Institute of Forensic Science), Dr. B. A. M. University Aurangabad, Maharashtra, India

ABSTRACT
A signature is one kind of written artwork that a person signs as a form of identification on any document. It's typically used to sign a check, a legal document, or a contract, among other things. In recent decades, handwritten signature verification has gained a lot of attention, but it's still a work in progress. The goal of signature identification systems is to determine if a particular signature can be used to identify a person. In this paper we have used two pre-processing techniques first crop and normalization these techniques have cropped the unwanted portion of the offline KVKR signature dataset and normalized its dimension, second is canny edge detection for noise- reduction in the image and identifying edges. The features extraction and matching using the Modified CNN model have automatically extracted features and RMSprop optimizer used for classification these features. This study performed experimental work of each VGG16, VGG19 and ResNet50 model and tested these three models with different dataset sizes of input train, test and validation data. The VGG16 and VGG19 models got a better recognition accuracy than REsNet50 models.

Keywords—VGG16, VGG19, ResNet50, Canny Edge Detection

I. INTRODUCTION

Biometrics is a fast-growing technology that is used in a wide range of governmental and commercial identification applications. A biometric approach is a pattern recognition system that determines the authority of certain physiological or behavioural attributes to make a personal identification [1]. Biometric authentication is the process of authenticating an individual's identity based on their unique biological characteristics. It's become the accepted method of gaining access to high-security systems. Using modern machine learning and statistics methodologies, many of these operations can now be successfully automated (face, fingerprint, iris etc. recognition). Signature verification is one of several biometric authentication jobs that try to figure out if a particular signature can be used to identify a person [2]. A signature is a one-of-a- kind written artwork that a

person signs as a form of identification on any document. It's typically used to sign a check, a legal document, or a contract, among other things. A difficulty arises when someone attempts to imitate it. Any person's signature has an image with a specific pixel pattern that irks them [3]. A handwritten signature is often considered a form of legitimacy in legislative, legal, and commercial transactions. Offline Signature identification systems are used to confirm a person's identity by examining their signature [4]. They distinguish between "authentic" signature samples (produced by the claimed subject) and "forgery" signature samples (generated by someone else) (created by an impostor). Signatures are gathered once the signwriting activity is done by scanning a document containing the signature in offline signature verification. In contrast, in online signature verification, the signature is captured instantly on a device (pen tablet), and the signature's dynamic information, such as the velocity of the pen motions, is available [5]. Deep learning might be applied in biometrics to represent unique biometric data and improve the functionality of authentication and recognition systems. The goal of this paper was to evaluate recognition performance using pre-trained VGG16, VGG19, and ResNet-50 models with Modified CNN for extracting features and matching with RMSprop optimization technique and SoftMax classifier using CNN techniques for offline Signature verification and person identification.

II. LITERATURE SURVEY

The following Table I shows a comprehensive review starting from the author, Year of publication, database use, techniques/algorithm, and lastly the recognition result.

TABLE I. LITERATURE SURVEY

Author & Year	Database	Techniques	Result
Buddhika J. et. al. 2006 [6]	Offline 2000 sign Own Created	Fuzzy Logic & Genetic Algorithm	90%
I.A. Ismail et. al. 2008 [7]	840 sign Offline Own Created	PCA & KNN	FRR is 15%
Vu Nguyen et. al. 2009 [8]	DBexp	SVM & HMM	85%
Ramon B. G. et. al. 2012 [9]	Different Mobile Davies	DWT	EER 0.29
Ruangroj Sa-Ardship et. al. 2015 [10]	SigWiComp & PRIP	HOG & PHOG	99.27%
Srikanta Pal et. al. 2016 [11]	Bangla and Hindi	LBP & ULBP	66.94%
Abdilbaree T. N. et. al. 2017 [12]	CASIA	SIFT & SURF	96.25%
Aravinda C. V. et al. 2019 [13]	BD-605	KNN	81.50%
Shallow et. al. 2020 [14]	Kaggle dataset	CNN	84.00
Ruben Tolosana et.al. 2021 [15]	Publicly Available Database	TRNN, RNN, and DWT	2.0% EER

III. METHODOLOGY

In Fig 1 show the recommended structure of offline signature recognition for person identification. The Signature identification process is divided into two steps, first training steps we have loaded the KVKR signature dataset then pre- processing, the database of labelled Signature images and reduced to 224 by 224 pixels in the training stage and then utilized to train the one-by-one model using the recommended structure and stored each train model wights file. Second testing steps, During the testing stage, the trained model will be used to identify individuals in an offline signature identification system, after conducting the signature identification technique using the previously trained model in the testing stage, Resize the test signature image to fit the input model after loading it, the signature label with the lowest confidence score is eliminated, while the signature label with a confidence score higher than the threshold is accepted. This approach will reduce the model's incorrect classifications. As a result of the biometric authentication system, the signature label appears on the screen with a person ID.

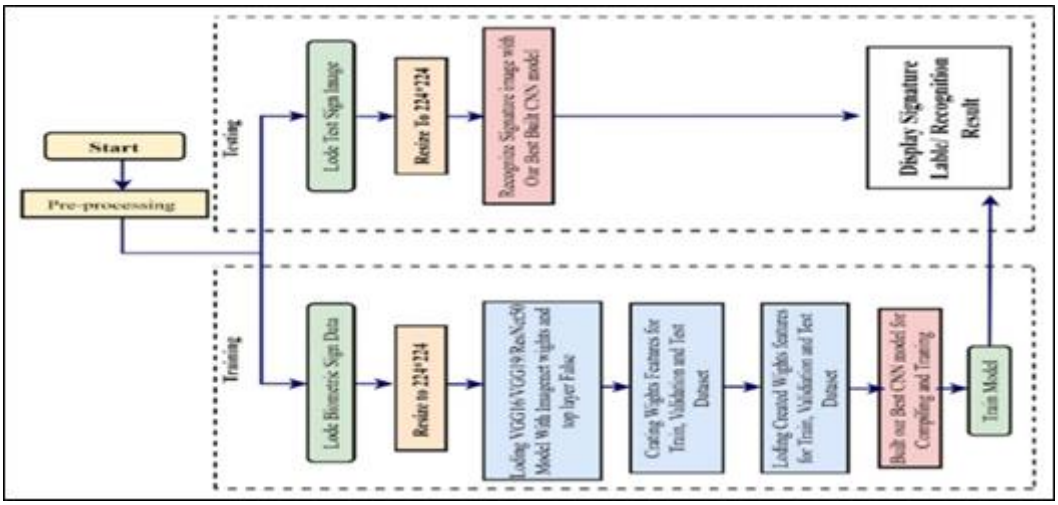


Fig 1 Proposed Methodology.

A. About Database

Under the supervision of Prof. Dr. K. V. Kale, Programme Coordinator, UGC SAP (II) and DRS Phase-I, the KVKR Multimodal Biometric Database includes uni-modal and multi- modal biometric databases collected in the Multimodal Biometrics Research Lab. at the Department of CS and IT, Dr. B. A. M. University. The signature database has been gathered offline. This database standard is gathering all data from Research Scholars, PG, and UG students in university and college departments between the ages of 21 and 40. On paper, each subject has 20 signatures. Then, using a Canon LiDE 110 sensor, data was captured in the form of colour pictures with an optical resolution of 2400x4800 dpi, images with a dimension of 250*370, and greyscale images with 48-bit input and 8-bit output. A total of 900 photos were collected from 45 people's signatures.

B. Pre-Processing

In the KVKR Signature dataset first, we have applied the cropping technique for cropping unwanted Parts of the images and after crop, images using the normalization technique for normalizing the dimension size of the images. second, we have to use Canny edge detection techniques on the KVKR signature dataset. This technique is a noise-reduction in the image and identifying edges. It extracts significant structural information from a variety

of visual objects, greatly lowering the amount of data to be processed. It's been used in a variety of computer vision applications. The criteria for employing edge detection in different vision systems, according to Canny, are rather similar [16]. In Fig 2 show that the crop & normalize and canny edge detection techniques pre-processing process.

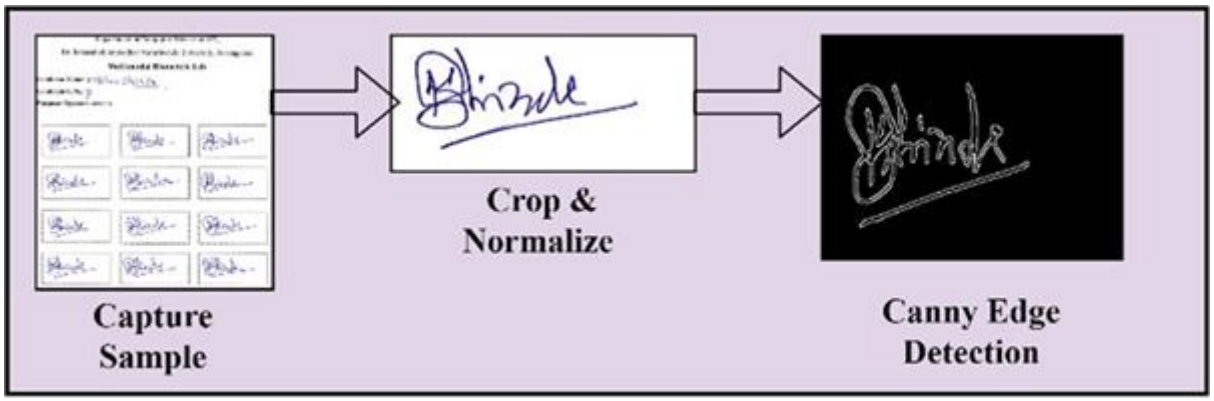


Fig 2 Pre-process Techniques

C. Features Extraction and Matching

The VGG16, VGG19 and ResNet50 Models and Modifying the Last few-layer using Modified CNN model use for features extraction.

1) Modified CNN

CNN is a deep learning model for analysing grid-patterned data, such as images and video, It is designed to learn spatial hierarchies of attributes and is inspired by the architecture of the animal visual cortex, patterns at all levels, from low to high, automatically and adaptively. Convolutional neural networks (CNNs) have three layers (or building blocks): convolution, pooling, and fully connected layers. Fig 1.3 show that the Modify last few layers of VGG16, VGG19 and ResNet50 models and using additionally modified CNN for training a model. calculating Signature recognition Accuracy including such measurement parameter model Training accuracy and Loss [17]. In Fig 3 show that the modified CNN model Summary.

```
Model: Built CNN Model For Compling and Traning
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
flatten_1 (Flatten)          (None, 25088)             0
_________________________________________________________________
dense_1 (Dense)              (None, 100)               2508900
_________________________________________________________________
dropout_1 (Dropout)          (None, 100)               0
_________________________________________________________________
dense_2 (Dense)              (None, 50)                5050
_________________________________________________________________
dropout_2 (Dropout)          (None, 50)                0
_________________________________________________________________
dense_3 (Dense)              (None, 45)                2295
=================================================================
Total params: 2,516,245
Trainable params: 2,516,245
Non-trainable params: 0
```

Fig 3 Modified CNN Summary

2) VGG16 and VGG19

The VGG deep CNN models were developed by the Visual Geometry Group at Oxford University. VGG16 and VGG19 are common models with 16 and 19 layers, respectively. The ImageNet database was used to train the VGG16 model extensively. This massive database has over 14 million photos separated into 20000 categories. There are five convolution blocks in the VGG16 model. Each convolution block has two convolutional layers (size: 3X3) and one max-pooling layer (size: 2X2). The prediction and classification tasks are handled by the Fully connected (FC) layers [18]. In Fig 4 and 5 show VGG16 & VGG19 model summary.

3) ResNet50

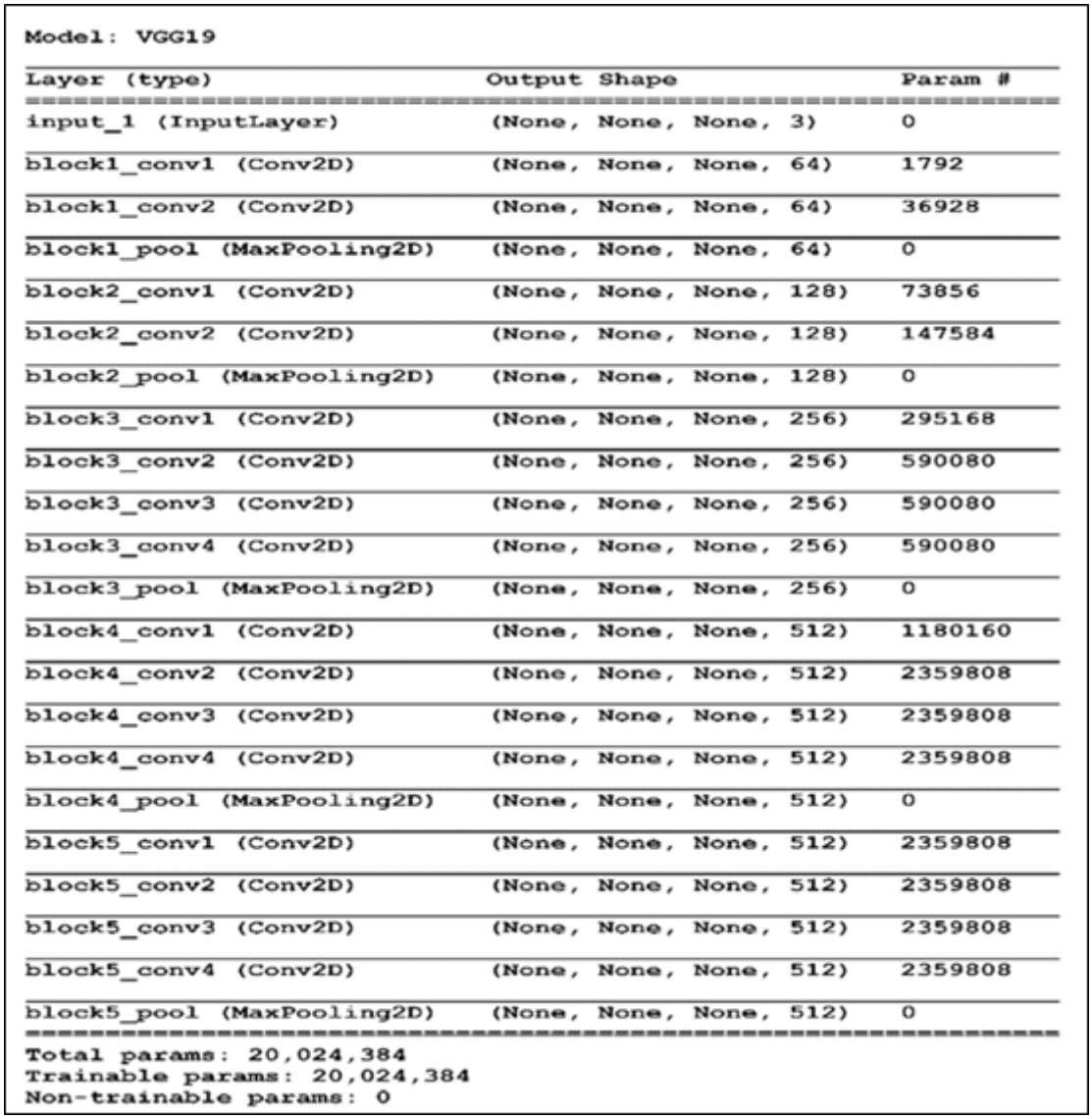
ResNet50 is an acronym for Residual Network, which refers to a network that facilitates Residual Learning. The number 50 represents how many levels there are. Resnet50 is a residual network with 50 layers. ResNet, or deep residual networks, was invented by Kaiming He et. al. [19]. Deep convolutional networks have made significant advances in image classification. The tendency is to advance deeper into the number of layers to execute complex jobs and enhance classification and identification accuracy. As we delve further into neural networks, however, the accuracy tends to saturate and finally decline. Residual training is a method of addressing this problem.

Model: VGG16

Layer (type)	Output Shape	Param #
input_1 (InputLayer)	(None, None, None, 3)	0
block1_conv1 (Conv2D)	(None, None, None, 64)	1792
block1_conv2 (Conv2D)	(None, None, None, 64)	36928
block1_pool (MaxPooling2D)	(None, None, None, 64)	0
block2_conv1 (Conv2D)	(None, None, None, 128)	73856
block2_conv2 (Conv2D)	(None, None, None, 128)	147584
block2_pool (MaxPooling2D)	(None, None, None, 128)	0
block3_conv1 (Conv2D)	(None, None, None, 256)	295168
block3_conv2 (Conv2D)	(None, None, None, 256)	590080
block3_conv3 (Conv2D)	(None, None, None, 256)	590080
block3_pool (MaxPooling2D)	(None, None, None, 256)	0
block4_conv1 (Conv2D)	(None, None, None, 512)	1180160
block4_conv2 (Conv2D)	(None, None, None, 512)	2359808
block4_conv3 (Conv2D)	(None, None, None, 512)	2359808
block4_pool (MaxPooling2D)	(None, None, None, 512)	0
block5_conv1 (Conv2D)	(None, None, None, 512)	2359808
block5_conv2 (Conv2D)	(None, None, None, 512)	2359808
block5_conv3 (Conv2D)	(None, None, None, 512)	2359808
block5_pool (MaxPooling2D)	(None, None, None, 512)	0

Total params: 14,714,688
Trainable params: 14,714,688
Non-trainable params: 0

Fig 4 VGG16 Model Summary



Model: VGG19

Layer (type)	Output Shape	Param #
input_1 (InputLayer)	(None, None, None, 3)	0
block1_conv1 (Conv2D)	(None, None, None, 64)	1792
block1_conv2 (Conv2D)	(None, None, None, 64)	36928
block1_pool (MaxPooling2D)	(None, None, None, 64)	0
block2_conv1 (Conv2D)	(None, None, None, 128)	73856
block2_conv2 (Conv2D)	(None, None, None, 128)	147584
block2_pool (MaxPooling2D)	(None, None, None, 128)	0
block3_conv1 (Conv2D)	(None, None, None, 256)	295168
block3_conv2 (Conv2D)	(None, None, None, 256)	590080
block3_conv3 (Conv2D)	(None, None, None, 256)	590080
block3_conv4 (Conv2D)	(None, None, None, 256)	590080
block3_pool (MaxPooling2D)	(None, None, None, 256)	0
block4_conv1 (Conv2D)	(None, None, None, 512)	1180160
block4_conv2 (Conv2D)	(None, None, None, 512)	2359808
block4_conv3 (Conv2D)	(None, None, None, 512)	2359808
block4_conv4 (Conv2D)	(None, None, None, 512)	2359808
block4_pool (MaxPooling2D)	(None, None, None, 512)	0
block5_conv1 (Conv2D)	(None, None, None, 512)	2359808
block5_conv2 (Conv2D)	(None, None, None, 512)	2359808
block5_conv3 (Conv2D)	(None, None, None, 512)	2359808
block5_conv4 (Conv2D)	(None, None, None, 512)	2359808
block5_pool (MaxPooling2D)	(None, None, None, 512)	0

Total params: 20,024,384
Trainable params: 20,024,384
Non-trainable params: 0

Fig 5 VGG19 Model Summary

IV. EXPERIMENTAL WORK

The suggested approach is implemented in Python 3.6, with the addition of the Keras, TensorFlow, and Pandas deep learning libraries, as well as the OpenCV, NumPy, Matplotlib, and sci- kit-learn libraries. The technique is run on a laptop with a Processor i5 CPU, NVidia 2GB graphics card, and 8Gb ram, while the training model is run on a Jupyter notebook IDE windows Platform and pre-processing of data use Spyder IDE. We have training first time 1200 images validation 300 and test 300, second time train 1200 images validation 600 and test 600, each model, set epochs is 19, batch size 64 and RMSprop optimizer. The VGG16, VGG19 and ResNet50 pre-train model with ImageNet wights and top layer false and additionally modify the last layer using modified CNN model and train one by one model.

V. RESULT AND DISCUSSION

The precision of the suggested model may be shown in Table II. VGG16, VGG19 and ResNet50 model. Table II show that each subject TR-train is 40, TE-test 10 and 20 and VA- Validation 10 and 20 images. the above mode used for signature recognition in this KVKR dataset comparing recognition rate than VGG16, VGG19 and REsNet50 Model get better recognition accuracy into VGG16 and VGG19.

A. Model Training Accuracy and loss

We have calculated VGG16, VGG19 and ResNet50 model training and validation accuracy and model training and Validation Loss. Figure 6 Show that the VGG16 Model Train Accuracy and Loss, Fig 7 show the VGG19 Model Accuracy and Loss and Fig 8 Show that the ResNet50 Model Accuracy and Loss. Table II show that in VGG16 Recognition we got a 99.99% accuracy and 0.01% Equal Error Rate and in VGG19 recognition we got 99.90% accuracy and 0.01% Equal Error Rate and ResNet50 we got a 99.78% accuracy and 0.22% equal error rate. Graph 1.1 show that in the comparative analysis VGG16, VGG19 and ResNet50 Modes for a Signature-based person identification system. We got in VGG16 and VGG19 model good recognition accuracy than ResNet50.

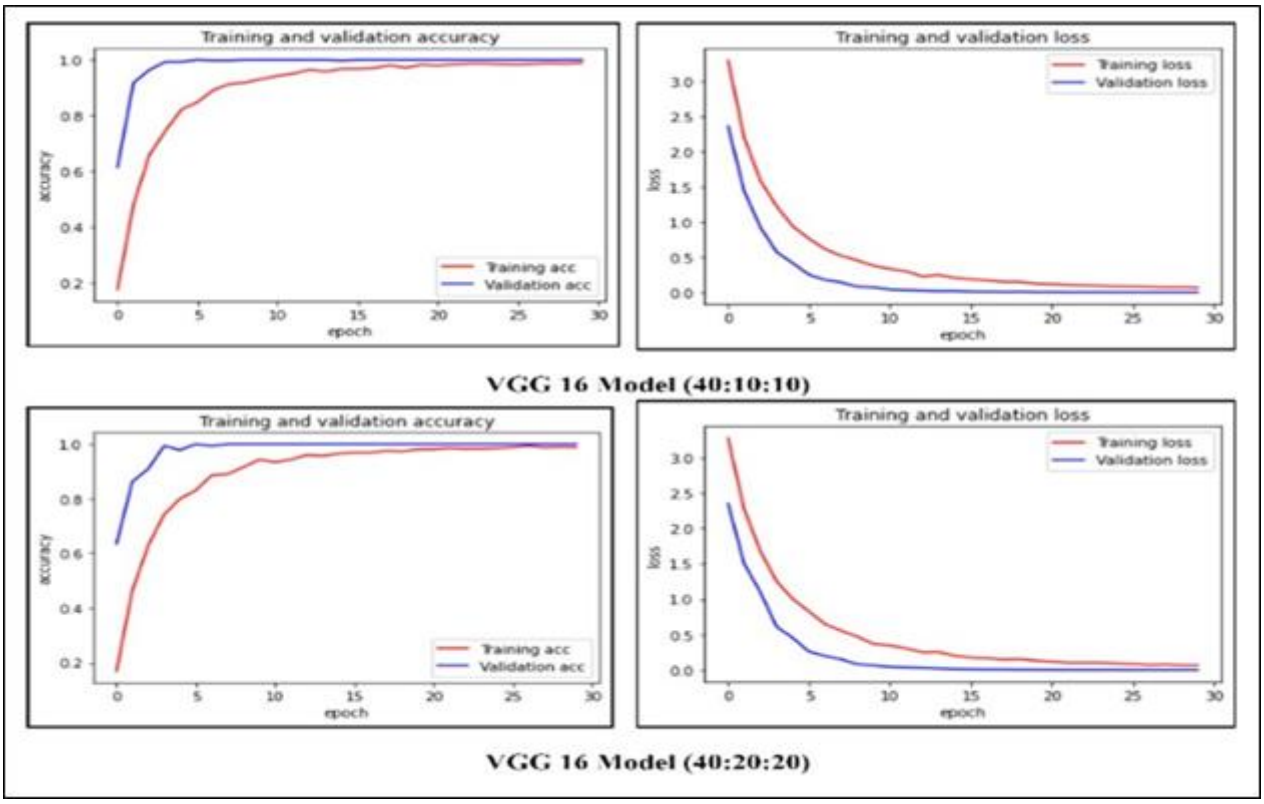


Fig 6 VGG16 Model Train Accuracy and Loss

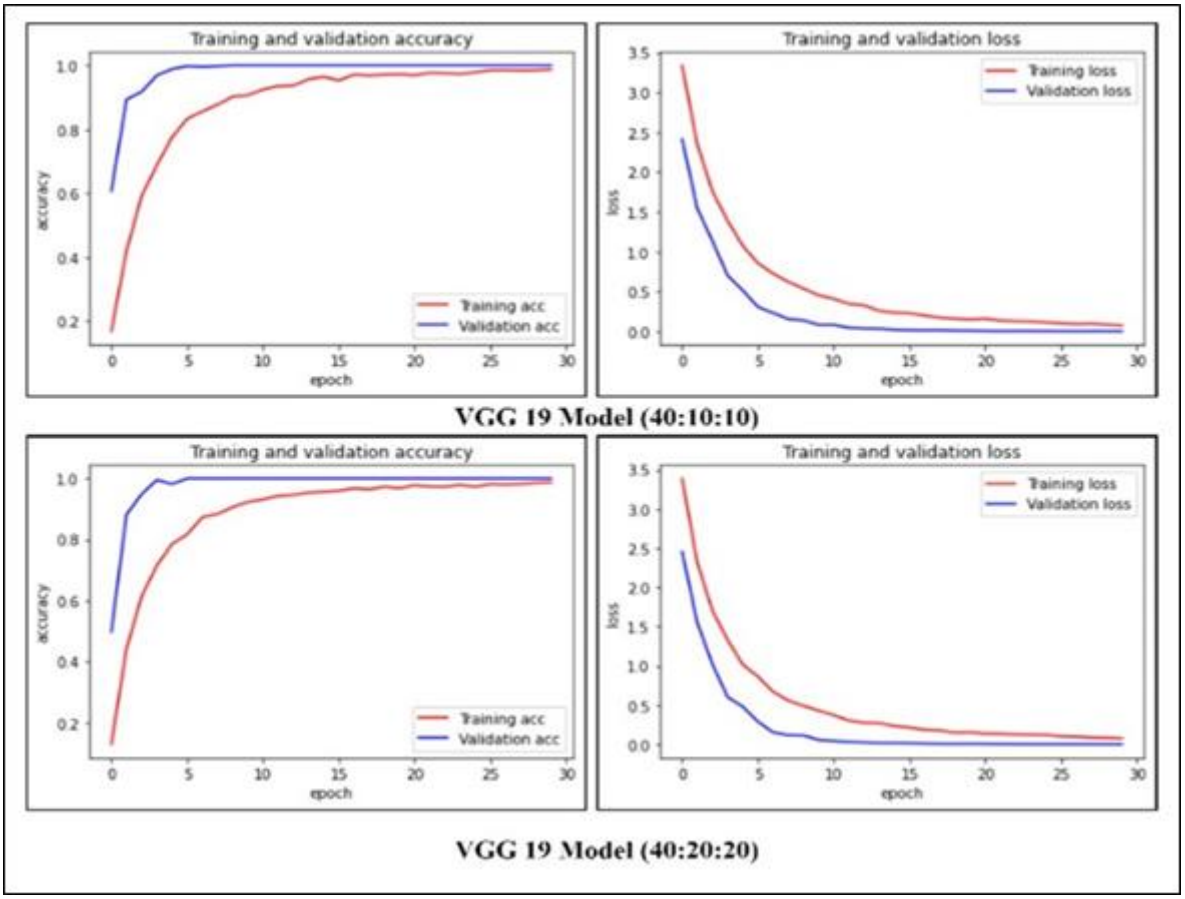


Fig 7 VGG19 Model Train Accuracy and loss

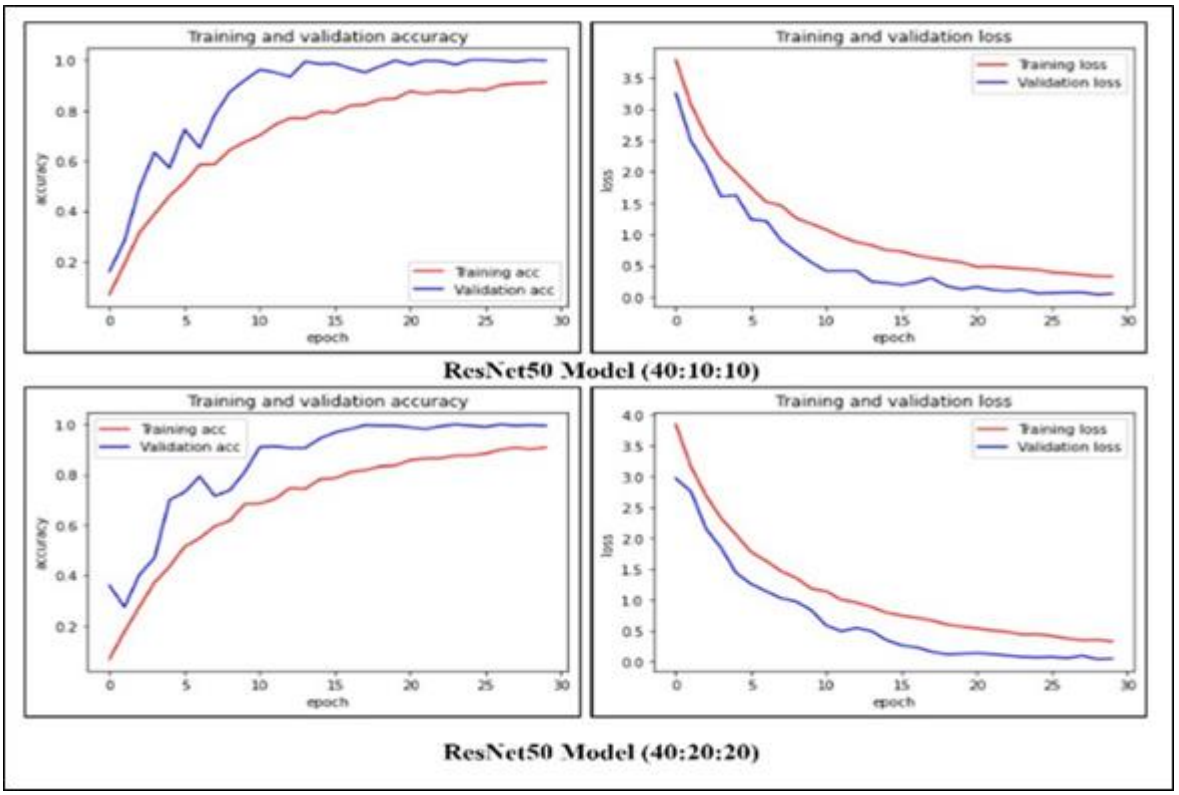
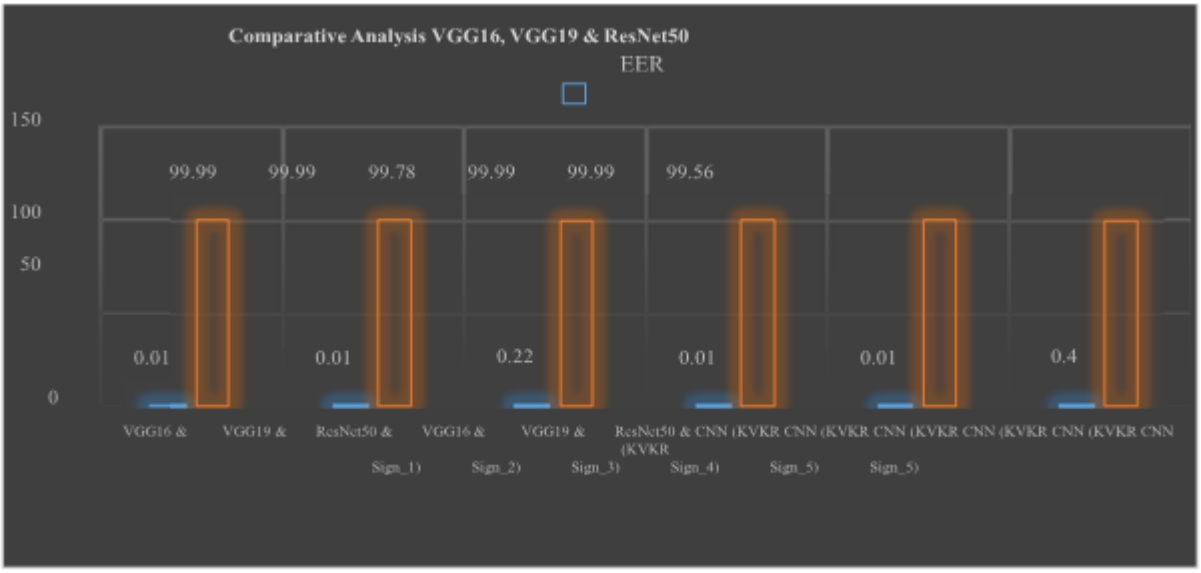


Fig 8 ResNet50 Model Train Accuracy and Loss

TABLE II. RECOGNITION ACCURAY

Data & Size TR:TE: VA	Mode l	Epoc h/Bat ch	EE R	Loss	Model Trainin g Time	Accura cy
KVKR_ Sign 40:10:10	VGG 16 & CNN	18/64	0.01	0.000525 2573261 128014	0:00:47. 768331	99.99%
KVKR_ Sign 40:10:10	VGG 19	18/64	0.01	0.000965 8672559 049187	0:00:48. 265934	99.99%
KVKR_ Sign 40:10:10	ResN et50	18/64	0.22	0.049755 7488746 1132	0:02:54. 714288	99.78%
KVKR_ Sign 40:20:20	VGG 16	18/64	0.01	0.000807 3804812 09192	0:00:49. 917570	99.99%
KVKR_ Sign 40:20:20	VGG 19	18/64	0.01	0.001144 0124727 475146	0:00:50. 301775	99.99%
KVKR_ Sign 40:20:20	ResN et50	18/64	0.40	0.049321 0985428 7571	0:03:01. 777605	99.56%



Graph 1.1 Comparative Analysis VGG16, VGG19 and ResNet50 models Recognition Accuracy

VI. FUTURE WORK

In the future capture more subjects offline as well as online signature databases and test other possible pre-train models in deep learning as well as other pre-processing techniques.

VII. CONCLUSION

In this paper, we apply modified CNN models to the Signature recognition system for a personal identification based deep learning approach. we have used the Root Mean Square Propagation (RMSprop) optimizer to train the model for 18 epochs and 64 batch sizes, then we ran six experiments on the offline KVKR signature dataset. First, we used pre-processing techniques to crop and normalise and canny edge detection techniques on the KVKR signature dataset. Then we have to train one by one VGG16, VGG19 and ResNet50 modes with pre- train ImageNet weights and divide the dataset into different percentages. In VGG16 model we got a 99.99% accuracy and 0.01% equal error rate and VGG19 model 99.90% accuracy and 0.01% Equal error rate and ResNet50 99.78% accuracy and 0.22% equal error rate. we discovered that the VGG16 and VGG19 model has a greater 99.99 percent recognition accuracy than the ResNet50 models

VIII. REFERENCES

[1]. Srikanta Pal, Umapada Pal and Michael Blumenstein "Signature-based Biometric Authentication" Computational Intelligence in Digital Forensics: Forensic Investigation and Applications pp 285-314,2014.

[2]. Gabe Alvarez, Blue Sheffer and Morgan Bryant "Offline Signature Verification with Convolutional Neural Networks"2016

[3]. Jivesh Poddar, Vinanti Parikh and Santosh Kumar Bharti "Offline Signature Recognition and Forgry Detection using Deep learning" 3 rd international conference on Emerging Data and Industry 4.0, Elsevier, 2020.

[4]. A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," Circuits and Systems for Video Technology, IEEE Transactions on, vol. 14, no. 1, pp. 4–20, 2004.

[5]. Luiz G. Hafemann, Robert Sabourin and Luiz S. Oliveira "Analyzing features learned for Offline Signature Verification using Deep CNNs" ICPR 2016.

[6]. Buddhika Jayasekara, Awantha Jayasiri, Lanka Udawatta "An Evolving Signature Recognition System" IEEE, 2006.

[7]. I. A. Ismail, M. A. Ramadan, T. El danf, A. H. Samak "Automatic Signature Recognition and Verification Using Principal Components Analysis" Fifth International Conference on Computer Graphics, Imaging and Visualization, 2008.

[8]. Luana Batista, Eric Granger and Robert Sabourin "Applying Dissimilarity Representation to Off-line Signature Verification" International Conference on Pattern Recognition, 2010.

[9]. Ramon Blanco-Gonzalo, Oscar Miguel-Hurtado, Aitor Mendaza-Ormaza, Raul Sanchez-Reillo "Handwritten Signature Recognition in Mobile Scenarios: Performance Evaluation" IEEE, 2012.

[10].Ruangroj Sa-Ardship, Kuntpong Woraratpanya "Offline Handwritten Signature Recognition Using Adaptive Variance Reduction" 7th International Conference on Information Technology and Electrical Engineering (ICITEE), 2015.

[11].Srikanta Pal, Alireza Alaei, Umapada Pal, Michael Blumenstein "Performance of an Off-line Signature Verification Method based on Texture Features on a Large Indic-script Signature Dataset" 12th IAPR Workshop on Document Analysis Systems, 2016.

[12].Abdilbaree Talib Nasser, Nuran Dogru "Signature recognition by using SIFT and SURF with SVM basic on RBF for voting online" IEEE, ICET, 2017.

[13].Aravinda C.V, Lin Meng, Uday Kumar Reddy K.R "An approach for signature recognition using contours-based technique" Proceedings of the 2019 International Conference on Advanced Mechatronic Systems, Kusatsu, Shiga, Japan, August 26 - 28, 2019.

[14].Shalaw Mshir, Mehmet Kaya "Signature Recognition Using Machine Learning" IEEE, 2020.

[15].Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez and Javier Ortega-Garcia "DeepSign: Deep On-Line Signature Verification" arXiv:2002.10119v3 [cs.CV] 22 Jan 2021.

[16].Li Xuan, Zhang Hong "An Improved Canny Edge Detection Algorithm" IEEE,2017

[17].Rikiya Yamashita, Mizuho Nishio, Richard Kinh Gian Do and Kaori Togashi "Convolutional neural networks: an overview and application in radiology" Springer, 2018.

[18].Karen Simonyan and Andrew Zisserman "VERY DEEP CONVOLUTIONAL NETWORKS FOR LARGE-SCALE IMAGE RECOGNITION" Published as a conference paper at ICLR 2015.

[19].He, K.; Zhang, X.; Ren, S.; Sun, J. Deep Residual Learning for Image Recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, 27–30 June 2016; pp. 770–778.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Digitalisation of PMPML Transport System : India

Amaan Awati, Sagarika Chadawar, Dr. Ganesh Jadhav, Dr. Suman Devadula, Dr. Sai Prasad Ojha
School of Design, MIT-WPU, Pune, India

ABSTRACT

This Public transport has always been an integral part of any city structure. Public transport, as we know, is a local travel option provided by any city or town. India has evolved from tanga (carriage) to its first railway in 1853, in Mumbai. India has seen a wide variety of public transport spread across its area. [1] Pune Mahanagar Parivahan Mahamandal Ltd. (PMPML) is one such major public transport offered by the government in Pune city, situated in the state of Maharashtra, India. 1.1 million people travel around the city daily through PMPML. [2] This bus transport facility was created to be used by everyone without any discrimination. Due to the lack of innovation and maintaining the quality with which it was created, people have shifted to different means. With the recent boom in digitalization in every sector, it is time for the PMPML public transport system to take a step ahead. This study focuses on the current PMPML system, the problems faced by its users, and how, by making use of digitalization, these problems can be solved. In-depth research was carried out, where primary research, secondary research, interviews, and surveys took place. A solution was found in the form of a new digital system, which included an application for the users and for the employees of PMPML, along with other hardware. All this would result in more people switching to public transport, which would bring immeasurable positive changes along.

Keywords— Urban planning, User Experience Design, User Centric design, bus transport; System design; UX Design, Public transport.

I. INTRODUCTION

Like the word suggests, public transport is a system for citizens to use to commute around the city without owning it. Public transport plays a crucial role in metropolitan cities like Mumbai, Delhi, Bangalore, Pune, etc., where the number of private vehicles on the road is high, which results in more traffic.

Figure 1. Aerial view of Pune City, Source: Proptiger

Cities are defined by their public transport systems. We see trams in Kolkata and the tubes in London. Public transport was created to connect and move people from one place to another, getting them one step closer to resources, people, and opportunities. As time passed, it became a necessity.

Pune, earlier known as Poona, is a metropolitan city in the state of Maharashtra, India. It is famous for various things and has multiple identities, like the Queen of the Deccan, the cultural capital of Maharashtra, also Oxford and Cambridge of India. With all this, Pune is also known for its traffic as it ranks 5th in the globe for traffic congestion. [3] Pune is home to over 6 million people [4], which has resulted in 3.88 million vehicles in Pune and 1.87 million in Pimpri Chinchwad by the end of March 2019, according to the RTO (Regional Transport Office). [5] Because of its good standard of living, industry, opportunities and lifestyle, it has witnessed a rapid migration of people. But even after all this, Pune is a city for everyone and welcomes everyone with open arms. With more people coming in, the population of Pune is rapidly increasing, but fewer people are opting for public transport as an option to commute. Public transport comprises merely a 15% share. It might see a drop and be reduced to 10% by 2031 if not looked after. [6]

Figure 2. Bus fleet of PMPML, Source: PMPML.

To support the people and stay connected to all parts of Pune, you will see a wide variety of public transport here, from rail to road, from cabs to rickshaws, and mainly its PMPML bus transport service. Pune has seen an evolution of public transport. In the early 1940s, tangas were the only mode of transport. The idea of public bus transport was brought in by Pune Nagarpalika. It started with 4 routes and 20 buses, and the fleet grew to 46 by 1948. In 1950, it was renamed PMT (Pune Municipal Transport). To cover the Pimpri and Bhosari areas under Pune urban, PCMT (Pimpri Chinchwad Municipal Transport) was formed on March 4, 1974. All this was merged on October 19th, 2007 to become a single entity, which gave birth to PMPML (Pune Mahanagar Parivahan Mahamandal Ltd). [7] PMPML (Pune Mahanagar Parivahan Mahamandal Ltd) is a core part of the Pune city public transport system. When you investigate the building blocks of this system, you will find that there are 2045 buses in its fleet, 1382 buses on the road per day, 13 bus depots, 2392 bus stops, 371 bus routes, and 17074 trips per day on average.

PMPML is a transportation system designed for everyone, with the goal of providing access to a safe, secure, affordable, accessible, efficient, reliable, and resilient transportation solution that reduces carbon footprint and promotes sustainable development. Public transport plays a vital role in such urban cities, with benefits like cheap transport and less traffic. It also helps to lower a city's per capita carbon footprint, noise pollution, less traffic and much more.

But even after PMPML being so well connected and cheap, it was observed that people aren't making the maximum use of this facility, with only 1.1 million ridership, which is only 16% of the entire population. [1] This leaves you curious about why people are not choosing PMPML as an option to commute. Research was carried out, where primary and secondary research took place, interviews were conducted, and the current PMPML system was studied. It was observed that people do not find PMPML reliable or safe as they do not know when the bus will come, if it has space, and have no assurance about the same.

Curitiba, Brazil saw the first BRT, known as the Rede Integrada de Transporte, in 1974. After being inspired by them, many countries quickly began experimenting with the same. In India, the first city to experiment with BRTS was Pune. PMPML started plying pilot routes in December 2006. The system was named Rainbow BRTS in the twin cities of Pune and Pimpri-Chinchwad in Maharashtra, India and is operated by the Pune Mahanagar Parivahan Mahamandal Limited (PMPML). Pune Municipal Corporation (PMC) and Pimpri-Chinchwad Municipal Corporation (PCMC) came together to build the needed infrastructure. The project is spread across 113km of route committed for the PMPML buses, bus stops, and terminals. [8]

Digitization is at its peak, and people are living in a rapidly growing world. India's digital journey is one of exuberance. The country had the world's second-largest internet population, with over 749 million users in 2020. Of these, 744 million users accessed the internet via their mobile phones. Estimates suggest that this figure will reach over 1.5 billion by 2040. The Digital India campaign came into the picture and was launched by the government in 2015. This has brought in a lot of infrastructural improvements. It is a big step and an initiative taken by the government of India. Several schemes have been launched around this plan, where they plan to take different sectors to an electronic platform.

In this study, you will see the optimum use of the existing resources present at the system's disposal so that a huge misspend can be avoided. By redesigning the current PMPML system, the aim is to create a more reliable and trustworthy bus transport system, where people can track the bus, view the vacancy on the bus, book tickets online, have a streamlined complaint and feedback system, do journey planning and much more. This will result in more people willingly switching to PMPML.

This study focuses on changing and improving the image that people carry of PMPML by redesigning the system to make it more user friendly, user-centric, reliable, and trustworthy. A healthy shift in pattern can be expected, and a behavioral change will be induced, in which more people will be motivated and willing to use the PMPML services.

II. METHODOLOGY

Different research methods were used to study the topic, like surveys, interviews, and open-ended conversation.

A. Field Visit
B. Primary and Secondary Analysis
C. Identification of problems/ issues with the help of collected data and data analysis.
D. Proposed Solution
E. Validation and Evaluation

III. RESULT

A. Field Visit

In-depth research was carried out. When the system was studied in a more detail-oriented fashion, these are some of the major stats that were observed.

To begin with, the current process of PMPML was studied. Some of the key operations in which the users were directly involved were focused. When the journey of a user was retraced, the key operations that were spotted were: (i) buying a ticket, (ii) buying a pass, (iii) finding the bus schedule, (iv) journey information, and (v) providing feedback.

To buy a bus pass, a citizen has to visit a PMPML pass center, fill in a form manually, pay the money, and wait to get the pass. This process is the same for senior citizens too. It proves to be very tiresome, especially for them, as they must physically travel to the center, stand in the queue, and apply for the pass. When we see the process of how students get their bus passes, they must go to the PMPML pass center, get the form, fill it out, get it signed by the institution they are studying at to verify it, go back to the office, make the payment in cash, and get a physical copy of the pass. Their pass is cheaper and only takes them to and fro from home to the institution.

Now, if a person wants to directly buy a ticket, they must board the bus that will take them to their destination, pay in cash, and then they will receive the bus ticket. Over here, there is no online payment option. Paper is being used as a ticket for a one-time action, and the passenger must preserve this piece of paper and keep it safe till the end of the journey. To find the schedule, one must log on to pmpml.org or go to a bus depot to find it. There is no solid way to find the details of the bus you are travelling on, for example, if you need the name of the driver or conductor. Lastly, when a passenger must raise a query, file a complaint, or give feedback, they have to go to the PMPML office or log on to pmpml.org. Even after doing this, they must follow up by going to the office as the information on the website is not updated, as reported by many.

Item	Data
Total Vehicles (per day)	2,066
No. of Breakdowns (per month)	875
Average Passengers (per day)	9,44,903
Routes taken by Buses (per day)	317
No. of complaints (per month)	1,877
Total no. of Cancelled kms. (per month)	36,22,158 kms.

Figure 3. Statistics of PMPML.

B. Primary and Secondary Analysis

The UX research was mainly divided into open-ended interactions, online research, and surveys with the help of Google forms.

For the open-ended interactions, people standing at the bus stops were approached. They were briefed on our goal and the reason for the research. The things that were gathered are, tracking of the buses is tough, even if the bus comes on time, it is too crowded, they don't have a choice but to board it because they don't know the timing of the next bus, they don't know how to manage and plan their journey, and if no one is there at the bus stop, it's difficult to figure out which bus has already left.

While diving into online research, different community platforms were studied and referred to, like Quora, the PMPML website, articles, and reports. In which incidents like rude behaviour of the conductors or bus drivers were most common, there was a lack of empathy for the passengers, especially for outsiders (non-Maharashtrians), as they do not know the local language, which is marathi and hence face discrimination. Some buses do not stop at bus stops even if they are vacant, the schedule is not followed, and the buses aren't well maintained. In many scenarios, passengers fail to receive change because the cost of the ticket is not a round figure. Most of the time the passenger leaves the change behind thinking it is just 1 or 2 rupees or in other situations, the conductors do not have change money, all this generates money which is left untraced and goes into the pockets of employees of PMPML.

C. Identification of problems/ issues with the help of collected data and data analysis.

Field surveys were carried out in the PMPML area, and with the help of Google forms and questions, 100+ people participated in our survey. The demographic to which our respondents belonged ranged between the age group of 19 to 50 years and were distributed across areas like Aundh, Pashan, Bavdhan, Kothrud, Punawale, Mundhwa, Kalyani Nagar, and Wadgaon Sheri. Our respondents are students in high school and college, homemakers, office goers, and most of them are graduates. The insights that we got from the survey are as follows:

- 50% of our respondents use private vehicles to commute in the city, especially to work. 18.7% use only public transport, and 32% of them use public and private modes of transport to commute around and to work.

- 31.2% of our respondents only use 2-wheelers to commute to work. Whereas 12.5% of people use 2-wheelers and 4-wheelers. It is also seen that 31.2% of people use PMPML and other public transport like auto-rickshaws and six-seaters. Only 18.7% of individuals use all modes of transport to travel to work.
- Around 53.8% of people have rated their PMPML every day journey experience as 3, where 1 is on the negative end and 5 is positive. 30% gave it a 4, 7.6% gave it a 2, and 7.6% gave it a 1 for the journey experience.

Figure 4. Overcrowded PMPML bus.

- The major reasons why people like and prefer PMPML are that it is cheap and affordable, they sometimes get space to sit, and you can sometimes reach your destination on time. With this, a lot of people also said that there is nothing to like about PMPML as such, and they are using it because they do not have any other alternative.
- When asked about what the respondents disliked about PMPML, the quality of the buses, unclean, overused buses, not maintained (this is reflected in the frequent bus failures), delays in reaching the destination, irregular timings, not comfortable, unsafe, and they only accept cash were the major responses. The rude behaviour of the conductors and drivers, especially with non-localities (non-Maharashtrians), is also one of the major reasons why people dislike PMPML.
- It was observed that the respondents spend between 1000/- and 4000/- rupees monthly on commuting. Here, 56% of them travel between 10km and 20km, 25% of the respondents travel between 21km and 30 km, and 18% travel between 31 km and 50 km on a daily basis.
- 81.3% of the respondents reach their workplace, office, or college on time, but this is because they generally leave a huge margin before leaving, so that even if they encounter any congestion on the way, they have time on hand. The remaining 18.8% arrive late due to traffic or because they rely on PMPML to get to their destination. These people leave early too, especially the ones who travel by PMPML, but because of the irregular timings, it becomes a task for them to calculate the time they will need to reach the destination.

Figure 5. Picture showing fight between a PMPML conductor and a passenger.

- On asking what changes they would want to see in the public transport system so that they would use it more, the suggestions that were received from the respondents speak a lot. The frequency of the buses should increase so that there is less rush on the buses. Their location should be known by expanding the area which PMPML covers. The employees should be better behaved. The buses should be clean and maintained. There should be more space for people to sit. Online booking and safety were the major feedback.
- The respondents were given the option of live tracking of the PMPML buses. Then the respondents were asked if they were willing to switch to PMPML and the response was as follows: 68.8% answered yes, 18.8% said maybe, and 12.5% said no.

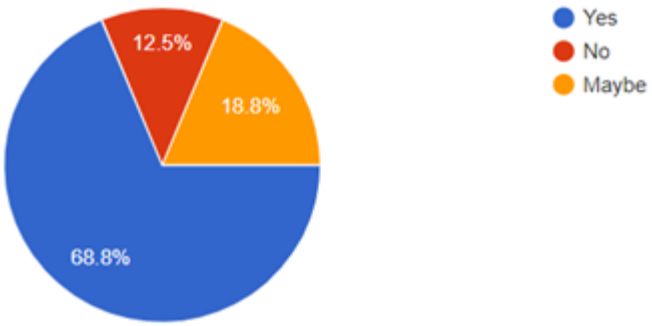


Figure 6. Live tracking option response

- On giving the option of getting points, offers and cashback, would people be more willing to switch to PMPML, 75% said yes and 25% said no.

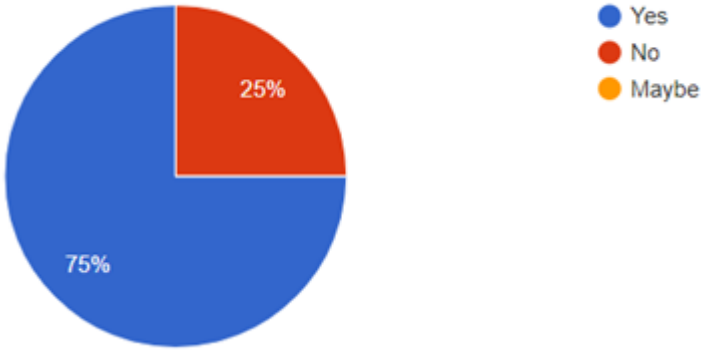


Figure 7. Reward option response

- To understand the ease with how well the individuals can navigate and use their phones and the application, they were asked to rate their skills from 1 to 5, where 1 was towards the negative end and 5 was towards the positive. 37.5% of people gave themselves a 5, 31.3% said 4 and 31.3% voted for 3.

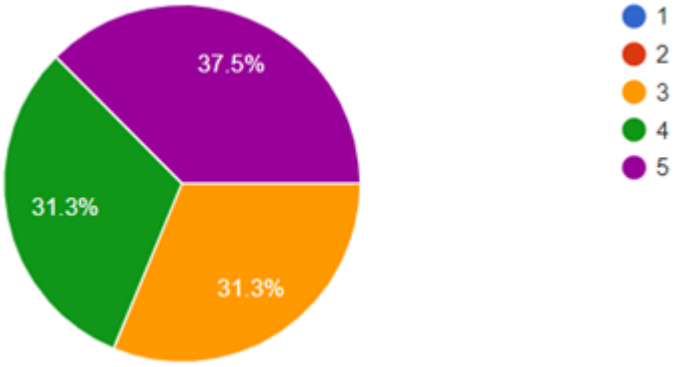


Figure 8. Technological usage

- Lastly, it was discovered that 81% of people prefer online payment and only 19% of people prefer cash as a mode of payment. Also, 42.9% have rated their comfort level as 5 with online payments; 42.9% have given a 4; and 14.3% have given a 3.

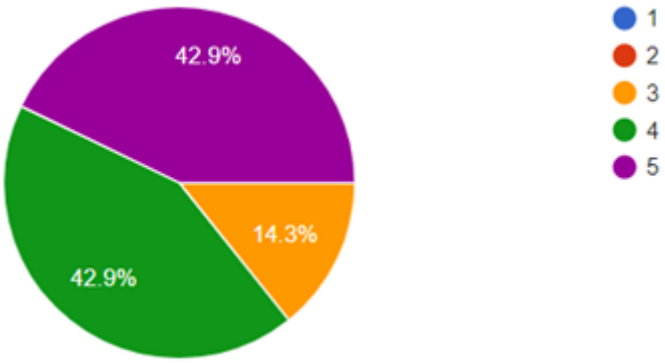


Figure 9. Preferable payment mode

It can be observed that people have started to give preference to private transport as it is time-saving, convenient, offers personalized spacing, is always on time, and reliable. [6]

A market analysis was carried out to study and find if there is any solution that solves the problems that users are currently facing or are close to bringing about a system change to promote the use of PMPML bus services. PMPML Traveller is an application released by PMPML to improve the experience of people using PMPML. There are other applications like PMP E-Connect, Pune (data) m-Indicator, and Pune local Bus Guide that exist in the market that help the user to see the location, bus routes, give feedback, etc.

The PMPML system has been built with the motive to help people, to make their lives easier and to make sure that they stay connected, but the majority of people, especially the youth, are unwilling to use the PMPML services. The current system is still benefiting from digitalization. Not only will they attract more riders, but it will also give PMPML a new identity. 75-80% of the commuters today have smartphones with an active internet connection, there will be a shift in the patterns seen in how people use and view public transport.

If no development is seen in the transport system, there will be an increase in the number of people shifting to personal modes of transport. As the number of vehicles on the road increases, there will be an increase in the demand for fuel, which will result in a hike in prices. The Pensioner's Paradise—Pune will no longer be a place for the elderly if this problem is not worked upon. [8]

D. Proposed Solution

After getting an in-depth understanding of the current scenario, it is apparent that change is needed, and this change can be brought in smoothly by using the existing resources at hand. With digitalization being at its peak right now, the proposed solution mentioned below will integrate digitalization to redesign the PMPML system and aim to bring a behavioural change.

Figure 10. Splash Screen of the UserApp.

Figure 11. Home Screen of the UserApp.

Headings, or heads, are organizational devices that guide the reader through your paper. There are two types: component heads and text heads.

Use of integrated elements like QR codes, smartphones with active internet connections, and portable Bluetooth printers will be implemented in this system. First the application will be explained, followed by the environment in which the application is going to be used.

After multiple alterations, revisions, and various versions of wireframes, this is the mock-up for our PMPML system. While making the application, the Rainbow BRTS was kept in mind as shown in Figure 10. Rainbow BRTS is a bus rapid transit system in the city of Pune. The system is operated by Pune Mahanagar Parivahan Mahamandal Limited (PMPML). The infrastructure has been developed by the Pune Municipal Corporation and Pimpri Chinchwad Municipal Corporation, Pune. The project currently envisages 113 km of dedicated bus corridors along with buses, bus stations, terminals and an intelligent transit management system.

The color palette has been decided based on the Rainbow BRTS brand colors. The primary color is Prussian Blue, and the secondary color is Dark Grey. On opening the application, the commuter will come across the splash screen, where one will see the rainbow logo.

In the entire application, one will see the use of multiple design principles and rules. Gestalt's principle has a strong influence on the application. When the commuter sees the home screen or the landing page, the major tasks that you will be able to view and carry out are: booking a ticket, scanning QR codes, buying a pass, and one will also be able to view their active ticket. "Your Active Tickets" will come in handy for commuters when they have an active ticket/s booked to see the information or get it validated by the conductor. The entire application is multilingual, अ icon enables the user to change the app language to their preferred language to increase the accessibility of the app, and the bell icon indicates the number of notifications and reminders commuters have. One can also see "Book a Ticket", "Scan QR", "Buy a Pass", and "Search Bus" and similar quick actions on the home screen of the app which can be seen in Figure 11.

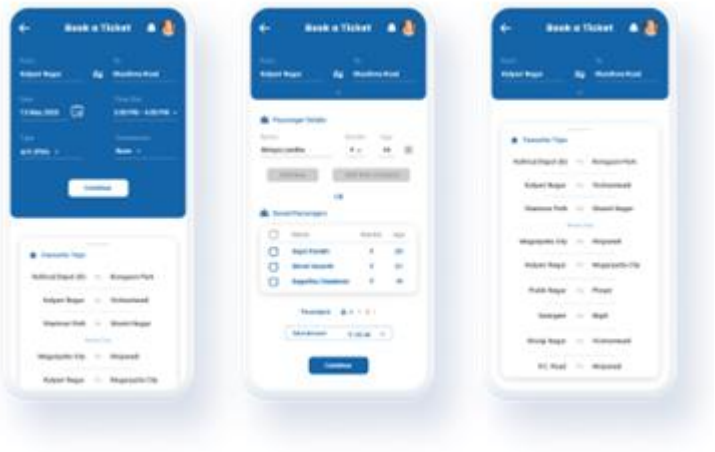


Figure 12. 'Book a Ticket' workflow of the UserApp

When the commuter comes to the Book Ticket page (Figure 12), they will witness a wonderful use of proximity and gamification. The function of this page is to enter the details of their journey. Starting with the location where one wants to go, time, and date, the use of AI can be seen where the app understands a particular travelling behavior where the user frequently travels and suggests the destination to go to with the 'Favorite Trips' section. After you fill in the required details, and make the payment through various online payment methods integrated through a payment gateway, it will generate an e-ticket. It also asks them if they are a frequent passenger or a one time or first-time passenger. After the commuter fills in the required details, it will generate an e-ticket. To increase the user experience, one will see micro-interactions on every page. Here they will see arrows to interchange the values of the pickup and destination, gamification for approval feedback, and flashcards that can be dragged and expanded.

Figure 13. QR code-based e-ticket.

After being directed to the e-ticket screen like shown in Figure 13, the commuter will get an auto-generated e-ticket for their trip, where the location, time slot from when the ticket is valid, date, number of passengers, type,

ticket ID, passenger details, and total amount will be mentioned. The introduction of online payment in the process of buying tickets can help people save a lot of time, and the issue of getting change will be resolved too. This screen will also give the commuter the option to share the ticket. This way, the passenger can book the ticket for someone else and share it with them. The ticket will also have a QR code, which the conductor will scan and validate to see if the ticket is authentic. Lastly, this screen will also show the commuter the option to set a reminder. It will also be mentioned in the paper ahead that the application will provide commuters with the live location of the bus. Using this data, the passengers will be able to set reminders or alarms for themselves, to remind them about their stop, so that in any case, if the passenger falls asleep during the journey, they will be notified about their stop.

After filling in all the needed information, the commuter will be shown a list of buses that will take them to their location, and they will have to choose a bus from the list. Commuters will be able to view the ETA of the bus at the bus stop. It will also have some feature icons which are going to be common across all the buses, like wifi-enabled, ladies-only, and seats for senior citizens.

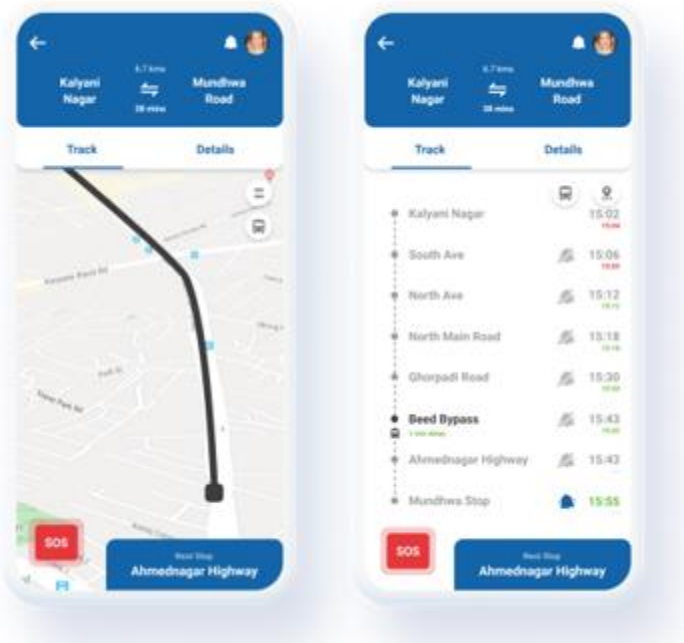


Figure 14. Live Journey mapping screens in the User App.

On the journey mapping screen, two main functions will take place. One is map tracking, where the location of the bus will be visible on the map and it will be followed along, both the options are shown in Figure 14. The other function is, stop wise tracking. Over here, the passenger will see which stop they have crossed and which stop will come ahead. With this feature, the passenger can see the current accurate location. There is a floating SOS button that has been placed on the left bottom corner, keeping ergonomics in mind. It is not an action that is carried out regularly, but when it is needed, it will be easily accessible.

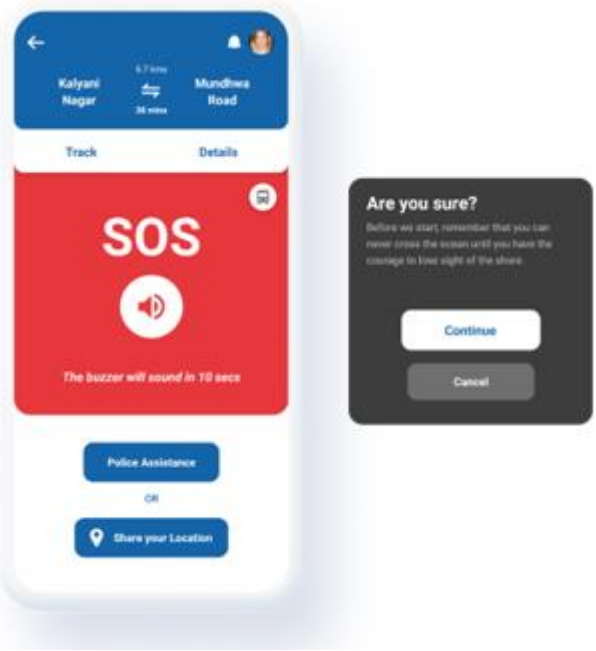


Figure 15. SOS screen.

When the commuter clicks on the SOS button, the commuter gets an option to use police assistance or share the location. The commuter can use this according to the urgency of the situation. Once clicked, it asks the passenger for a confirmation message, which gives the passenger a lobby to rethink and takes a step back if they clicked it by mistake, like represented in Figure 15.

Figure 16. Bus details screen.

The journey details page is shown once the passenger has boarded the bus. To engage them, they are asked for feedback. This will increase the accuracy of the feedback as the passengers will be giving it while they are in the

environment. The feedback will have basic questions like the availability of the seats, if the bus arrived on time, was it clean, etc.

When on the bus details screen, it will have all the information about the bus like who is driving, who is the conductor, their ratings, feedback, and achievements. If the commuter faces any issue or wants to appreciate their service, they can leave a review there. Icons of batches are given for achievements; stars are used to represent ratings of the PMPML employees; and flashcards are used for feedback, this can be seen in Figure 16. This will motivate the drivers and conductors to treat the commuters in a better manner as they will be answerable to the higher authorities. The bus live tracking screen will show the passengers the live location of the bus when they are looking for a new bus and when they are riding the bus too. With the help of the colour coded system, as shown in Figure 17, the commuter can also see the vacancy on the bus.

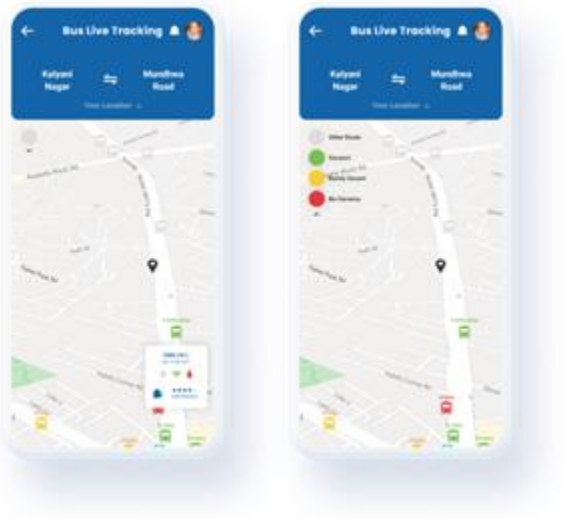


Figure 17. Live vacancy tracking of buses.

Now, the environment in which the application is going to be used needs QR code installation in the buses and a portable Bluetooth printer. For features like bus details, the commuter will have to scan the QR code that is assigned to the bus and installed on it. This is for commuters who have not pre-booked their ticket with the application. With the help of this, the commuter will also be able to track the location of the bus and give feedback using the same.

Figure 18. QR Code displays on the buses for users to scan and view bus, conductor and driver details.

For commuters who do not have access to smartphones or an active internet connection, they can still pay in cash and collect the ticket from the conductor. In case the commuter wants to pay using an online method and doesn't want to use the application, the conductor will generate a QR code that the rider can scan and pay.
The proposed solution will make public transport more accessible to the vulnerable groups of society, like the disabled

Figure 19. Conductors can use the conductor app to generate and print ticket for users who don't have access to smartphones, using handy Bluetooth printers.

and ethnic minorities. As the project will be run by using the current available resources, money can be saved by the PMPML [9]

E. Validation and Evaluation

The proposed solution was validated by multiple people post design process. It received wide acceptance from people and got positive feedback. The high-fidelity prototype was taken to people and after the idea was explained to them, it was much appreciated and welcomed. People were also open to the idea of using PMPML bus transport system if the problems mentioned above were solved on implementation of the proposed solution. The prototype was shown to over 100 people and were asked to rate the solution on four aspects: i) Usability ii) Motivate to use PMPML iii) User Experience and iv) Safety and Trust. With this an unstructured interview and open-ended conversation took place with the audience to take any feedback into consideration which was overlooked while the people were rating the solution.
With respect to the four aspects, 81% of the respondents found the application user friendly, easy to understand and navigate through. 89% of the respondents said that they are motivated to use PMPML bus transport services on implementation of this application. The entire user experience of the application was well appreciated by the respondents with 94% of them saying that they found the user experience really impactful. Lastly, 96% of the respondents found the application safe to use, trustworthy and reliable. With this the respondent were keen on knowing more about the application and appreciated the idea.

IV. DISCUSSION

South Africa has been going through a similar situation where multiple policies and strategies have been put in place to solve the issue. Some worked and some didn't, but using these existing policies and strategies, they are coming up with a better solution. [10] Similarly, this study sheds light on how bringing digitalization into the PMPML system will increase ridership. This is an important intervention as not only will it change the face of PMPML in the eyes of the public, it will also support the Smart City mission and Digital India campaign initiated by the government of India. The proposed solution will help in digitalizing all the information required for the commuters to view and will also make it more accessible to them. The Smart City Mission was launched in 2015 with the aim of improving the quality of life in 100 cities and towns, and this solution can be applied in these cities too, to promote the initiative.

V. CONCLUSIONS

To conclude, it would be safe to say that change is the only constant, and if the proposed solution is implemented and the PMPML system is redesigned, it will witness the biggest behavioral shift in people. People will be more willing to use the PMPML bus service, which will increase the revenue of PMPML, reduce the traffic in Pune city, reduce the carbon footprint and much more. This application and system will make commuting with PMPML buses easier, more reliable, and might make PMPML the first choice of people to commute with. All this can be implemented with a minimum investment, without building any infrastructure and by using the resources present on hand.

VI. REFERENCES

[1]. https://en.wikipedia.org/wiki/Pune_Mahanagar_Parivahan_Mahamandal_Limited
[2]. https://timesofindia.indiatimes.com/city/pune/daily-average-of-pmpml-buses-on-roads-up-by-just-25/articleshow/74501385.cms
[3]. Global Traffic Congestion Ranking Pune ranked 5th in the globe https://timesofindia.indiatimes.com/india/mumbai-bengaluru-delhi-in-top-10-world-cities-in-traffic-congestion-indicating-revival-of-economic activities/articleshow/80246426.cms#:~:text=In%202019%2C%20Bengaluru%20topped%20the,less%20than%20that%20of%202019.
[4]. https://worldpopulationreview.com/world-cities/pune-population
[5]. https://www.thebridgechronicle.com/pune/total-number-vehicles-pune-dist-reaches-617l-34002
[6]. Sandbhor, R. B., & Nawalakha, V. (2017). Comparative Study of using Own Private Vehicle and using PMPML Bus for the Purpose of Local Commutation in the Areas of PMC and PCMC. Indira Management Review, 11(1), 70-76.
[7]. https://www.pmpml.org/en/about-us/statistics/
[8]. Goyal, M. (2017). Digitization of Pune Mahanagar Parivahan Mahamandal Ltd.(PMPML): DAMINI-A Real-Time Bus Tracking App for the Commuters. Indira Management Review, 11(1), 22-37.

[9]. Davidsson, P., Hajinasab, B., Holmgren, J., Jevinger, Å., & Persson, J. A. (2016). The fourth wave of digitalization and public transport: Opportunities and challenges. Sustainability, 8(12), 1248.

[10]. Walters, J. (2013). Overview of public transport policy developments in South Africa. Research in Transportation Economics, 39(1), 34-45.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Customer Churn Analysis in Telecom Industry using Machine Learning Algorithms

Vinit Gawali, Vatsal Tikiwala, Dr. Sachin Bhoite
School of Computer Science, MIT World Peace University, Pune, Maharashtra, India

ABSTRACT
Customers play a vital role in the telecom industry. Churn prediction is having significant importance according to the telecommunication industry. The Churn analysis is helpful for the company to discover the customers who are probably discontinuing a subscription to a service. Recently, the mobile telecommunication market has been modified from a boom market to a shape of overcrowded. The focus of telecommunication companies is to move from large customer growth to keep customers reliable. For that reason, it is crucial to know which customers are likely to leave the services of the company in future. Our proposed solution is for customer churn prediction for telecommunication companies by applying various machine learning techniques like Logistic Regression. An available dataset on Kaggle is used for model building.

Keywords—Churn analysis, churn prediction, machine learning, data mining, customer relationship management.

I. INTRODUCTION

The term customer churn is usually defined as the percentage (%) of consumers who will stop using the company's outcome or assistance after a certain period of time. Eventually, the studies on customer churn analysis started when the concept of Customer Relation Management (CRM) came into existence. As and when the market started to impregnate due to the internationalism of businesses and furious competition, the hiring cost of customers increased. As and when Loyal customers also increased. Due to such loyal customers there is a healthy competition between the companies in the market and help the companies in their own aspects.
Different kinds of various algorithms have been applied on this dataset such as decision tree, linear regression, logistic regression etc. By referring various research papers, we have concluded that logistic regression should be used as it is a classification task.

A. Types of Churners
Churners are divided into two classes: 1) voluntary and 2) involuntary. The Voluntary Churners are again divided into two categories i.e., deliberate churners and incidental churners. Involuntary churn happens due to unavoidable reasons such as payment failure or server failure of our website while transferring the funds etc. The

voluntary churning is an act where the customers are about to exit the services due to factors such as they are not satisfied with they are getting or they getting better services from other companies. Such Churners are difficult to find.

The incidental churners are those churners which have no intention to leave the service but due to other factors such as change in location or change in Social Structure etc. The deliberate churners happen due to customers which demand change in the technology of current service or want the products on great deals / offers.

II. LITERATURE SURVEY

The existing research, which mainly focuses on regression, classification algorithms or decision trees, and such other machine learning techniques. Customer churn makes mention of circumstances that customers no longer buy services or products of a company due to different facts [1].

While dealing with the customer churn issue in telecommunication business, researchers have largely conducted similar research in many important aspects like churn reasons, win – back approaches, and models creation [2].

The network scale has a major bond with the churn of telecom customers, scrutinized under the influence of client comfort and shifting price of customer churn on other telecommunications services and supposed that when the customer happiness stays constant, the higher the switching cost is, the less likely it is to churn [3].

This paper discussed the tie up among client's point of view, diverting hurdles, customer satisfaction, and customer retention. It is understood that customer's happiness totally correlates with the customer's retention. [4].

In the existing studies, it has shown us that churn analysis plays an important role in customer relationship management. However, in management practice, this analysis will bring mighty losses to the profits and evolution of the enterprises. [5].

III. DATASET

Data/Source: Kaggle

Dataset Description:

Each row in the dataset represents a customer. Whereas each column contains the customer's various attributes like gender, tenure, internet service, contract, mode of payment, monthly charge and total charge. This dataset contains 7043 records and 21 customer's attributes.

Our Data set has 12 String columns, 5 Boolean columns, 5 Integer columns and 2 Others

The "Churn" column is the target attribute of our dataset.

The dataset is explained:

- Services for each are customers signed on for – phones, multiple lines, internet, online security and streaming TV and movies.
- Customer Bank Account Information – how long they have been the client for the enterprise, payment method, paperless billing, monthly and overall billing.
- Demographic information about customers – gender, age range, and if they are married or bachelors and in which area they stay.

IV. METHODOLOGY

In Methodology, we have explained about some of the machine learning algorithms that have been used on the data.

A. EDA

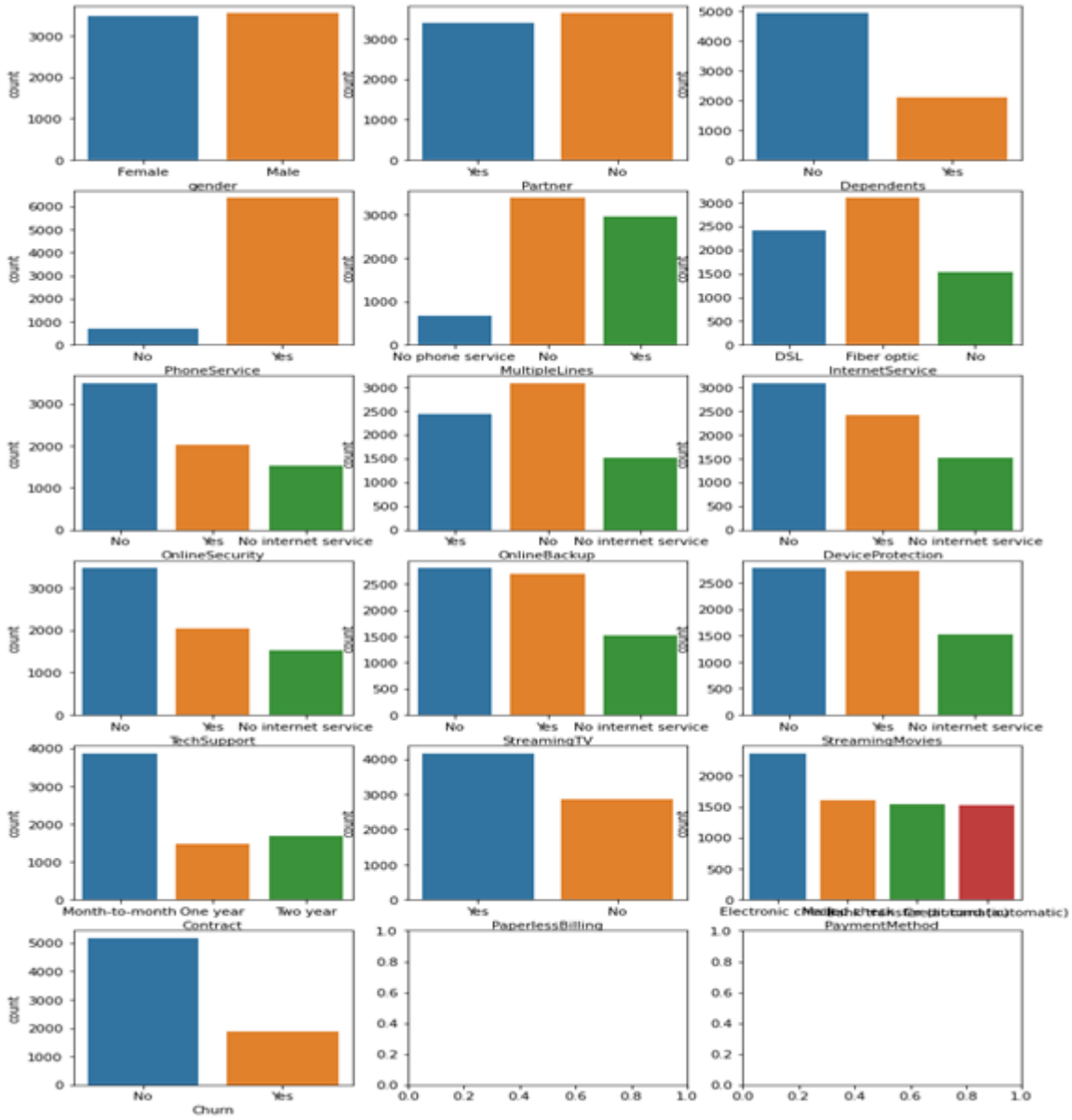


Fig. 1. Countplot

From this count plot, we can see no. of customers in every attributes distributed in three different classes i.e., “Yes”, “No”, “No phone service”.

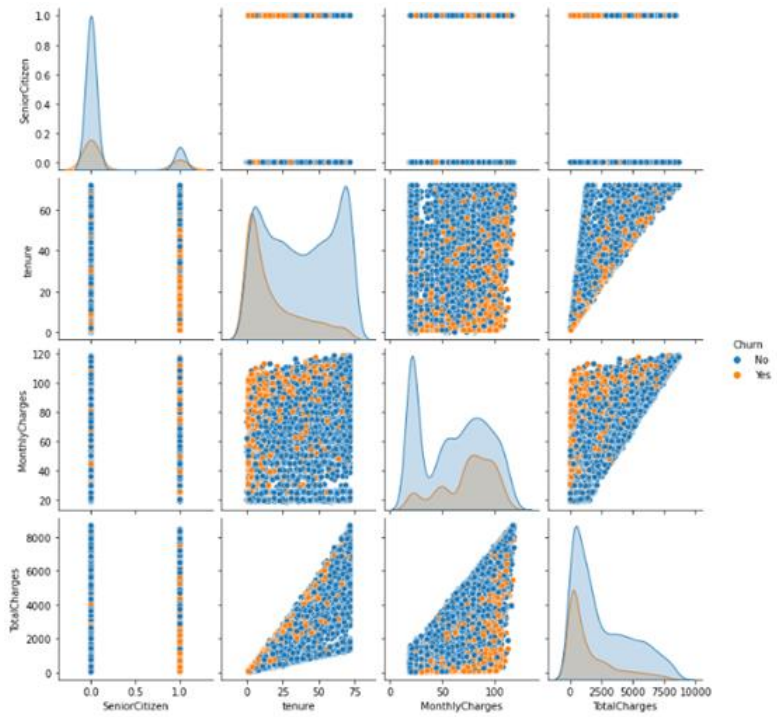


Fig. 2. Pairplot

Target attribute's correlation with other attributes:

Churn	1.000000
PaperlessBilling	0.191825
MonthlyCharges	0.183523
SeniorCitizen	0.150889
PaymentMethod	0.107062
MultipleLines	0.038037
PhoneService	0.011942
gender	-0.008612
customerID	-0.017447
StreamingTV	-0.036581
StreamingMovies	-0.038492
InternetService	-0.047291
Partner	-0.150448
Dependents	-0.164221
DeviceProtection	-0.178134
OnlineBackup	-0.195525
TotalCharges	-0.231873
TechSupport	-0.282492
OnlineSecurity	-0.289309
tenure	-0.352229
Contract	-0.396713

Name: Churn, dtype: float64

Fig. 3. Target's Correlation

Through the above Exploratory Data Analysis, we can understand the correlation of attributes with each other as well as with respect to target attribute.

B. Logistic Regression

Logistic Regression is one of the most popular Machine Learning algorithms, which comes under the Supervised Learning technique. It is used for classification problems as this customer churn analysis is a classification problem. Logistic regression is used to describe data and to explain relationship between one.

Dependent variable and one or more nominal, ordinal independent variables. Therefore, the outcome must be a categorical or discrete value. It must be either Yes or No, 0 or 1, True or False, etc. Logistic Regression can be used to classify the observations using different data types and can easily determine the most effectual variables.

Model accuracy achieved after using Logistic Regression was around 79.61%.

V. RESULTS

Algorithm	True Positive	False Positive	True Negative	False Negative	Accuracy (in %)
Logistic Regression	235	140	1158	228	79.61

In the result we can seen how the confusion matrix tells how the performance of our algorithm is on the dataset. It has given us insights about all the mistakes made by our algorithm and how the confusion matrix helps to interpret the results.

We can say that the variables `Total Charges` and `Senior Citizen` are highly positively correlated. In the correlation matrix we can see the direct correlation between these two variables. We can also spot that there are no outliers present in them.

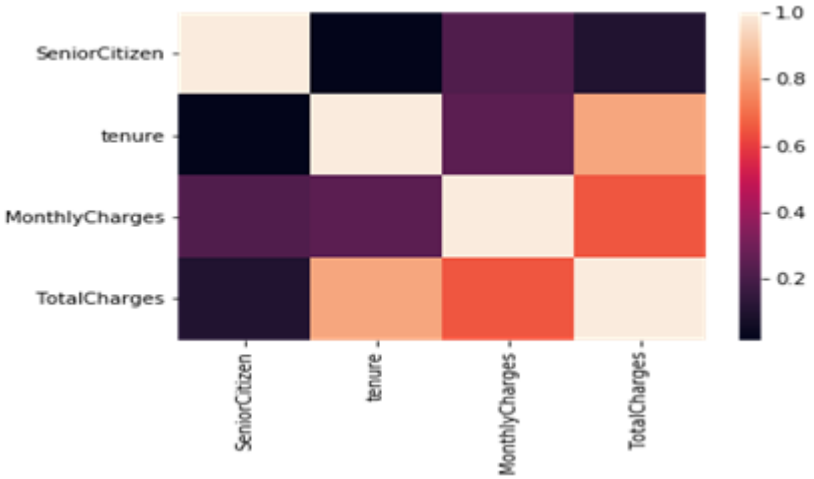


Fig. 4. Correlation Matrix

```
# fit the model with data
lr_model_single.fit(X_train,y_train)
y_pred=lr_model_single.predict(X_test)

lr_acc = metrics.accuracy_score(y_test, y_pred)
print("Accuracy: ",lr_acc)
```

```
Accuracy:  0.7961385576377058
```

Fig. 5. Accuracy

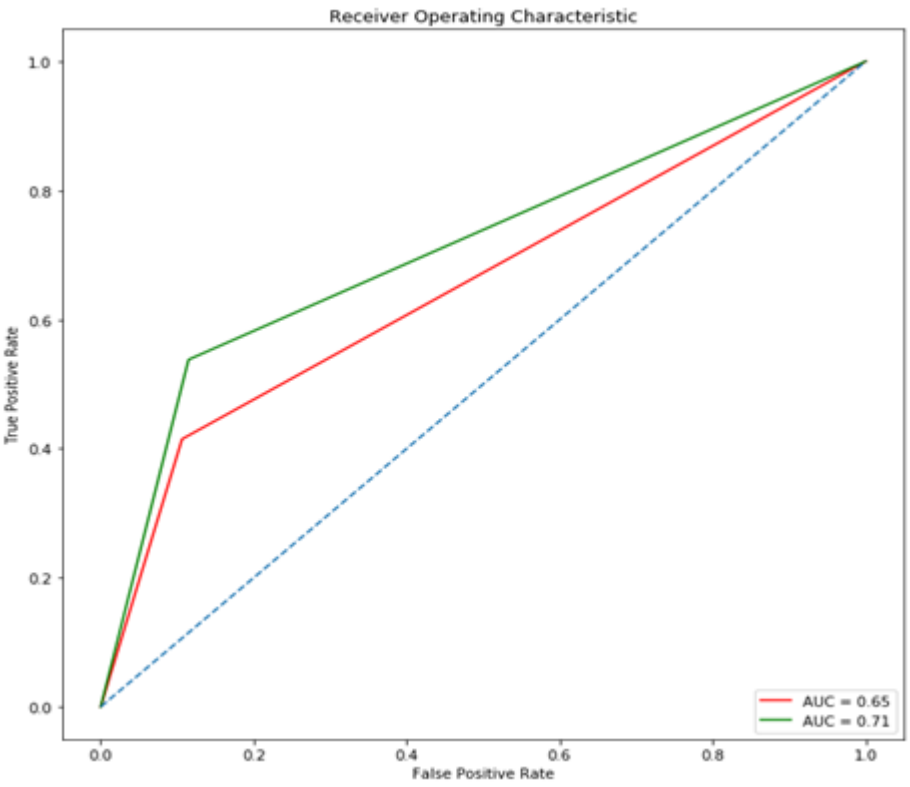


Fig. 6. ROC Curve

Through above ROC (Receiver Operating Characteristic) curve, we can understand the true positive (TP) rate of three classes. We can say that, our proposed model is accurate enough which is providing less false positive (FP) rate than TP (true positive) rate. Because of this behaviour of our model, we are able to achieve 79.61% ≈ 80% accuracy.

VI. CONCLUSION

The main objective of our research is to help companies to make profit. The main purpose of our proposed solution is to predict whether the customers are likely to churn in a telecom industry or not. The analysis of the organizations (with their past data for a particular period of time) helps them to understand a particular day's circumstances of the company and helps the companies to evaluate the churning factor of the company so that the telecom companies can implement new strategies to attract new customers as well as the customers already using their product or services.

VII. REFERENCES

[1]. G. Olle, "A Hybrid Churn Prediction Model in Mobile Telecommunication Industry,", International Journal of E-Education, e-Business, e-Management and e-Learning, https://doi.org/10.7763/ijeeee.2014.v4.302, 2014.

[2]. J. H. Ahn, S. P. Han and Y. S. Lee, "Customer churn analysis: Churn determinants and mediation effects of partial defection in the Korean mobile telecommunications service industry. Telecommunications Policy,", vol. 30, pp. 552-568, 10.1016/j.telpol.2006.09.006, 2006.

[3]. K. J. Back and B. Barrett, "Influencing factors on restaurant customers' revisit intention: The roles of emotions and switching barriers,", International Journal of Hospitality Management, vol. 28, pp. 563-572, 10.1016/j.ijhm.2009.03.005, 2009.

[4]. V. Umayaparvathi and K. Iyakutti,. "A survey on customer churn prediction in the telecom industry: Datasets, methods and metrics", International Research Journal of Engineering and Technology (IRJET), vol. 3(04), 2016.

[5]. S. Qureshi, A. Rehman, A. Qamar, A. Kamal and A. Rehman, "Telecommunication Subscribers' Churn Prediction Model Using Machine Learning,", 8th International Conference on Digital Information Management, ICDIM, 10.1109/ICDIM.2013.6693977, 2013.

[6]. Q. Bi, "Cultivating loyal customers through online customer communities: A psychological contract perspective", Journal of Business Research, vol. 103, pp. 34–44, 2019, https://doi.org/10.1016/j.jbusres.2019.06.005, 2019.

[7]. Y. Xiao, C. Li, L. Song, J. Yang and J. Su, "A Multidimensional Information Fusion-Based Matching Decision Method for Manufacturing Service Resource", IEEE Access, vol. 9, pp. 39839–39851, https://doi.org/10.1109/access.2021.3063277, 2021.

[8]. F. Reichheld and E. Sasser, "Zero Defections: Quality Comes to Services. Harvard business review", vol. 68, pp. 105-11, 1990.

[9]. T. O. Jones and W. E. Sasser, "Why satisfied customers de- fect," Harvard Business Review, 1995.

[10].H. Jain, A. Khunteta and S. Srivastava, "Churn Prediction in Telecommunication using Logistic Regression and Logit Boost", Procedia Computer Science, vol. 167, pp. 101–112, https://doi.org/10.1016/j.procs.2020.03.187, 2020.

[11].S. Chandrasekhar, "Predicting the Churn in Telecom Industry", 2015.

[12].J. Ondrus and Y. Pigneur, "Coupling mobile payments and crm in the retail industry", 2004.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

A Study on Machine Learning and Deep Learning Anomaly-Based Intrusion-Detection Models

Nishit Patil[1], Dr Shubhlaxmi Joshi[2]
[1]Research Scholar, School of Computer, Science, MIT-WPU, Pune, Maharashtra, India
[2]Associate Dean, Faculty of Science, School of Computer Science, MIT-WPU, Pune, Maharashtra, India

ABSTRACT
In the last few years, computer networks have grown larger and more intricate, and intrusion detection systems (IDS) have become an integral part of the system structure. A lucrative underground cyber-crime market and sophisticated tools that make it easier to break into computer networks have led to a big rise in the number of intrusions in the last decade. For more than 40 years, researchers in both industry and academia have been working on ways to detect and stop these kinds of security breaches. They have also built systems to help them do this. It's important for an intrusion detection system (IDS) to deal with things like a low detection rate and a lot of work. One of the most pressing challenges in the world today is data security. Data can be hacked in a variety of ways, causing any network or system to be less effective. Today's intrusion detection systems (IDSs) can't keep up with the ever-changing and complicated nature of infiltration activities on computer networks. One of the most difficult challenges is locating and preventing these types of attacks. Intrusion detection systems (IDS) are censorship systems that continuously monitor the system for suspicious or potentially hostile behaviours and raise an alarm so that the appropriate person may respond swiftly. There are several IDS systems available today, and one of the techniques is to detect intrusions using machine learning (ML), deep learning (DL) which are categorized as Anomaly Based IDS (AIDS) and Signature Based IDS, respectively (SIDS). The study focuses on existing AIDS systems that can detect both known and new attacks.

Keywords : Intrusion Detection, Machine Learning, Deep Learning, Attack Detection

I. INTRODUCTION

The usage of many sorts of networks (including communication networks, social networks, mobile internet networks, and Internet of Things networks) by people all over the world has increased dramatically in recent years, and these networks have enabled many parts of daily life to become easier (such as buying and selling, medical consultation, business, and education). One of the most severe challenges for all of these networks is security. A large number of academics have offered a variety of strategies to address this problem (including firewalls, cryptography, and network access limits). Each of these solutions has a significant shortcoming: none of them are capable of detecting network breaches or attacks. Due to its ability to detect both internal and external

attacks and incursions, intrusion detection systems have been presented as a possible solution to this problem. Users' inbound network traffic is monitored by these systems in order to detect any odd user behaviour or potential fraud. Attackers may be prevented from causing damage to the network structure or data that is transferred across it if these technologies can detect intrusions early enough.

Today, there are many distinct types of IDS systems, one of which is known as Anomaly Based IDS (AIDS) or Signature Based IDS (SBS). Machine learning (ML) and deep learning (DL) are used to detect intrusions, which are split into two categories: AIDS and SBS (SIDS). We'll look at existing AIDS systems to see if they can detect both known and new infections as part of this study. These systems have advantages and disadvantages. Because of its propensity to surpass the constraints of SIDS, AIDS has piqued the interest of many scholars. To construct a typical model of a computer system's behaviour in AIDS, researchers used machine learning, statistical, or knowledge-based methodologies[3]. Any significant deviation from expected behaviour is regarded as an anomaly, which could be interpreted as an intrusion. This method is based on the assumption that harmful behaviour is distinct from regular user behaviour[2]. Intrusions are characterised as unusual user behaviour that differs from the norm. Training and testing are the two phases of AIDS development. When a typical traffic profile is used in the training phase, a model of normal activity is created; when a new data set is used in the testing phase, it is determined whether the system can generalise to previously unanticipated incursions[2]. AIDS can be classed into a variety of categories based on the type of training that was used, which can include statistical, knowledge-based, and machine learning-based training, among other things (Butun et al., 2014)[1,2]. Because it does not rely on a signature database to detect anomalous user behaviour, AIDS' principal feature is its ability to detect zero-day assaults[4]. When the observed behaviour differs from the norm, AIDS sends out a risk signal. Apart from that, there are other perks of having AIDS. First and foremost, they are capable of detecting potentially dangerous indoor activities. In the event that a hacker begins performing transactions in a stolen account that aren't consistent with typical user activity, an alarm is set off[5]. First and foremost, because the system is based on customised profiles, a cybercriminal will have a difficult time determining what constitutes normal user behaviour without sending off a warning[4].

II. REVIEW OF EXISTING SYSTEM INTRUSION DETECTION

Ahmed (2016) et al. The key items to look at are IDS evasion and intrusion detection strategies. There were no papers that discussed intrusion detection, dataset issues, evasion tactics, and various forms of attacks all at a similar time. A new intrusion-detection system is also required, as there have been many innovative concepts in recent years, and it is critical to have one that is current. This article provides an updated review of the field's taxonomy of intrusion detection[1].

Liao (2013) et al. An "intrusion" is someone who performs anything without permission that harms an information system. If there's a danger that information's confidentiality, integrity, or availability will be jeopardised, it'll be classified as an incursion. Intrusions, for example, are things that render computer services unsuitable for individuals who are intended to be utilising them. An intrusion detection system (IDS) is a piece of software or hardware, aids in the security of computer systems. A network intrusion detection system (IDS) can determine whether a computer is being abused. In order to detect and prevent numerous sorts of malicious network traffic and computer usage that a regular firewall may miss, an IDS is installed. This is essential in order to safeguard computer systems against actions that could jeopardise their availability, integrity, or confidentiality. Anomaly-

based and signature-based intrusion detection systems are the two basic types of IDS systems (AIDS). This type of technology is known as a signature intrusion detection system (SIDS), and it looks for a known attack by matching patterns. Knowledge-based detection systems or They are also known as abuse detection systems (Khraisat et al., 2018). There are several techniques used in SIDS to determine if an intrusion occurred previously. The triggering of an alert occurs when an intrusion indicator matches one that has already been recorded in the database. In order to identify whether any command or activity sequences had previously been detected as malware, SIDS scans the host's log files. "Knowledge-Based Detection" (also known as "Misuse Detection") is another term for "Security Information and Data Sharing" (SIDS).

Xiao (2018) et al. Machine learning is based on large amounts of data. To identify and predict behaviour, machine learning algorithms employ complicated "transfer functions." In the fight against AIDS, machine learning is widely used.

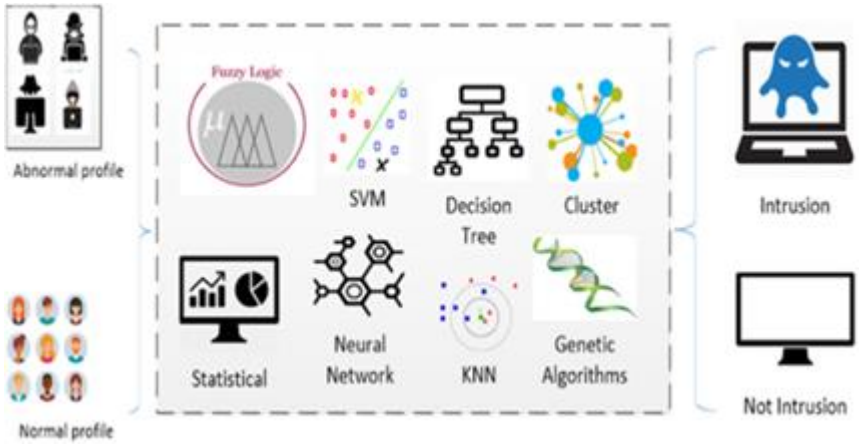


Figure 1. Machine learning techniques in Anomaly Based IDS (AIDS)

The machine learning techniques that were used to build AIDS are depicted in Fig 1. Artificial intelligence (AI) attempts to develop IDS that are more accurate and require less human comprehension. The number of AIDS patients who use machine learning has significantly increased. IDS research focuses on applying machine learning to recognise trends and build intrusion detection systems. Machine learning, both unsupervised and supervised.

Yang, (2012) et al. This technique is based on Bayes' principle and strong attribute independence assumptions. Using conditional probability formulas, Nave Bayes solves problems like "how likely is it that a given type of attack will occur, based on what we know about how the system is being used?" The Naive Bayes algorithm is based on traits that have varying possibilities of being employed in attacks and normal behaviour. Because it is simple to use & does not involve a lot of math, it is one of the most popular models in IDS. This is due to the assumption of conditional independence.

Wang et al., 2010 The Artificial Neural Network is one of the most widely used methods of machine learning (ANN). It has been proven to be effective at detecting many types of malware. The backpropagation (BP) algorithm is the most commonly used approach for supervised learning. It is the BP algorithm that determines how much of a gradient the network's mistake has as a function of the network's variable weights. However, this is not the only problem with ANN-based intrusion detection systems. Even though attacks are becoming less frequent, there is still room for improvement in terms of precision and accuracy of detection. When it comes to assaults that happen less frequently, the training datasets are smaller than when it comes to attacks that happen

more often. As a result, the ANN finds it difficult to learn the properties of these attacks in a timely manner, and as a result, it has problems. Because of this, the precision with which attackers can be detected when they are less frequent is decreased. Unless they are detected, tiny attacks in the field of information security can cause substantial damage. A cybercriminal can get root user permissions and use them to cause damage to a victim's computer systems if the attack is not detected early on. In most cases, it is the rare attacks that stand out.

In 2015, Annachhatre and colleagues published their findings. This statistical model, known as the Hidden Markov Model (HMM), takes into account that the system under study is a Markov process that has not been seen yet. It has previously been demonstrated by The Elhag group et al (2015) However, rather than the usual true or false Boolean logic upon which PCs are founded, this technique is predicated on the degree of ambiguity in an event. As a result, even when the input data is ambiguous, noisy, erroneous, or missing, obtaining a final decision is straightforward. In a fuzzy domain, fuzzy logic enables an object to be a member of multiple classes concurrently. As a result, fuzzy logic is a suitable technique to categorise IDS issues because security isn't always clear, and the distinction between normal and abnormal situations isn't always evident. The data gathered by an intrusion detection system contains a big number of numerical features in addition to a large number of statistical metrics computed on the basis of those numerical features. A substantial number of false alerts are generated when IDSs are developed using stringent thresholds on numbers. An activity that differs only slightly from the model may go unnoticed, while a minor shift in regular activity may trigger false alarms. Fuzzy logic allows you to figure out how to model this little fault so that it doesn't happen too often, lowering false alarm rates. Using fuzzy logic, researchers were able to reduce the number of false alerts when trying to figure out intrusive actions that HMM analysis is effective at detecting various types of malware. Markov Chains with a Secret Training against known malware traits is accomplished through the usage of models (e.g., operation code sequence). The trained model is then used to score all of the traffic that comes in after the training stage has been completed. This indicates that the machine has been infected with malware if the score exceeds a certain threshold. Normal is defined as a score that is less than or equal to a specified level of traffic.

The work of Lin and his associates (2015). K-Nearest Neighbour (k-NN) classification is a non-parametric classification method that is extensively used in machine learning. As a result of grouping unlabelled data into the same class as its k nearest neighbours, these strategies allow the data to be labelled with the names of those nearest neighbours (where k is an integer defining the number of neighbours to be considered). An illustration of the classification performance of a K-Nearest Neighbours classifier with a total of 5 neighbours is illustrated. The point X represents a date that needs to be categorized. Three Intrusion patterns and two Normal patterns are comparable to X. X can be added to the Intrusion class if a majority of people vote in favour.

TABLE I. DETECTION METHODOLOGY CHARACTERISTICS FOR INTRUSION-DETECTION SYSTEMS

Author	*Detection Methodology*	*Characteristics*
Bhuyan, et al. (2014)	Network traffic is monitored, and the data is processed using complex statistical algorithms.	Based on statistics, network traffic is analysed and processed using advanced statistical techniques.
Hall, et al. (2009)	Rule-based: detects a potential attack on suspicious network traffic using an attack "signature."	Rule-based systems may be too expensive to implement due to the requirement for pattern matching.

		Estimating what actions will take place and when is extremely difficult. Determining all conceivable attacks necessitates a huge number of rules. Low rate of false positives High rate of detection
Liao, et al. (2013a) Riesen and Bunke (2008)	Pattern-based: recognises the data's characters, shapes, and patterns.	•It is possible to identify objects using the hash function. •Easy to implement.
Abbasi, et al. (2014) Butun, et al. (2014)	Heuristic-based: recognises any anomalous behaviour that is outside of the norm.	•Knowledge and experience are required. •Learning that is both experimental and evolutionary
Kenkre, et al. (2015a)	State-based: evaluates a series of events to spot any potential threats.	•Probabilistic, self-training •Low false positive rate.

TABLE II. Comparison of results achieved by various methods on publicly available IDS datasets

References	*Observations*	*Results*	*Dataset*
Hu, et al. (2009)	SIDS is applied without AIDS	According to Snort's detection, 69 percent of all generated warnings are false alarms.	DARPA 98
McHugh (2000)	For the preparation and testing of the framework, an artificial neural network (ANN) classifier was used.	With a detection rate of 96 percent, the ANN analysis system is called upon.	DARPA 98
Chen, et al. (2005)	Because it can deal with multidimensional data, An information hyperplane or set of hyperplanes is used to divide information into multiple classes in SVM. When dealing with binary class problems, SVM usually performs well.	When applied to the DARPA 98 dataset, SVM achieved a detection rate of 99.6 percent (see Figure 1).	DARPA 98
Shafi and Abbass (2013)	A good detection accuracy is achieved by this SVM-based classifier, which can be attributed to the use of SMO. Due to the fact that this dataset is more comprehensive and detailed than the one used by DARPA in 1998, the accuracy reported is lower than the accuracy stated for the dataset used by DARPA (Chen et al., 2005).	The SMO classifier has a detection rate of 97 percent (97 percent).	KDDCUP 99

Adebowale, et al. (2013)	Each labelled training instance is used to create a model for the target function, which is implemented by the k-NN algorithm. A similarity-based search technique is used during the classification phase of the algorithm to obtain a hypothesis function that is locally optimal.	The K-Nearest Neighbour (k-NN) method has a 94 percent detection rate.	NSL-KDD
Ahmed, et al. (2016)	According to the probability of each cluster, EM produces a "soft" duty of assigning each row to distinct groups. Because EM does not include a parameter covariance matrix for standard errors, the accuracy of this method is restricted.	Clustering using Expectation Maximization (EM) has a 78 percent accuracy rate.	NSL-KDD
Usteba, et al. (2018)	The Fisher Score algorithm is used to pick features.	When MLP is used alone, 94.5 percent accuracy is achieved; It is possible to attain 95.2 percent accuracy when the MLP and the Payload Classifier are used in conjunction.	CICIDS2017
Creech and Hu (2014b)	There are completely new assaults in the ADFA-WD because it is a whole new data collection. When compared to the accuracy acquired using the earlier KDD98 data, the claimed accuracy for each machine learning technique was reduced as a result of this. Several studies have demonstrated that the SVM is the most accurate.	For the data they were given, Creech and colleagues used Hidden Markov Models (HMM), Extreme Learning Machines (ELM), and Support Vector Machines (SVM) to simulate the results (SVM). They discovered that the accuracy of HMM was 74.3 percent, that of ELM was 98.57 percent, and that of SVM was 99.64 percent.	ADFA-WD
Thaseen and Kumar (2013)	It is C4.5's data characteristic that is most effective in splitting its collection of samples into subgroups, resulting in improved accuracy.	Detection rates of 99 percent were achieved with C4.5.	NSL-KDD
Bot-IoT	The detection accuracy of this SVM-based technique is moderately high (Mitchell & Chen, 2015; Chen et al., 2005; Ferrari & Cribari-Neto, 2004).	The SVM model has the best level of accuracy. Detection rate of 98 percent	Koroniotis, et al. (2018)

III. DISCUSSION AND FUTURE DIRECTION

In this section, the intrusion detection system of different techniques takes place in Table 3 and Fig. 2. From the obtained results, it is obvious that the Genetic Algorithm, Naive bayes, Fuzzy logic and Random Forest methods offered higher privacy over the SVM, KNN and ANN models. In addition, the Genetic Algorithm and Naïve bayes have identified the insider attacks effectively over the other methods in a considerable way. Followed by, the Genetic Algorithm technique has accomplished maximum confidentially over the other methods. In line with this, the Naïve bayes and fuzzy logic techniques have offered enhanced performance in the detection of intrusion. Finally, all the compared methods have demonstrated equivalent performance in terms of accuracy performance.

TABLE III. Security Analysis (%) of Various Methods

KDD'99 Data set Accuracy Performance	
Methodology	*Accuracy Performance*
SVM	86.79
KNN	90.28
Naive Bayes	94.9
Fuzzy Logic	93.45
Genetic Algorithm	97.04
Decision Tree	92.05
ANN	89.22
Random Forest	92.58

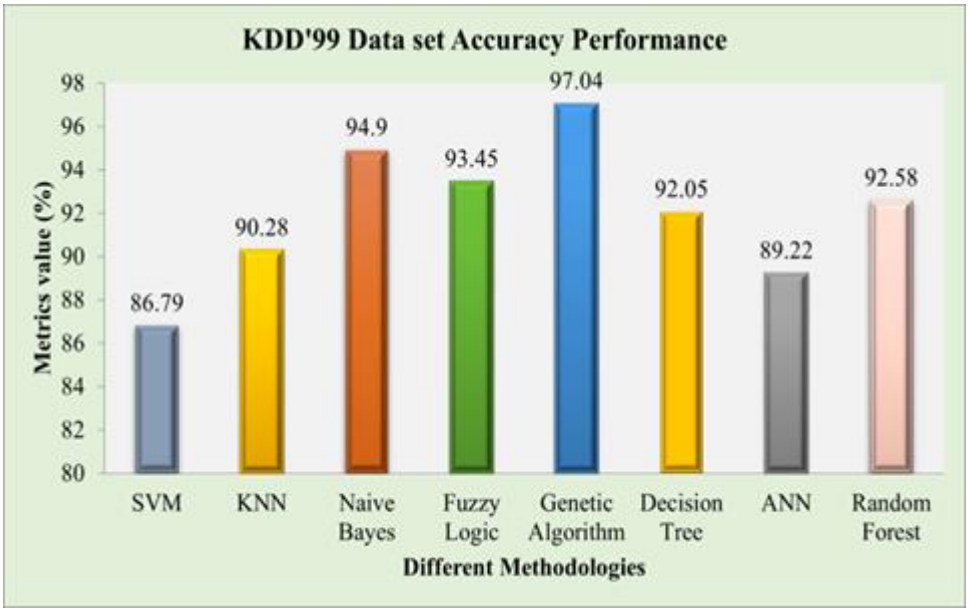


Figure 2. Performance comparison with various existing methodologies

For instance, the Genetic algorithm, Naïve bayes and Fuzzy-logic methods have obtained higher accuracy of 97.04%,94.9% and 93.45% respectively. whereas the SVM, KNN, Decision Tree, ANN and Random Forest

methods have showcased lower accuracy of 86.79%, 90.28%, 92.05%, 89.22% and 92.58% respectively. Moreover, the Genetic algorithm technique has resulted in maximum accuracy performance of 97.04%.

IV. CONCLUSION

We took a close look at how intrusion detection systems function, what types of systems they are, and how they work and don't work in this research. Various machine learning strategies for detecting zero-day threats are investigated in this article. The problem with this is that they may struggle to keep up with all of the information concerning new attacks, resulting in a high number of false alarms or errors. We examined recent research findings as well as current models for increasing AIDS performance as a means of addressing IDS issues. Also included in this analysis were the most regularly utilised public datasets, as well as their data gathering methodologies, evaluation conclusions, and limits. The requirement for fresh and more comprehensive malware datasets that cover a broad spectrum of malware activities is necessary by the fact that typical malware behaviours change over time and may no longer be as successful as they were previously. DARPA/ KDD99 is an old dataset that does not contain any new malware. The majority of machine learning algorithms are taught and evaluated on this old dataset, which does not include any fresh virus activities. Because these datasets were collected in 1999 and are publicly available, they are used for testing because there are no other appropriate datasets. These widely used benchmark datasets do not reflect the behaviour of recent zero-day attacks. Despite the fact that the ADFA dataset includes a large number of new attacks, it is insufficient. As a result, using these datasets to test AIDS does not provide a true evaluation and may lead to false claims about their efficacy, and they should not be used.

V. REFERENCES

[1]. M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," J Netw Comput Appl, vol. 60, pp. 19–31, 1// 2016

[2]. Khraisat A, Gondal I, Vamplew P (2018) An anomaly intrusion detection system using C5 decision tree classifier. In: Trends and applications in knowledge discovery and data mining. Springer International Publishing, Cham, pp 149–155

[3]. Khraisat, A., Alazab, A. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecur 4, 18 (2021). https://doi.org/10.1186/s42400-021-00077-7.

[4]. Zargar J, Tipper (2013) A survey of defence mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys & Tutorials 15(4):2046–2069.

[5]. L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning," arXiv preprint arXiv:1801.06275 , 2018.

[6]. D. Wagner and P. Soto, "Mimicry attacks on host-based intrusion detection systems," presented at the Proceedings of the 9th ACM conference on computer and communications security, Washington, DC, USA, 2002.

[7]. Vigna G, Kemmerer RA (1999) NetSTAT: a network-based intrusion detection system. J Comput Secur 7:37–72.

[8]. Shiravi A, Shiravi H, Tavallaee M, Ghorbani AA (2012) Toward developing a systematic approach to generate benchmark datasets for intrusion detection. computers & security 31(3):357–374.

[9]. Debar H, Dacier M, Wespi A. A revised taxonomy of intrusion-detection systems. Annales des Telecommunications. 2000;55(7–8):361-337.

[10]. Pedro G-T. Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security. 2009;28(1):18-28

[11]. Patcha A, Park J-M. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks. 2007;51(12):3448-3470.

[12]. A. Abbasi, J. Wetzels, W. Bokslag, E. Zambon, and S. Etalle, "On emulation-based network intrusion detection systems," in Research in attacks, intrusions and defenses: 17th international symposium, RAID 2014, Gothenburg, Sweden, September 17–19, 2014. Proceedings, A. Stavrou, H. Bos, and G. Portokalidis, Eds. Cham: Springer International Publishing, 2014, pp. 384–404

[13]. A. H. Sung and S. Mukkamala, "Identifying important features for intrusion detection using support vector machines and neural networks," in Symposium on Applications and the Internet, 2003, pp. 209–216

[14]. Subramanian S, Srinivasan VB, Ramasa C (2012) Study on classification algorithms for network intrusion systems. Journal of Communication and Computer 9(11):1242–1246

[15]. P. Stavroulakis and M. Stamp, Handbook of information and communication security. Springer Science & Business Media, 2010

[16]. Studnia I, Alata E, Nicomette V, Kaâniche M, Laarouchi Y (2018) A language-based intrusion detection approach for automotive embedded networks. Int J Embed Syst 10(1):1–12

[17]. Shen C, Liu C, Tan H, Wang Z, Xu D, Su X (2018) Hybrid-augmented device fingerprinting for intrusion detection in industrial control system networks. IEEE Wirel Commun 25(6):26–31

[18]. Liu X, Zhu P, Zhang Y, Chen K (2015) A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. IEEE Transactions on Smart Grid 6(5):2435–2443

[19]. W.-C. Lin, S.-W. Ke, and C.-F. Tsai, "CANN: an intrusion detection system based on combining cluster centers and nearest neighbors," Knowl-Based Syst, vol. 78, no. Supplement C, pp. 13–21, 2015/04/01/ 2015

[20]. S. Elhag, A. Fernández, A. Bawakid, S. Alshomrani, and F. Herrera, "On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems," Expert Syst Appl, vol. 42, no. 1, pp. 193–202, 1// 2015

[21]. S. Dua and X. Du, Data mining and machine learning in cybersecurity. CRC press, 2016

[22]. H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion-detection systems," in Annales des telecommunications, 2000, vol. 55, no. 7–8, pp. 361–378: Springer

[23]. Z. Du, K. Palem, A. Lingamneni, O. Temam, Y. Chen, and C. Wu, "Leveraging the error resilience of machine-learning applications for designing highly energy efficient accelerators," in 2014 19th Asia and South Pacific design automation conference (ASP-DAC), 2014, pp. 201–206

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Different Aspects of Stability for ML Algorithms

Priyank Pandey[1], Dr. Rajeshree Khande[2]
[1]Department of Computer and Information Systems, Specialization – Data Science, University of Wisconsin – Parkside, United State
[2]Department Faculty, School of Computer Science, MIT World Peace University, Pune, Maharashtra, India

ABSTRACT
Even though the training set is different, the prediction of the stable method is the same. Stability of Different Machine Learning Algorithms is explored, and its stability is determined using methods such as hypothesis stability, error stability, cross validation stability, and leave-one-out cross validation stability, among others, and then merged into a more accurate mode. It will help you choose an algorithm based on its stability and efficacy on the given dataset, among other factors. Develop a set of information-theoretic algorithmic stability metrics and apply them to the challenge of establishing the upper limit on learning algorithms' generalization bias.

Keywords—Stability, Machine Learning, Algorithm, Data Science.

I. INTRODUCTION

to The most crucial factor to consider when evaluating a machine learning algorithm is its accuracy. Several studies have been conducted in order to develop exact algorithms capable of properly anticipating the outcome. To benefit from the stability that only training can bring, it's critical to understand what to expect. This allows us to get a sense of how a model will perform in real life. Check to see if it can be used in a variety of situations. The system's stability must be determined. In the late 2000s, stability analysis became popular as a means of determining the general limit. Rather than being a direct property of the hypothesis space H, algorithm stability is often addressed in algorithms with unbounded or indeterminate VC- dimensions. Stable algorithms do not change significantly even if the data is somewhat changed. Is a machine learning concept that states that the predictions remain the same even if the training data changes? This is an excellent example of how training data may be modified without affecting prediction.

When selecting a machine learning algorithm, we frequently wonder if we've chosen the proper one. Is the information provided accurate? How well does the algorithm handle a variety of situations? We have answers to all of these problems, with the exception of algorithm stability.

To begin, we must define stability and discover why it is so important. The stability of an algorithm is a crucial problem during the training phase of algorithm development since the goal is to have a high degree of confidence

in forecasting the result. A machine learning algorithm's stability is based on the assumption that even slight changes to its inputs can have a significant influence. The prediction of a stable learning algorithm does not change considerably even if the training data is marginally altered. Stability analysis can be used to figure out how changes in inputs affect our system's output. An algorithm that learns from data could be utilized in the system.

Entering data into an algorithm and then developing a model from that data was part of the coaching process. We'd like to see how well the model functions now that we have it. This number, on the other hand, says nothing about the impact of the training dataset on classification accuracy. Will the model remain the same if a subset of the training dataset is chosen? Is the model's efficiency the same if we run the experiment again with smaller subgroups? We'd like the model to be stable and accurate in the best-case scenario. But how can we be certain? This is where the concept of stability analysis comes into play in many circumstances.

To put it another way, stability refers to how changes in training data affect the algorithm's output. The training dataset may change due to a variety of factors, such as the selection of a new subset for training or the presence of noise. For a noisy dataset, setting an upper limit on this type of error might be a simple solution.

The goal is to see if the machine learning algorithm can acquire generalized stability depending on how it reacts to various scenarios.

II. LITERATURE REVIEW

A. Leave-one-out error and stability of learning algorithms with applications

Cross-validation is a valuable method for testing the generalization performance of models rather than attempting to estimate the generalization performance of a model created by a specific process. Leave-one-out cross-validation is used to assess the generalization performance of a model trained on n1 samples of data, which is often a pessimistic estimate of a model's performance trained on n samples.

LOO-CV can be used to get a more conservative overall assessment of the model's performance than simply picking a single model and fitting it to all the data.

It's crucial to remember, too, that despite its apparent neutrality, LOOCV has a lot of variation (the value you obtain changes widely depending on the random sample of data you select). I'm only using it because it's so cheap when it comes to model selection.

It explains how to measure the stability of learning algorithms using the "leave-one-out" method, which uses a range of analyses to show how the algorithm works and how it is almost unbiased. introduce the paper, explain the techniques, and focus on the concept of stability to derive bounds and general error of learning algorithms, present other possible ways to justify the leave-one-out error, and explore various ways to use stability in the context of kernel machines, known for its pattern analysis to study types of relations, an overview of leave-one-out error in other machine learning problems other than classification, and present other possible ways to justify the leave-one-out error in the context of kernel machines, known for its pattern analysis to study types They use stability as a stepping stone to analyze the algorithm's generalization mistake. In addition to its practical application, the work seeks to rationally support the employment of leave-one-out by citing many K-NN reference articles. Other forms of learning tasks, such as classification and regression, may also involve the leave-one-out mistake.

Leave-one-out error and empirical stability, as well as their applications in neural networks and decision tree algorithms, are still unanswered topics in this research.

B. Information-theoretic analysis of stability and bias of learning algorithms.

These algorithms are simply stochastic hypothesis transformations of training data. Extensions to Bousquet and Elisseeff's work show how the result isn't unduly dependent on any single training sample. The study's stability is demonstrated through the use of space constraints to test the strong notation. There are theorems and observations from many information-theoretic backgrounds. Current theories on model stability, in particular how changes in training data affect model estimates, and how well deterministic learning algorithm extensions perform when applied to randomized algorithms are among the subjects discussed in this work.

Non-asymptotic restrictions on the difference between empirical and anticipated error, as well as leave-one-out and projected error, should be established for randomized algorithms that rely on random stability. The framework we created for this reason could be useful in future research into randomized learning algorithms. Machine learning algorithms use stochastic transformation to link training data to hypotheses.

According to Bousquet and Elisseeff's definition, an algorithm is steady when the output does not rely too heavily on any single training sample. By taking into account the stability features of machine learning algorithms, we may obtain exact quantitative estimations of their generalization bias, which is important both theoretically and practically. This paper proposes multiple information theory metrics of algorithmic stability, which we use to determine the upper limit on the extension bias of learning algorithms. You can use these precise results to study the stability and predictive capacity of bagging, as well as to demonstrate that there are no asymptotic limits on prediction accuracy that were previously impossible to verify using the bagging approach. Because it's an extension project, there aren't many interesting topics to investigate, hence it's a bad article for stability research

C. Stability of Randomized Learning Algorithms

Current theories on model stability, in particular how changes in training data affect model estimates, and how well deterministic learning algorithm extensions perform when applied to randomized algorithms, are among the subjects discussed in this work. Should be supplied for randomized algorithms that rely on random stability. The primary goal of this work is to investigate the predictive performance of randomized learning techniques utilizing stability, or the extent to which changes in training data affect model estimations. The second goal is to apply these broad insights to the investigation of bootstrap procedures. It is crucial to define stability, as well as the leave-one-out and expected error, which all rely on random stability, when considering randomized techniques in the context of random stability. These first findings lay the groundwork for a more in-depth research of bagging's (also known as Bootstrap Aggregating) stability ramifications and non-asymptotic constraints on bagging's predictive performance. Bagging is considered when a large number of copies of a training point are treated by the base machines. We show that bagging has a bigger impact on stability and tighter limitations on the difference between empirical and projected error when small sub-samples of the original data are used (referred to as subagging). Consider how bagging impacts learning method stability, and utilize these broad conclusions to create hitherto unprovable limits on bagging prediction performance using the existing deterministic learning algorithm definition of stability. Asymptotic baggers are no longer possible.

D. Bias and the Quantification of Stability

Research on bias in machine learning systems has focused on the impact of bias on forecasting accuracy Prejudice, in our opinion, should be assessed in the context of other circumstances. Two of these characteristics are reproducibility of outcomes and algorithm stability. If both sets of data come from the same event with the same underpinning probability distribution, we want our learning system to understand essentially the same principles from both sets of data. The impact of bias on anticipated accuracy in machine learning algorithms has been extensively researched. Additional criteria, we believe, should be taken into account when deciding whether or not prejudice exists. One of these characteristics is the algorithm's stability, or, to put it another way, the results' reproducibility. When we acquire two different sets of data from the same PD, the learning system should get nearly identical thoughts from both sets. This study proposes a method

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

A Review on Border Patrolling Robot with In Built AI System for Fence

Arnavsingh[1], Swarali Lendghar[1], Shravani Lokhande[1], Navnaat Shete[2]
[1]Student, F.Y. B.Sc. CS, School of Computer Science, MIT World Peace University, Pune, Maharashtra, India
[2]Assistant Professor, School of Computer Science, MIT World Peace University, Pune, Maharashtra, India

ABSTRACT

Recognizing the threats and security to the border fencing which causes illegal border interruptions by terrorist and many other illegal activities. As we all know that they are many areas at the borders where the posting of soldiers is the most difficult task at all time because these areas are having rough terrains and difficult climatic conditions, because of which there are many terrorist groups which find a way through these areas where military forces are not posted and can launch harmful attacks and threat to our country financially, socially and it causes a huge threat to people living near the boundary.

So, the Innovative work in the field of Artificial Intelligence has offered to ascent to Robotics. Now-adays robots are the most important helping hands to all the protection, manufacturing, battling and so forth.

So here I goanna present a Basic idea of How robotics can give its huge contribution to the border patrolling and safety system of our country. Robots can be utilized in to guard the borders and secure the non-reachable areas by just through its Ai detection and signaling. These can also relive the life of many soldiers and the family's only hope.

Border patrolling robot intended to use in such a outrageous and security threat conditions. It tends to be worked and controlled by the Military Headquarters situated in the nearby areas by just giving the signals and informing them about the border's current state. If anybody unknown even touches the fence these reports will be directly send to the military headquarters. Even we install a radar system in it so that any person which appears suspicious to the robot approaching the territory which the robot is guarding will send these reports and alarm the military headquarters.

Now-a- days AI technology gives numerous assets to help us out from these types of situations. This idea assists with creating enthusiasm just as advancement in the field of robotics while moving in the direction of a down to earth and possible answer for to protect us from the harmful terrorist attacks and the damage to life of people and the property.

Keywords: - Autonomous Navigation, fence interruption source detectors, Telecommunication devices for transmitting immediate signals.

I. INTRODUCTION

Border patrolling and safeguarding the border area with a rough terrain and harmful climatic conditions, which can cause death of a human being is an unsafe assignment. And also there are multiple chances of shelling or

military test firings which sometimes leads to death of many soldiers at the borders. Military soldiers need to move on through extreme hardships to survive and protect the borders in these types of risky terrains. And this is not a one day task these soldiers risk their life in these risky terrains for almost 3-4 months . They need to confront many Hazardous conditions such suppose in cold climatic regions such as Ladakh which always as an average temperature of 1-15 degree Celsius, which causes a frost bite which can ultimately sometimes lead to a painful death. Moreover Things become even worse when the altitude is high, there also comes the respiration factor, because at high altitudes we cannot breathe properly. Soldiers also go through hunger and medical problems because at these types of risky areas the transportation system is a bit slow and requires a span 15-20 days to provide the soldiers with the essentials required. As we all know about the Uri attack which occurred in 2016 where a set of grenade attacks carried out by four terrorists against an Indian Army brigade headquarters near the town of Uri in the Indian union territory Jammu and Kashmir on 18 September 2016. The 30 others. It was reported as "the deadliest attack on security forces in Kashmir in two decades".

The terrorist group Jaish-e-Mohammed was involved in the planning and execution of the attack. At the time of the attack, the Kashmir Valley region was a centre of unrest.

So from these we can generate a basic Idea that In future the chances of these type of attacks can be more if we don't switch to a AI powered robot so that not only a specific part of border but the full border is under military surveillance and is protected all the time. These Outcomes needs border patrolling robots to help the military department to save the life of many soldiers which are risked for the protection of borders.

So, if a robot is utilized rather, which can be controlled from a separation or which can perform activities cleverly independent from anyone else, which will lessen the danger of this undertaking of border patrolling. Robot is a mechanical gadget that is utilized for performing assignments that incorporates high hazard like surviving in rough terrains and extreme climatic conditions. There are numerous sorts of robots like fixed-base robots, portable robots, submerged robots, humanoid robots, space robots, medications robot and so on. The fixed base robot has a restricted workspace because of its structure. The workspace of the robot can be expanded by utilizing a versatile stage. These sorts of robots are called versatile robots. Versatile robots are utilized in mining, military, ranger service, security and so forth. Portable robots can likewise be utilized for extinguishing the fire in burrows, enterprises, medical clinics, research centres, and homes. A border patrolling robot will lessen the need of soldiers to get into risky circumstances.

It is difficult to do surveillance and telecommunicate with the headquarters at the earliest when a terrorist group is suddenly into an attack mode. Robot innovation can be productively utilized in such cases to communicate with headquarters at earliest and will also save the life of the soldiers. In this manner, robotics can reduce the workload of the military. The fast advancement in innovation improves the instruments and supplies utilized in surveillance and quick communication. These development apparatuses and types of gear can be progressively compelling and proficient.

The border Patrolling Robot can detect the interruptions through the censors which are implanted on the fencing of the area allotted to the Robot. These censors creates a virtual frame before the fence allotted to the robot. Even if the robot is hacked the virtual frame created infront of the fence to which a continuation of other virtual frame are connected will get discontinued and the other robots will detect this send the response of the hacked fencing area.so Even if one AI robot is hacked the other robots will detect its situation and status and report to the headquarters immediately. But as we know due to so much advancement in the computer technology the chance of getting hacked will be much less. Nowadays, with the development of technology,

several robots with very special integrated systems are particularly employed for such risky jobs to do the work diligently and precisely. This article is intended to give relevant information about such military robots and their working capabilities and efficiencies.

II. METHODOLOGY

1. It is the land u it which uses Atmel Atmega328-PU microcontroller as its core.

Now what actually is a Atmel Amega 328PU:

As we know our robot requires a processing system to govern the actions and functions of it so that it can detect and transmit signals and protecting itself we give it another property of moving from one place to other . So for this a strong processing unit is required This type of functionalities is provided by this software chip:- The high-performance Microchip 8-bit AVR® RISC-based microcontroller combines 32 KB ISP Flash memory with read-while-write capabilities, 1 KB EEPROM, 2 KB SRAM, 23 general purpose I/O lines, 32 general purpose working registers, three flexible timer/counters with compare modes, internal and external interrupts, serial programmable USART, a byte-oriented Two-Wire serial interface, SPI serial port, 6-channel 10-bit A/D converter (8channels in TQFP and QFN/MLF packages), programmable watchdog timer with internal oscillator, and five software selectable power saving modes. The device operates between 1.85.5 volts. By executing powerful instructions in a single clock cycle, the device achieves throughputs approaching one MIPS per MHz, balancing power consumption and processing speed.

2. All the basic sensors such as IR sensor, PIR sensor, LDR sensor, Metal detector, Hall sensor, Moisture sensor, flame sensor and ultrasonic sensor are interfaced to the microcontroller which is supplied with a voltage of 5V, which is obtained at the output of LM317 voltage regulator IC.

(a) IR SENSORS:- As we are aware that for detection of unwanted activites within the range of 5km of border we may require the IR sensors What are they?

An infrared sensor (IR sensor) is a radiation-sensitive optoelectronic component with a spectral sensitivity in the infrared wavelength range 780 nm … 50 µm. IR sensors are now widely used in motion detectors, which are used in building services to switch on lamps or in alarm systems to detect unwelcome guests.

(b) PIR SENSORS:- A passive infrared sensor (PIR sensor) is an electronic sensor that measures infrared (IR) light radiating from objects in its field of view. They are most often used in PIR-based motion detectors. PIR sensors are commonly used in security alarms and automatic lighting applications.

(c) LDR SENSOR:- These devices are used where there is a need to sense the presence and absence of light is necessary. These resistors are used as light sensors and the applications of LDR mainly include alarm clocks, street lights, light intensity meters, burglar alarm circuits.

(d) METAL DETECTOR:- Metal detectors work by transmitting an electromagnetic field from the search coil into the ground. Any metal objects (targets) within the electromagnetic field will become energised and retransmit an electromagnetic field of their own.

(e) HALL SENSOR:- The Hall-effect Sensor is able to distinguish between the positive and negative charge moving in opposite direction. The magnetic field detected by the hall-effect sensor is converted to the suitable analog or digital signal that can be read by the electronic system, usually a motor control system.

(f) MOISTURE SENSOR:- A resistive soil moisture sensor works by using the relationship between electrical resistance and water content to gauge the moisture levels of the soil. ... A electrical current is sent from one probe to the other, which allows the sensor to measure the resistance of the soil between them.

3. **All these sensor values are continuously sent to the control unit which is located at the headquarters for monitoring. To send these information, and for the communication between robot and the control unit, the system uses ASK module.**

ASK module:- Description The RX – ASK is an ASK Hybrid receiver module. It is a effective low cost solution for using 433 MHz. The TX-ASK is an ASK hybrid transmitter module. TX-ASK is designed by the saw resonator, with an effective low cost, small size and simple to use for designing.

4. **Uses cogged wheel technology for the movement in areas such as sloppy areas, rocky areas etc. and the gear motor used for this motion is controlled by a motor driver IC called L298 H-Bridge driver IC.**

THE CONTROL UNIT

1. Located around 1000m away from the robot.
2. Uses ASK transmitter Receiver pair for the communication with the robot.
3. All the sensor values which are sent by the robot is displayed on an OLED.
4. A separate display unit or monitor also present to display the image/video captured by the robot

PROCEDURE: -

(1) DEALING WITH THE CENSORS

(A) WE IMPLANT THE TOUCH SENSORS ON THE BORDER FENCING SO THAT ANY UNUSUAL ACTIVITIES HAPPENING TO BORDER FENCING MAY BE IMMEDIATELY RECORDED AND TRANSMITTED TO THE HEADQUARTERS. BUT THIS TYPE OF CENSING WILL BE THE LAST STAGE OF THE SECURITY SYSTEM

(B) THE ROBOT IS EQUIPPED WITH IR ,PIR AND HALL CENSORS WHICH CAN IMMEDIATELY RECORD THE RADIATIONS AND EVEN THE SMALLEST LIGHT SIGNALS AND FORWARD THIS TO THE HEADQUARTERS.

(C) NOW EVEN IF IN CASE ONE OF THE ROBOT IS HACKED THEN TO OTHER ROBOTS WHICH ARE INTERLINKED WITH IT CAN SEND THIS MISHAPPENING TO HEADQUARTERS

(2) DISTANCE BETWEEN TWO CONSECUTIVE ROBOTS

(A) NOW AS THE IR SENSORS CAN DETECT ANY INTERRUPTIONS UPTO RADIUS OF 5 KM

(B)SO MINIMUM DISTANCE WE NEED IS APPROX 6-7 KM

(3) CONTROL UNIT

(A) THE MOST IMPORTANT PART FROM WHICH A PARTICULAR BATTALION OF ROBOTS ARE FUNCTIONABLE.ALL VISUALS AND RECORDS ARE TRANSMITTED HERE.

(B)THESE HEADQUARTERS SHOULD BE PLACED CONSECUTIVELY WITHIN THE DISTANCE OF 40-50 KM

(C) THE REASON FOR SUCH A CLOSE DISTANCE IS THAT EVEN IF A WHOLE BATTALION OF ROBOTS IS HACKED THEN TO IT WILL TAKE MINIMUM TIME TO REACH THE SPOT.

III. A REVIEW ON BORDER PATROLLING ROBOT WITH IN BUILT AI SYSTEM FOR FENCE

Literature Review

In the present scenario border security is one of the most sensitive issue as it leads to both border infiltration and a threat to indian military and for the local livelihood along the borders. There are different kinds of robots that are specifically employed for doing special tasks in military applications. In military services, there are some areas in which some of the tasks involve greater risk and danger, and therefore, those tasks must be performed without military personnel, solely by the robots.

(1.) A group of creators MS. ASHIKA A K, MS. BHAVYA S N, MS. CHAITHRA C P ,MS. G R BHARANI. They all created a multitasking defence prototype. These multiple tasks include Surveillance, Defence and Attack. The major application of this robot combination system would be in the country borders, war-torn regions and sensitive areas of a country. These can also fulfil capabilities in times of disasters and natural calamities. The recent accidents including border security forces and central reserve police force in regions of regular terrorist attacks as well as militant attacks and the sensitive country border areas where the constant danger of fire as well as natural calamities are claiming hundreds of precious life's at the borders. The idea of the project was to come up with a novel and approachable idea to safeguard the people at the country borders. The idea is more of a precautionary step towards their safety rather than a aide after attack. it is considered to be a dependable support system to fight against violence and dangers befalling our soldiers. It is a system consisting of three major sub-system namely: Bigger robot system, smaller robot system and a Control unit. The Bigger robot is a multiterrain treading land system built to ensure rugged usage and harsh environment operation. It has arrays of sensors for continuous updation of vital parameters and sensing technologies to detect obstacles, fire, magnetic field, metal and moisture. These detected data as well as data that need updation are continously streamed to a control room contaning the control unit. The control room situated at a safe distance of 500m away from the bigger and smaller robot combination and can be increased much more in a real time senario. The incoming data to the control unit would be monitored continuously by a trained technician with good knowledge of the robot system as well as good connectivity to a back-up unit in case of any emergency. The bigger robot also consists of a metallic arm acting as the attack unit, it has a missile launcher, distance approximator (target locator), a laser gun and a PIR sensor. Using the PIR sensor the system is capable of performing human detection. The attack unit mounted on the metallic arm can rotate 180 x 180 horizontal as well as vertical i.e., in up-down and clockwise- anticlockwise orientation to obtain precise target lockon. The Smaller robot system can be deployed in the case of non-mobility of the bigge robot system due to size constraints or environmental constraint. The flying smaller robot system would venture into the sky to capture real time video and live stream it to ensure surviellence of entire marked up area. Both bigger robot and the smaller robot are controlled wirelessly and have night vision cameras for the continuous live streaming, whose data will be sent to the control unit continuosly. The control unit has the receiver transmitter section for complete control of the system as well as display monitor for the live-streamed images.

(2). A website named “edgefx” has displayed many such military robots prototypes and projects but they have not disclosed the creators of these projects but have given us the access to explore them. Below we have mention some of the prototypes and projects from the website

(A) War Field Spying Robot with a Night Vision Wireless Camera by Android Applications War Field Spying Robot

This intelligent robot with wireless camera can be operated remotely for monitoring as well as controlling purpose. In the dark nights or dark places, this robot is capable of capturing videos, and then transmitting them remotely to a PC or TV by using wireless technology. This prototype of military robot is used in war fields to know about the status of the enemies around that area. It monitors the area with a camera by moving the camera to various positions or places remotely by an android application.

This war field spying robot uses microcontroller as the central processing unit, a Bluetooth modem to receive the command signal from the Android phone, an Android phone with a GUI application, a night vision wireless camera with remote area transmission capabilities, an IR LED for night vision lighting, a motor driver to drive a set of motors to control the vehicle movement and other miscellaneous associated components.

The user can monitor the war field area by controlling the movement of the vehicle by an Android application. When the user touches the position command in the Android application, the signal from the system is received remotely through a Bluetooth modem in the robot, and is further transferred to the microcontroller as shown in the figure.

The microcontroller is programmed in such a way that upon receiving corresponding signal from the Bluetooth, it sends the command signals to a motor driver that drives the set of motors to move the vehicle in the desired direction. And, also the wireless camera sends the video signals to a receiver station or unit, wirelessly, for monitoring purpose.

(B) Fire Fighting Robot Remotely Operated by Android Applications

Fire Fighting Robot

Fire-fighting robot is implemented as a fire engine to extinguish the fire. This type of robot is used in military as well in other sectors for extinguishing fire if it happens by accidents such as train accidents. The robotic vehicle consists of a water tank and a pump to sprinkle water.

Similar to the above project, this robot can also be controlled by using an Androidbased application for remote operation purpose, but – also requires another motor driver and a motor to operate the sprinkle arm in a desired direction and a pump to increase the pressure of water.

This robot also uses a microcontroller to control the overall operation. By receiving the command signals from the android application via a Bluetooth modem, the microcontroller adjusts the movement of the vehicle through a motor driver IC. Next, the sprinkle bow or arm position of the robot gets adjusted by another motor driver IC that receives commands from the Android mobile.

The microcontroller of this system is programmed in Keil software and operates the relay for the pump (for switching on and off), and also operates two motor driver ICs for moving the vehicle and the sprinkle arm.

(C) Pick-N-Place Robotic Arm and Movement Controlled by Android Wirelessly Pick-N-Place Robot

This military robot can safely handle bombs especially while catching them and avoids the danger of explosion or extra pressure on suspected object. It is equipped with a soft catching gripper for pick and place function. The remote operation is achieved by a Bluetooth modem via an Android phone based GUI applicationThis pick and place robot uses two motor driver ICs to control two sets of motors. One set of motors is used to control the vehicle's movement and the other set to operate the soft catching gripper, and this can be done by pressing the corresponding buttons on an Android application. After picking the object, the soft gripper holds the object and places it to another place by adjusting the vehicle movement.

The microcontroller's program manages the overall control operation, and the program can be modified by the user based on the requirement. Based on the signals from the Bluetooth, the microcontroller sends command signals to the motor driver ICs. In this system, there is a possibility to add a wireless camera for monitoring overall process.

(D) Voice Controlled Robotic Vehicle with Long Distance Speech Recognition This type of robotic vehicle's operation depends on the voice commands that are received by the speech recognition module. The command can be operated by both speech and push buttons controls. Such a type of Voice-controlled robotic vehicle comprises both transmitter and receiver circuits to achieve control objective.

Transmitting circuit consists of voice recognition module and push buttons as input controllers. By receiving these signals, the microcontroller sends these signals to an RF transmitter; from there the signals are transmitted to a receiver circuit.

The receiver circuit consists of a microcontroller which is placed inside the robotic vehicle and consists of devices like an RF receiver, a LASER module, a motor driver IC, and a set of motor, and so on.

Upon the voice command, speech recognition module sends the information to the microcontroller, and then the information is transmitted to the transmitter circuit.

After receiving the command signals from the transmitter circuit, the receiver transfers those signals to the microcontroller. And then, the microcontroller sends the signals to the motor driver to control the vehicle movement.

(E) Metal Detector Robotic Vehicle

This robot is useful to find landmines in the ground by sensing them while moving a vehicle ahead. A metal detector circuit is attached to this robotic vehicle to detect metal parts in the ground. The Remote operation of this vehicle to control the direction can be possible with an RFbased remote as transmitter that sends commanding signals to the receiver circuit.

This metal-detector robot is same as the voice-based vehicle that has been discussed above – in which the transmitting circuit consists of a push button control and an RF transmitter. However, an additional metal detector is added to the receiver circuit, here.

Whenever the vehicle encounters any metal part on its way, a resonance change occurs in the coil- as a result, the control signals move forward towards the microcontroller.

Upon receiving the signals from the detector, the microcontroller gives out a buzzing sound and also continuously interacts with the receiver to move the vehicle in a desired direction or path.

(4) Creator Abhijeet Deshmukh created a robo-soldier

This project is development of existing technologies for better use in military and industrial use to save as many as human lives possible. It is a remote controlled soldier which will detect and defuse bombs, surveillance on border, a robotic arm to pick-up objects. It will do tasks which are dangerous for humans. Motivation behind this project is to risk money instead of precious human lives

IV. CONCLUSION AND FUTURE WORK:

Technology changes day by day and this change continues at an increasing pace, specially for military technology and defence system, with its widespread, all terrorists research organization and development modules are affected positively.

In upcoming days robotic weapon systems, nano technologies of warfare, and vital weapon systems are going to intro themselves. The conclusion shows that although warfare technologies are now more effective, there is less warfare in the world—based on casualties as a percentage of population— than ever before. Armed conflict between developed and undeveloped states will remain predominantly asymmetric. It is not impossible to predict what technologies are going to develop in modern era. At last but not least I want to conclude my topic by the permission of respected honours. Thank you Jai Hind , Jai Bharat!

V. REFERENCES

[1]. MS. ASHIKA A. K., MS. BHAVYA S. N., MS. CHAITHRA C. P., SAMBHRAM INSTITUTE OF TECHNOLOGY, BENGALURU

[2]. edgefx website Link:- (https://www.edgefx.in/top-militaryrobots-project-ideas-for-real-timeapplications-in-2014) (a). War Field Spying Robot with a Night Vision Wireless Camera by Android Applications (b). Fire Fighting Robot Remotely Operated by Android Applications (c). Pick-N-Place Robotic Arm and Movement Controlled by Android Wirelessly (d). Voice Controlled Robotic Vehicle with Long Distance Speech Recognition (e). Metal Detector Robotic Vehicle

[3]. Abhijeet Deshmukh:- “Robo-soldier”

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Sentiment Analysis using Facial Expression

Sumit S. Maurya, Prajakta P. Kelkar, Umang K. Doshi, Prof. Swapnil Goje
School of Computer Science, MIT WPU, Pune, Maharashtra, India

ABSTRACT
Public sentiment is everything. It can never fail, and it can never be defeated. Only the people with the most public sentiment can truly excel. Face Detection has been around for ages. Sentiment analysis is the procedure to capture the emotion shown by a person's face from video or image. Modern AI systems can now mimic and gauge the expressions and actions shown by a person's face. This process can be useful for analyzing and determining intent or security threats. This paper scouts the feature extraction techniques that would help in the precise recognition of human emotion.

Keywords— Machine Learning, Image recognition, emotion analysis , emotion classification.

I. INTRODUCTION

Artificial Intelligence is now makes tremendous impact on emerging technologies like big data, robotics, and IoT. One of the application of artificial intelligence is Sentiment Analysis.
Sentiment Analysis is the use of natural language processing detecting the emotion or connotative notion of an individual. The facial expressions are helpful to gain an overview about their opinions and views.
Sentiment analysis and opinion mining is the field that measures people's opinions, emotions from large text data. It is studied in data mining. It is a method to automatically find the opinions of people. To automate the analysis of data, the area of Sentiment Analysis has emerged. Human opinion is always part of decision making and nowadays any organization knows about its products and services. Sentiment analysis is a process of gaining overviews from the opinion of users. Humans expresses their thoughts and emotions. It influences the way humans think, and how they act. Human perception and users' views have greater potential for discovery of knowledge and decision support. Sentiment analysis focuses on polarity of text and also detects feelings and emotions. The analysis contains various tasks like classification, subjective analysis, and extraction of opinions. Extraction of the opinion holder becomes very important because, some times, it is essential to know the author of the opinion.
Now a days computer systems, programs are more focused on the interaction of images. Places like entertainment, login- logout, counting number of peoples, and many more human- machine interface (HMI) where face emotion can be used. For detecting sadness , depression, anger issues and negative emotions

sentiment analysis is used.Even anger issues can be found out by this. With the help of sentiment analysis, many risks and psychological issues can be avoided..

II. LITERATURE REVIEW

The word “sentiments” views or opinions is always used or referred in the context foranalysis automation of the data to get a judgement when its evaluated or getting to the conclusionpart, this part of analytics was done in a paper published by “ Das and Chen”,2001[4].The same enhancement and conclusion were made after research andevaluationby“Turney”[5]and“Pangetal[6].

For sentiment analysis, classification based on polarity is the main job in opinion mining and also in sentiment analysis such as sarcasm(neutral), bad(negative) and good(positive) polarities in the opinion[10].

In the paper [1] they had tried to get the best approach towards sentiment analysis. Among the three levels of sen- timent analysis, aspect-based sentiment analysis is the most detailed than sentence-based and document-based sentiment analysis. [1]

Based on the paper in [9], it is claimed that the Lexicon- based approach outperforms the Supervised Machine Learning approach not only in terms of Accuracy, Precision, Recall and F-measure but are also seen in economy of time and efforts used.

According to paper [2], it is found that sentiment classifiers are severely dependent on domains. It is also found to increase the efficiency of the classification performance of sentiments many classification algorithms and different types of features where combined. This also help to surpass the drawbacks.

Sentiment analysis of online review from social media or surveys has taken a drastic increase in its position as anemerg- ing research. Which is taking advantage of the achievements in areas such as text mining, customer feedback analysis, natural language processing, market research, web mining,and machine learning.[3]

Mining from the opinions to establish a analysis of sentiments is not in itself a new research domain or you can say theme. According to TheContent Analysis Guidebook Sage(Neuendorf, K. A. 2002) from 1980 to 2002 there had atleast 6 times increase in Automated methods for content analysis [11]. The theme for the research is established from the disciplines which are based on well established computer science. Such as AI(Artificial Intelligence), NLP(Natural Language Processing), ML(Machine Learning), Automated Content AnalysisApplications, etc. So as per Pang and Lee-2008, we are seeing a growing awareness of many problems as well as many opportunities and there have been subsequently many number of papers published on the topic since 2001 [5].One can say the new thing for today is the major growth of quantity of unstructured data. This is mainly because of adaption and adoption of social media that is readily available to get trained for model with the help of machine learning algorithms. We can get sentiment and opinions by nature reflects on social media content.To this in past analysis was totally focus on identifying topics. (Vaithyanathan, Pang and Lee 2002). Thus we can say that the processing is dealing with more tedious and complex natural language processing, which is due to drastic increase in the volume of data which is available widely and more complex concepts to analyze. It is seen in recent years there has been a decrease in the semantic-based application, and a major movement is seen towards use of statistics and visualization. Using of these visualization and creating dashboard for the same is in trend now. Automated content analysis with proper algorithms is now days becoming a data-intensive science where new things arecomingupinafastway.

Major work in this particular area is carried out by Paul Ekman(Psychologist)[13]. He said that or always had an argument over the facial expression principles. He stated that facial expression are independent and innate from cultural influence. This method helped to create a recognition system for emotions solely based on the information available on face virtually.

The facial Action Coding System is developed by Ekman, which helps to reduce any emotions to an isolated movement of the facial muscles.[14]. For example, an emotion like joy or happiness can be interpreted as a contraction of the orbital portion of the orbicular muscle in combination with the greater zygomatic muscle. This type of movement changes the relative position of some points of the face such as the corner of the lips or the edges of the eyebrows. So nowadays that are easily detected by new technologies.

In the past decade, a considerable amount of research has been done inacademia[7],[8]. Numerous commercialcompanies provide emotion miningservices.

III. IMPLEMENTATION

Creating Dataset:

We are collecting data using google form and we had also used data from kraggle.com where we had divided photos and images into 7 types of folderslike anger, Hatred, Panic/terror, happiness, sadness, Shock, Plain. We had kept each emotion's images in each folder. After that, we had created open CVV in image cascade classifiers with the help of that we are storing images. We are converting the colored image to a black and white form. Then after this, we had collected this whole data in opencv. So basically to train model we had to get data from kraggle.com. Then with the help of data which we had collected the algorithm is tested.

Dataset :

Train: To train data we had used following count of images.

Categories	Count
Anger	4950
Hatred	550
Panic/terror	5121
Happiness	8996
Sadness	6070
Shock	6190
Plain	4010
Total	35887

Creating Solution :

We are using python, scikitplot, tensorflow, seaborn, matplotlib, sklearn and keras to train the data.

After collecting data and creating datasets we are training data with the help of above libraries . To train data we had given integer values to a particular expression like

0 for anger,

1 for Hatred,

2 for Panic/terror,

3 for happiness,

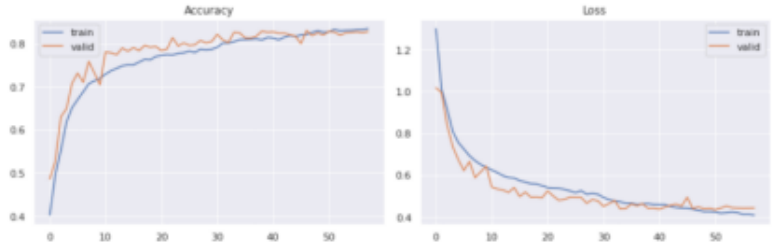
4 for sadness,

5 for Shock,

6 for Plain.

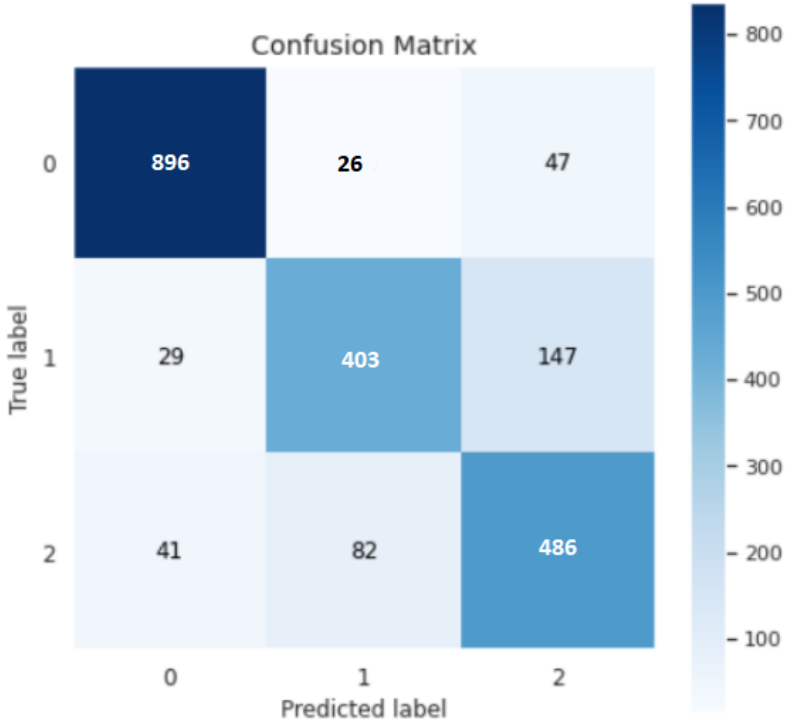
With the help of the seaborn library, we had generated each type of emotion. We had made data compatible for neural networks using the lambda function. For each type of emotion, we had trained with the help of deep learning. With the help of optimizers like Adam and nadam, we had processed the data and then trained the same. So now to work in a simplistic way we planned to 1st try to train and test with only happiness, sadness and plain or simple emotions. So these emotions data had been made compatible with neural networks. The size of array come as (21264,48,48,1).

We had calculated the accuracy of the data unavoidable.



Now to test the data we had used again cascades to get the real-time data from users. We had converted this data in open cv. So as we got users open cv we are comparing open cv data with trained data. Using mapper we had given values as mentioned above for each expression. So whatever the emotions of the user it will show in that formatonly.

Confusion Matrix- So from the below matrix we can see that the model is working pretty much good. Best results are obtained for Happiness. While for the rest two either the data is less or we can say that the rest too are pretty much tuf to guess for the neural networks.



After Testing with random image data we got output as below

IV. RESULT

The test data output is in the following format.

We are successfully able to differ the images and getting the outputs.

V. CONCLUSION

We can say overall till now many efforts have been made to find different moods on face of the user.
With the motivation to explore and do something in sentiments from the emotions of human face this paper is drafted. To begin with few models and now to have psychological motivation to create a model for facial behavior analysis in terms of emotions, which is anyhow going to be a great asset for the future automation.
The facial emotion analysis algorithms overall gives an optimized values forunits like nose, eyebrow, lip , eye etc . With the help of these values which is then inputted to the neural network which in return give us emotions.
The model had given a 80% accuracy for the testing data.Though emotions were able to identified . This model can have many application in real time environment. Thus many things can be done for the improvement and optimization of the algorithm.
For the future scope and enhancing the current model many applications can be generated such as changing the environment according to facial expression.

VI. REFERENCES

[1]. SuadAlhojely , ”Sentiment Analysis and Opinion Mining: A Survey”,Volume 150-No 6,September 2016.
[2]. G.Vinodhini, RM.Chandrasekaran, “SentimentAnalysis and Opinion Mining: A Survey”, Volume 2, Issue 6, June 2012.
[3]. ”Sentiment Analysis: A Literature Review” by - ZHU Nanli, ZOU Ping, Li Weiguo, CHENG Meng
[4]. Alec Go, Richa Bhayani, and Lei Huang. Twitter sentiment classification using distant supervision,Stanford, 2009.
[5]. B.Pang and L. Lee. 2004. A sentimental education: Sentiment analysis usingsubjectivity summarization emotions based on minimum cuts.ACL.
[6]. Alexander Pak and Patrick Paroubek. 2010. Twitter as a corpus for sentiment analysis and opinion mining.Proceedings of LREC.
[7]. Liu, B. Sentiment analysis and subjectivity. InHandbook of NaturalLanguageProcessing, Second Edition, N. Indurkhya and F.J. Damerau, Editors. 2010.
[8]. Pang, B. and L. Lee. Opinion mining and sentimentanalysis. Foundations andTrendsin Information Retrieval, 2(1-2): p. 1-135, 2008.
[9]. N. Mukhtar, M. A. Khan and N. Chiragh, “Urdu Sentiment Analysis,” Telematics and Informatics, Vol. 35, no. 8, pp. 2173-2183,2018.
[10]. "A lexicon-based method to search for extreme opinions",S. Almatarneh and P. Gamallo, vol. 13, no. 5, pp.19,2018.
[11]. The Content Analysis Guidebook “Kimberly A. Neuendorf” Published: 2017, vol.2 NC27513-2414, 2002.
[12]. Victor M. Álvarez, Ramiro Velázquez, Sebastián Gutiérrez“A Method for Facial Emotion Recognition Based on Interest Points”10.1109/RICE.2018.8509055Published in: 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE)

[13]. P. Ekman and W. Friesen, “Constants across cultures in the face and emotion”, Journal of Personality and Social Psychology, 17(2), pp. 124- 129, 1971.

[14]. P. Ekman and W. Friesen, “Facial Action Coding System: A technique for the measurement of facial movement”,Consulting Psychologists Press, Palo Alto, USA, 1978.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Prediction of Healthcare Quality Using Sentiment Analysis

Dnyaneshwar Panchal, Mahesh Shelke, Sachin Deshmukh, Seema Kawathekar
Department of Computer Science and I.T., Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India

ABSTRACT
Hospital is the most important service for human health. Doctors and staff are playing a major role in hospitals. Many Patients' treatment is very carefully handled by hospital staff. Some hospitals have a very bad record about their service. Many times, patients are confused to select the desired hospital. Patients need some previous information about the hospital, so that patient can choose the desired Healthcare center. To search previous patients' feedback, need to visit online healthcare websites, blogs, and related online social sites. Information about different hospitals is provided by online web services. The Hospital list is sorted with the detailed record. On these websites, users can search for various patients, experienced feedback about specific healthcare centers. This research work predicts hospital and their service quality, for that aspect sentiment analysis method, is used. The Sentiment analysis technique nowadays is very popular to predict results from text data.

Keywords— Patient, Doctor, Sentiment analysis, Service, Hospital, Healthcare, Aspect-Sentiment, Feedback.

I. INTRODUCTION

As we all human beings live in the 21st century, every sector provides online services for their business improvement. The Healthcare sector is also improved, patients can access needful information from the internet and healthcare-related websites.

The patient is a customer of healthcare, the patient is paying for healthcare service. If the patient is not getting the required quality service from the hospital, he must have the right to complain about the particular hospital. Many patients which are internet users can share their experience about a healthcare center.

Experienced patient feedback text data available on healthcare-related websites. i.e., comments posted on healthcare websites are collected. The Healthcare website contains information about various doctors followed by patient feedback. After visiting these websites users can read and analyze the feedback of the Physician, after reading this feedback, patients can decide to choose the doctor for their treatment.

In this work first collect the text i.e. comments (feedback) posted by patients, after data collection different procedures are carried out on collected text. I.e. Preprocessing, Sentiment analysis, Aspect Sentiment, categorization algorithms, and many statistical processes are used. After that, predict an estimated result based on

the patient's preference for a specific qualified hospital to the reference, as in [1]. To predict the result a technique is used known as the Sentiment Analysis technique explained as follows.

A. Sentiment Analysis

The sentiment analysis or opinion mining states an analysis of text data of the approach of focus concerning a particular subject. This approach can be a decision, a sentimental state, or the proposed sensitive statement. Commonly, sentiment analysis is implemented based on natural language processing, the analysis of computational linguistics, and text. Data can be gathered from different websites.

Sentiment analysis of text data using specific text, (Examples: structured maintains text semantics, another example is social networks i.e., tweets, comments, etc.), where the text is in an unstructured format.

Sentiment analysis has various levels to be analyzed. First document level, second sentence level, and aspect level. We see one by one as follows.

1) Document Level: Document-level sentiment analysis finds the entire document's opinion about a particular product or service mentioned in the document. The opinions are positive, negative, or neutral. At this level, it can find only single product opinions not multiple since it is called document-level sentiment analysis.
2) Sentence Level: Sentence level sentiment analysis can find the opinion of a single sentence about a product or service, not multiple sentences once at a time. The opinion presented as positive, negative, and neutral, neutral means neither positive nor negative. This level of analysis is included in subjectivity classification, subjectivity means which shows opinions and views. Objectivity shows original information from sentences.

- For example, "he bought medicine from a medical but it was expiry dated".

3) Feature/Aspect Level: Feature level or aspect sentiment analysis which finds the opinion about a particular feature or aspect from a text. It means what exactly patient negative or positive about a service or healthcare.

- For example, "hospital cleanness is lovely but the staff is impolite".
- In the above example cleanness and staff are two different aspects, expressing cleanness positive but staff negative.
- Hospital patients reacting different opinions about different aspects. So hare aspect level is analyzed more deeply about a sentence to the reference, as in [2]. The Diagram of Sentiment analysis is shown in Fig. I.

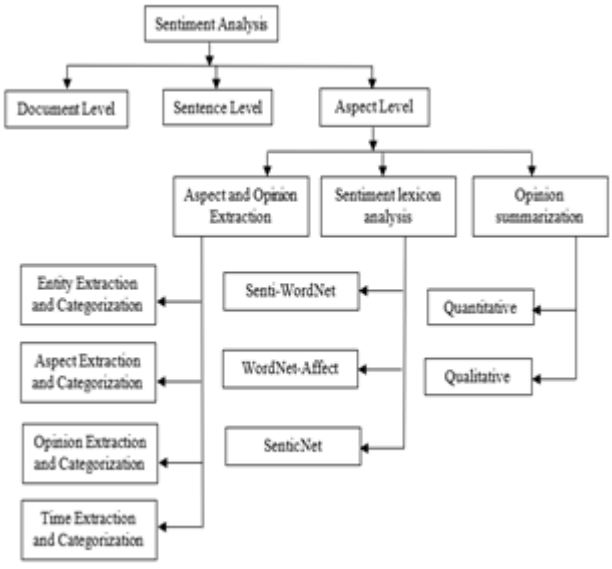


Figure 1. Sentiment Analysis.

II. STATEMENT OF THE PROBLEM

There are many complaints about private and government hospitals for their service, which they are given by patients. To find a qualified, genuine hospital we need to know the experienced patients' feedback, the previous record of a specific healthcare center. So that we can quickly select the best hospital for patients' treatment.
Some Healthcare centers are providing good quality services, so need to analyze both quality services and services having negative records about their healthcare center.

III. LITERATURE SURVEY

Frequent sicknesses are treated with regular medicine i.e., cold, cough, fever, etc. healthcare is an individual service, it is depended on the available resources for treatment. Various patients have different experiences with healthcare.
Preferably, high-quality service would be chosen but there are many issues, some anonymous, this can be the effect on patients' reaction on the healthcare service provider. Patient feedbacks are available in the form of positive, negative, and neutral. Different types of techniques are available to collect and manage the feedback of patients of the healthcare service provider.
Publicly funded health service providers such as NHS are playing a major role in patient feedback. The patient feedback comments are actually important to evaluate and increase the healthcare service quality. It helps to enhance the confidence of healthcare staff to provide careful service.
In 2012, the Prime Minister of the United Kingdom declare a scheme to develop patient care in England i.e., the Friends and Family Test (FFT). This was an easy metric, a particular query that was investigated to find out whether a patient would suggest the health service to their friends and family if they necessary related care. NHS was implemented this test by their different departments together with, maternity wards, dentists, accident and emergency departments in all the UK. Five million reactions are be given in April 2013, by February 2015 to FFT (NHS England, 2015). This is very a much smaller number of responses as compared to the population of the UK, NHS at that time, this is sufficient feedback comments to analyze healthcare service quality.
The reply that was pulled together on a five-point scale how likely a patient was to advise the service, ranging from very unlikely to very likely. Given the resulting proposal advice, some organizations investigate follow-up queries to find out further details related to what in particular a patient liked and disliked, and had they some suggestions to the reference number, as in [3].

A. Healthcare Sector and Sentiment Analysis

Where follow-up questions were asked and get together, some organizations used sentiment analysis software to recognize trends in the resulting verbatim feedback. This was not used by all organizations though, as certainly composed replies using documents like feedback, the essential physical record before analyzing the feedback. The handwritten text requires more time, need many writers to interpret and manually input the word comments into the database, this incomplete the ability for the program to analyze several comments.
The review archive of the FFT (NHS Britain, 2014) studied that at an important level feeling analysis was being treated with regard, as the suitability and precision of the techniques in the clinical area had not been shown. This is reasonable, given the honestly restricted work accomplished by analyzing the arrangement of valuation in

reports from the clinical sector. Regardless-of, as a society, contributes in a consistently expanding advanced way, and with the desire that the NHS will encounter a development in the number of online remarks, the assignment of physically examining each word-to-word thing of input turns out to be increasingly additionally testing to the reference number, as in [4].

B. Healthcare and Aspect based Sentiment Analysis

Every human being requires the healthcare sector to maintain their health. Aspect sentiment analysis is a sort of sentiment analysis that examines the characteristics of a specific service or product. As we previously discussed, hare sentiment analysis is applied at several levels. The deep analysis leads to aspect sentiment analysis, which is the next level. Patients leave a variety of comments about healthcare facilities on the internet. In single feedback, patients discuss various aspects of healthcare, some of which are positive and some of which are unfavorable. So, for a more in-depth study, break the sentence down and focus on specific qualities mentioned by the patient throughout the full feedback or sentence. Aspect sentiment analysis can examine the full statement, break it down, and determine whether the service is positive or negative.

Using machine learning to analyze large amounts of text regarding healthcare is difficult. Although difficult, aspect-based sentiment analysis meets this criterion. To understand healthcare features, consider the following:

Doctor, treatment, personnel, cleanliness, medicine, infrastructure, cost, medical service, ambulance, diagnostic, and so on.

These characteristics are clearly noted by the patient when reading the patient comments. Patients want to feel good about their health. Machine learning must be trained using the text analysis method to extract aspects of polarity. It is accurately performed using aspect-based sentiment analysis. It displays a summary of all patient input while also extracting certain characteristics and detailed information using feedback polarity. The healthcare quality and current state of healthcare centers or a physician can be determined using aspect-based sentiment analysis to the reference number, as in [5].

IV. PROPOSED METHOD

In this work, we propose a model predicting aspect-wise sentiment score, Data collected from the website www.ratemds.com contains moderate data of broad scope of specialists. This website has various physicians and specialists in the clinical field are available with their detailed information for example name, address, degree, and specialty in the healthcare sector. Under this, the patient feedback system is facilitated. Where visited patient shares their experience with the particular physician to the reference number, as in.

A. Data collection

Data is extracted from the www.ratemds.com website, this website related to healthcare and physicians. Near about 69 various physicians are chosen. We eliminated the Personal information of the doctor for keeping the privacy of identity. All Physicians are selected from various cities in India. Maximum cities from Maharashtra state in India.

This dataset comprises over 300 English sentences of various 69 physicians, where some doctors' feedback comments are very less in number and some are more than fifteen to forty, some feedbacks are large sentences and some are 1 or 2 sentences. www.ratemds.com original dataset to add remarks for aspect words occurring in

sentences, aspect term polarities, coarse aspect categories, and overall sentence polarities. Also fixed several problems in the original dataset.

The site permits patients to rank their physician's staff, trustworthiness, supportiveness, and information on a score of more than zero; one star means "actual small in worth" while a score of five stars determines that the specialist, "great worth full service." Similarly, the survey contains a remarks section that allows the patients to talk about the specific parts of their consideration, which they liked or disliked to the reference number, as in [6]. As shown in Fig. 2, this figure shows the entire procedure to decide aspect-wise polarity.

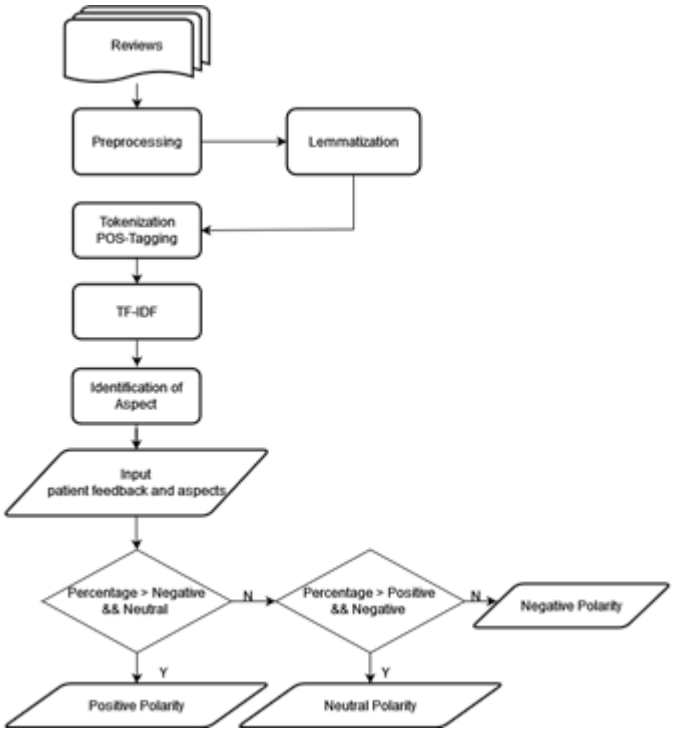


Figure 2. The Diagram to find the Aspect Sentiment score and classification.

B. Preprocessing

As data collection is completed then preprocessing is needed, in preprocessing some cleaning operations are needed to analyze the data i.e. Removing HTML tags, stop words, punctuation, white spaces, URL, and making lowercase from a data file.

A huge data supervision environment is used for preprocessing, Text data is preprocessed through the R tool. I.e. R language tool. Once preprocessing is completed then text normalization is used to normalize the data to the reference number, as in [7].

C. Normalization

- POS tagging, Lemmatization, tokenization, TF-IDF, are the processes to perform normalization. To perform these operations an R Tool is used.
- POS-Tagging: Part of Speech tagging is used for grammatical rules of words of the sentence by assigning specific meaning of word or sentence.
- E.g. noun, adjective, Personal Pronoun, Determiner, adverb, verb, etc. tag as NN, JJ, PRP, DT, RB, VBZ, etc.) To distinct words.
- Term Frequency (TF): This is a quantity based on the number of times a particular term appears in the data source.

- Inverse Document Frequency (IDF): is a metric for determining how infrequent a word is thru documents to the reference number, as in [8].

D. Aspect Based Sentiment Analysis

Text analysis of healthcare centers is significant since various aspects of healthcare are linked to the overall facility. The entity of a healthcare center include,

e.g., healthcare, hospitals, refers to entire hospitals. Features of the Healthcare center refer to a doctor, diagnosis, service, cleanliness, medicine, cost, and so on.

An aspect-by-aspect analysis is critical because if the healthcare infrastructure is good but the physician isn't, the entire infrastructure will be unusual. In this task, aspects are extracted and analyzed. The following subtasks are included in the task.

1) Extraction of Aspects

Extract all of the various aspect terms contained in a group of phrases with well before entities (e.g., Hospital) and produce a list. The word 'aspect term' narrates to a feature of the objective unit.

"Brilliant doctor great knowledge diagnosis",

In the above sentence the Aspects are: '*doctor'*, and '*diagnosis'* two aspects, as extracted aspect by using tokenization along with part of speech tagging (POS).

Aspect terms with several words (for example, "*homeopath doctor*") should be treated as single terms (for example, the sole aspect term in "excellent homeopath doctor for infectious conditions" is "*homeopathic doctor*," which is a single term with multiple words).

Due to the dissimilar inconsistencies of aspects stated above, aspect extraction is the most difficult portion of the aspect-based sentiment analysis. For aspect extraction, unsupervised approaches are favored since they search the entire domain for aspects rather than guiding them to a certain sort of aspect. The known components of the supervised technique will be identified with great accuracy, but any unknown aspects will be ignored. Aspect extraction is divided into two stages,

2) Aspect Identification

The process of recognizing nouns and noun phrases as relevant aspects is known as aspect identification. The relevant aspects are those that are most likely to produce aspects. The frequency of occurrence or some matching patterns in which they may occur support the aspect identification process.

E.g. "……of the diagnosis" or "diagnosis by….." are two examples of diagnosis aspects. They're known as factors, and this method of identifying aspects is known as a frequency-relation-based method.

As the name implies, it generates a huge list of relevant characteristics based on frequency, then filters out those that aren't found in the precise relation pattern. The presence of a sentiment word together with a low-frequency aspect is added to the list as an indication of being an aspect. The probabilistic subject prototypes extract features based on the co-occurrence of words.

Multi-term aspects are created by making sets of relevant aspects if they appear together in a sentence from the list of aspects designated as relevant aspects. Only the order in which the words appeared in the sentence determines the formation of sets. The created multi-term aspects are also included in the list.

3) Polarity of Aspect Term

Evaluate whether the polarity of every aspect term in a sentence is positive, negative, or neutral for an includes specific aspect terms.

Patient feedback 'excellent doctor awesome treatment'
Polarity 'doctor- positive', 'treatment- positive'
Patient Feedback 'saddened management care information moving patients freshman doctors arriving min patient overview clear treatment upset'
Polarity 'management-negative'
Patient feedback 'doctor available anytime'
Polarity 'doctor- neutral' to the reference number, as in [9].

V. RESULTS AND DISCUSSIONS

A. Aspect-Based-Sentiment-Score extraction

Doctor D9's information is provided in Table I AND Table II, D9 is chosen as an example of obtaining an aspect-wise sentiment score out of a total of 69 physicians.
Table I shows the inclusion of Doctor Number, city, preprocessed patient feedback and Table II shows the aspects, feedback date, and aspect sentiment score of Table I. Table I and Table II are split into two tables.
A doctor's serial number is D9. Doctors' identities are kept hidden in order to protect their privacy. The aspect sentiment score extraction program is written in Python, and the result is a percentage of aspect-wise sentiment score, as given in Table II.
Aspect sentiment score is calculated as first the inputs is given as single patient feedback i.e. "preprocessed patient feedback", like the sentence, Table I".
Input aspects as, "aspect 1, aspect 2, and aspect 3", i.e. diagnosis, treatment, and appointment, as given in Table II. The python program is used to accomplish this task, and the extracted aspect-based sentiment scores are displayed in Table II, Aspect section, namely Aspect1, Aspect2, and Aspect3 to the reference number, as in [10].

TABLE I. DOCTOR D9 FEEDBACK INFORMATION

Dr. No	City	Preprocessed Patient Feedback	Feedback Date
D9	Pune	humble soft-spoken point diagnosis happy line treatment lost weight thyroid control sir pre-appointment preferred	6/3/2019
		honest suggestion appropriate diagnosis uncle spent time questions relating diagnosis undue tests doctor options medication depending suit	6/3/2019
		doctor following advice results experienced treatments highly recommend	8/17/2018

TABLE II. DOCTOR D9 FEEDBACK INFORMATION TWO

Aspects		
Aspect1	**Aspect2**	**Aspect3**
Diagnosis [0.001 0.003 **0.996**]	treatment [0.106 **0.594** 0.301]	appointment [**0.94** 0.013 0.047]
diagnosis [0.015 0.002 **0.982**]	doctor [**0.958** 0.008 0.034]	medication [**0.993** 0.003 0.004]
doctor [0.002 0.001 **0.997**]	advice [0.051 0.003 **0.946**]	treatment [0. 0.001 **0.999**]

B. Aspect Sentiment Polarity

Aspect sentiment polarity is shown as positive, negative, and neutral.

1) The sentence as input: following Table III Showing patient feedback as a sentence, this feedback posted by the experienced patient about Doctor D9. This commented sentence is given as input to the python program, this python program is about aspect-based sentiment analysis, and the program can analyze the aspect contained in this sentence.
2) Aspect as input: Table no III shows some aspects which are given input to the python program followed by a feedback sentence, all aspects assigned to a variable.

TABLE III. SENTENCE AND ASPECT AS INPUT OF D9

Dr. No.	Input		
D9	Sentence	Aspect	Date
	humble soft spoken point diagnosis happy line treatment lost weight thyroid control sir pre appointment preferred	diagnosis, treatment, appointment	6/3/2019
	honest suggestion appropriate diagnosis uncle spent time questions relating diagnosis undue tests doctor options medication depending suit	diagnosis, doctor, medication	6/3/2019
	doctor following advice results experienced treatments highly recommend	doctor, advice, treatment	8/17/2018

"Positive," "negative," and "neutral" are the three potential values for the polarity field. Table IV displays the results of aspects 1, 2, and 3 along with sentiment scores for each aspect. The highest polarity is colored, with the first value being neutral (Blue Color), the second being negative (Green Color), and the third being positive (Red Color).

Aspect polarity has the highest point percentage among these values, as indicated in Table IV. The positive polarity of 0.996 is higher than the neutral polarity of 0.001 and the negative polarity of 0.003. As a result, the aspect 'Diagnosis' on 6/3/2019 is a positive aspect of doctor D9's sentence one. In the same way, the second and third sentence aspects are evaluated in Table IV.

TABLE IV. ASPECT WISE OUTPUT WITH POLARITY D9

Dr. No	Date	Aspect	Neutral	Negative	Positive
D9	6/3/2019	Diagnosis	0.001	0.003	0.996
	6/3/2019	Diagnosis	0.015	0.002	0.982
	6/3/2019	Treatment	0.106	0.594	0.301
	8/17/2018	Treatment	0	0.001	0.999

Graphical representations of Table IV are shown in the following Fig. 3. Graph 1. The aspects are Diagnosis and Treatment. As per the graph positive polarity is found maximum as compared with the neutral and negative polarity of Doctor D9. The graph clearly shows the difference in aspect sentiment score when comparing dates. See the same aspects on various dates.

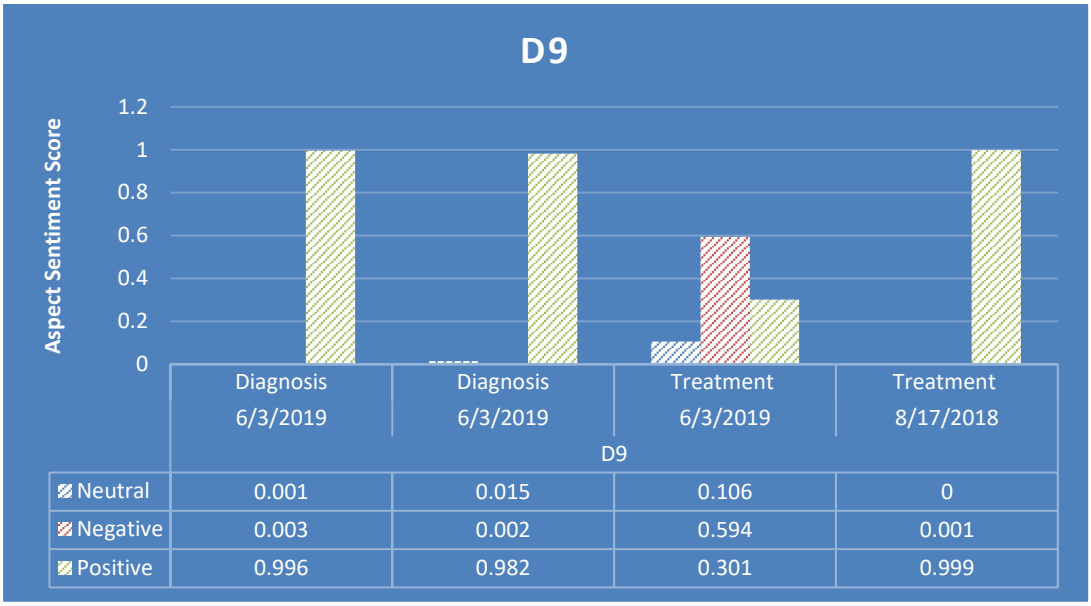


Figure 3. Graphical Representation of TABLE IV.

VI. CONCLUSIONS AND FUTURE SCOPE

The research article examines and evaluates the quality of healthcare services in different aspects. Aspect-based sentiment analysis is used to examine the features of a healthcare facility, and it is observed that the healthcare sector has a number of different factors, such as specialists in various human diseases. Heart surgeons, gynecologists, psychiatrists, bone surgeons, and so on are examples of specialization.

Other considerations include the healthcare center's facilities, hospital staff service, medicine quality, cleanliness, pricing, and schedule. These are important aspects of a healthcare facility, and attention must be paid to each one so that the facility's overall quality may be predicted.

This research work focuses on extracting aspect sentiment scores and analyzing them date-by-date, it is found that the service of healthcare regularly changes as time passes.

In the future, this work has more aspects of healthcare center and perform classification operations so that more accuracy we can find for better improvement. Various classification technique in the future has a scope to analyze more results.

VII. REFERENCES

[1]. D. H. Kristina, L. M. Danielle, D. Chrissy, MS, W. C. Wendy, M. Conway, "Understanding patient satisfaction with received healthcare services: A natural language processing approach," Annual Symposium proceedings / AMIA Symposium, pp. 524-533, 2016.

[2]. R. S. Jagdale, S. S. Deshmukh, "Sentiment Classification on Twitter and Zomato Dataset Using Supervised Learning Algorithms," International Conference on Smart Innovations in Design, Environment, Management, Planning, and Computing (ICSIDEMPC), pp. 330-334, 2020.

[3]. P. John, B. Anne-Marie, "Harnessing patient feedback data: A challenge for policy and service improvement," Digital Health, vol. 1, pp. 1-3, 2015.

[4]. S. PHILLIP, Sentiment analysis of patient feedback. School of Computer Science College of Engineering and the Physical Sciences University of Birmingham, pp. 1-271, 2015.

[5]. B. Ankita, K. Niranjan, "Aspect Based Sentiment Analysis Using Attribute Extraction of Hospital Reviews," New Generation Computing, Ohmsha, Springer, vol. 27, pp. 1-20, October 2021.

[6]. M. H. Anthony, U. Maria, "Using sentiment analysis to review patient satisfaction data located on the internet," Journal of Health Organization and Management, vol. 29 issue 2, pp. 221 – 233, August 2013.

[7]. D. S. Panchal, S. S. Kawathekar, S. N. Deshmukh, "Sentiment Analysis of Healthcare Quality, "International Journal of Innovative Technology and Exploring Engineering (IJITEE)," vol. 9, issue 3, pp. 3369-3376, January 2020.

[8]. S. Milan, H. Jan, S. Jana ˇ a´, "UDPipe: Trainable Pipeline for Processing CoNLL-U Files Performing Tokenization, Morphological Analysis, POS Tagging, and Parsing," Proceedings of the Tenth International Conference on Language Resources and Evaluation ({LREC}', pp. 4290-4297, May 2016.

[9]. S. Josef, B. Toma´s, K. Michal, "Aspect-Level Sentiment Analysis in Czech," Proceedings of the 5th Workshop on Computational Approaches to Subjectivity, Sentiment and Social Media Analysis," pp. 24-30, June 2014.

[10]. R. Rafał, "Do You Trust in Aspect-BasedSentimentAnalysis? Testing and Explaining Model Behaviors," Ebook_Explainable Sentiment Analysis, pp. 1-15, 2021.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Detection of Type 2 Diabetes Mellitus Using Machine Learning

Salliah Shafi Bhat[1], Prof. Dr. Gufran Ahmad Ansari[2], Prof. Dr. Venkatesan Selvam[3]

[1]Department of Computer Science, B.S Abdur Rahman Crescent Institute of Science & Technology, Tamil Nadu, India

[2]Department of Computer Science, MIT World Peace University (MIT-WPU), Pune, Maharashtra, India

[3]Department of Computer Science, B.S Abdur Rahman Crescent Institute of Science & Technology, Tamil Nadu, India

ABSTRACT

Type 2 Diabetes Mellitus (T2DM) is a medical disease in which the insulin produced by the pancreas does not work properly. Throughout India diabetes affects more than 30 million people with millions more at danger. To avoid diabetes and its related health problems early treatment are necessary. The focus of this research is to determine a patient's risk of diabetes based on their lifestyle and family history. Different Machine Learning algorithms were used to predict the risk of T2DM because these algorithms are extremely accurate which is essential in the healthcare profession. Individuals can self-assess their diabetes risk once the model has been trained with high precision. Machine Learning was used in this study to detect the existence of T2DM in patients. Several classification algorithms were used such as the Support Vector Machine, Random Forest and XGBoost algorithms were computed to determine the impact of features on the Machine Learning model's performance. Random Forest has the highest accuracy better execution on several criteria such as accuracy, precision, recall.

Keywords— Type 2 Diabetes Mellitus, Machine Learning, Support Vector Machine, Random Forest, and XGBoost algorithms.

I. INTRODUCTION

Diabetes Mellitus (DM) is a long-term condition characterized by the inability of the body to digest sugar. Early diagnosis of the illness lowers medical costs and reduces the risk of people having more serious health concerns [1]. Diabetes, often known as (DM), is a group of metabolic illnesses characterized by continually elevated blood glucose levels. High blood sugar is characterized by excessive excretion, frequent thirst, and a rise in hunger. Diabetes develops when the pancreas is unable to produce enough insulin or when the body's cells and tissues fail to utilize the insulin that is created [2]. Excessive urination, continuous thirst and hunger are all signs of high blood sugar. When the pancreas is unable to produce enough insulin or when the cells and tissues in the body fail to use the insulin diabetes develops [3]. Diabetes Mellitus is divided into two groups. Insulin-subordinate Diabetes Mellitus is a kind of diabetes characterized by the pancreas releasing less insulin than the body requires

(IDDM). People with type 1 diabetes require insulin injections to compensate for their pancreas' decreased insulin output [4]. Children under the age of 20 are affected by Type 1 Porizine Disorder. Glucose for type 1 diabetes has resulted in lifelong breaks for some people. Hypoglycemic drug resistance is the starting point for type 2 diabetes. This is a condition in which cells do not respond well to hypoglycemic medications [5]. People who have high BMI or who live a sedentary lifestyle are more likely to get type 2 diabetes. Hypoglycemia is a serious complication in people with Type 2 diabetes and it has been associated to higher morbidity, death and healthcare expenditures. Hypoglycemia is also a major impediment to getting the most out of glycemic control. Individuals who take regular self-monitored blood glucose (SMBG) readings or use continuous glucose monitors may be able to employ statistical techniques to predict hypoglycemia [6]. The mean standard deviation, coefficient of variation, and glucose distribution pattern can all be used to calculate the risk of hypoglycemia. The dataset was subjected to exploratory data analysis as well as various Machine Learning Techniques in this study (Support Vector Classifier, Random Forest and XGBoost) have been used to evaluate whether or not the patient will develop type 2 diabetic mellitus. The effect of features in the development of the Machine Learning model has been established utilizing feature significance scores.

Material

a) **Dataset:** The categorization challenge is being worked by the Machine Learning. Most scholars have used the Pima Indian Dataset (PIMA) to measure classification performance. It can be obtained in the UCI machine learning dataset. There are 369 records in the data set.

b) **Risk Factors:** The parameters that contribute to the development of diabetes are listed below.

Age: Diabetes strikes Indians earlier than it does the rest of the world's population. Early symptoms allows for the development of long-term diabetes problems. Diabetes becomes more common as people get older.

Family history: Diabetes is more likely to occur if you have a family history of the disease Diabetes has a significant prevalence including first relatives.

Lifestyle: Diabetes is caused by a deskbound lifestyle which is an independent factor.

Obesity: Obesity and Diabetics have a close relationship. BMI (Body Mass Index) rises as weight r

Stress: Physical and mental stress as well as lifestyle changes have an impact on the occurrence of Diabetics in those with a significant genetic heritage. The main Contribution of this paper is author focused on Proposed Framework of Type 2 Diabetes.

The subsequent sections of this study are arranged as section II describes about the Literature Review, Section III is about the Proposed Framework for Type2 Diabetes. Section IVdiscusses about the Result. Finally Section V is followed by Conclusion and Future Scope.

II. LITERATURE REVIEW

Many researchers use the Machine Learning Technique (MLT) to extract data from current medical statistics in the diabetic field. Artificial Neural Network, Linear Regression, and J 48 techniques were used to forecast diabetic illness using globe datasets collected in sequence by scattered communication patterns [7]. In the medicinal field Machine Learning algorithms are used to make an accurate diagnosis. The hyper-plane is discovered using a MLT resulting in a knowledgeable and accurate classification [8]. Diabetes prediction using several Machine Learning Methodologies aims to improve the accuracy of a system that predicts the diabetic risk level of a person using

four Machine Learning Algorithms: DT, Artificial Neural Network, Navies Bayes, and Support Vector Machine. The model yields 85 percent for DT, 77 percent for Nave Bayes, 77.3 percent for SVM, and 76 percent for ANN. The use of Principal Component Analysis to research Machine Learning methods such as Support Vector Machine, Nave Bayes, Decision Tree, and PCA for disease prediction [9]. Predicting diabetes in Pima Indians using Machine Learning (ML) classifiers. The research depended on a 768-patient Pima Indian diabetes dataset (PIDD) was used. A comparison of four different ML classifiers was conducted using knowledge discovery operations: Nave Bayes (NB), J48, Logistic Regression (LR), and Random Forest (RF). When rating the algorithms, other factors such as precision, f1-score, recall, and AUC were considered [10]. LR had an AUC of 83 percent, RF had an AUC of 82 percent and NB had an AUC of 81 percent. These models were identified as the best for predicting whether or not a patient is diabetic [11]. When data is collected in a raw format from numerous sources, there is a danger of several changes that the model may not be able to handle.

III. PROPOSED FRAMEWORK FOR TYPE 2 DIABETES

A Framework has now been proposed and well explained in detail with a focus on Machine Learning based prediction. In addition, this part provides insight into the Diabetic Patient population's data extracted from UCI Machine Learning repository. The proposed Machine Learning based Framework for Diabetes Mellitus prediction as shown in Fig. 1 motivates the future Machine Learning based disease prediction of Diabetes. Author proposed a Framework in which data is collected after that data processing is done. Then applying the Machine Learning algorithms and finding the result and analysis. Then if the patient is diabetic if yes verify the type of diabetes. Patient is not diabetic then stops.

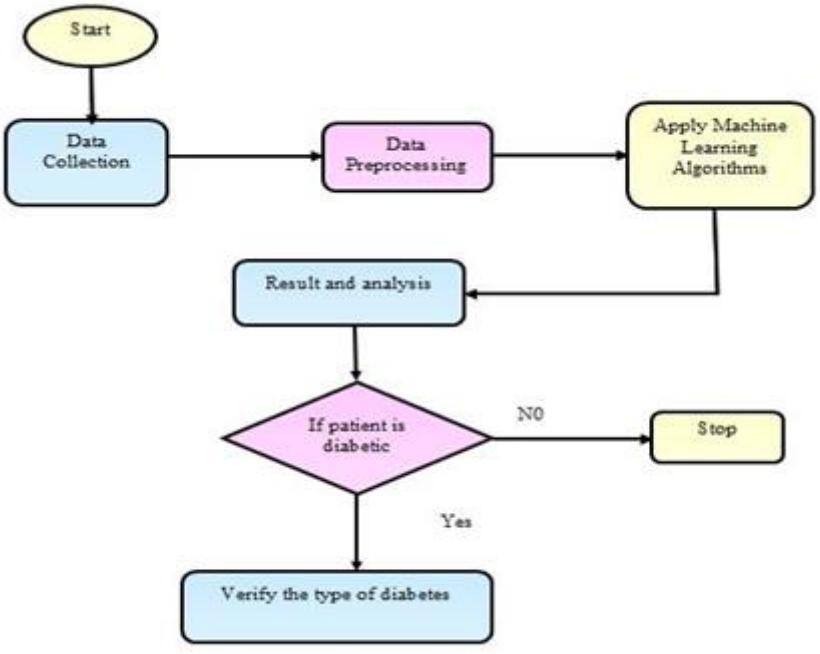


Fig.1 Proposed Framework for Type 2 Diabetes

3.1 Data Collection: The data used for this paper is collected from the UCI machine learning repository. These affect health data collection and analysis in order to investigate patterns and trends which aids in forecasting and

valuating outcomes. It consists of 390 instances.i.e Patient number,Cholestrol,Glucose,hdlchol,age,gender,height,weight,BMI,Systolic-bp,Diastolic-bp,Waist,Hip,Waist-hipratio,Diabetes. The above affect health data collection and analysis in order to provide data and trends that can help in forecasting and evaluating results. The following is a description of the dataset as shown in Table 1. The data collection consists of 390 instances and 15 attributes.

Table 1.Dataset Information

Attributes	Type
Patient number	Int 64
Cholesterol	Int 64
Glucose	Int 64
hdl-chol	Int 64
age	Int 64
gender,	object
height	Int 64
weight	Int 64
BMI	Int 64
Systolic-bp,	Int 64
Diastolic-bp	Int 64
Waist	Int 64
Hip	Int 64
Waist-hip ratio	object

3.2 Data preprocessing: This step of the Framework deals with inaccurate information in order to produce better precise and accurate outcomes. There are missing values in this collection. As a result, we imputed missing values for a few select attributes, such as Glucose, age, BMI, Systolic-bp, Diastolic-bp, because these attributes aren't allowed to have 0 values. The dataset is then scaled to standardize all values.

3.3 Machine Learning Algorithms: This is the most important time, as it involves diabetes prediction. We used a variety of MLT to predict diabetic in this research. These algorithms include the following: SVM, RFand XGBoost.

Algorithm 1: Prediction of diabetes using a variety of Machine Learning Algorithms

Build training and a test set at randomization.
Identify the algorithms that will be utilized in the model.
no= [Support Vector Machine, Random Forest, and XGBoost]
For (i=0;i<12;i++)do
Model=no[i];
Model.fit ();
Model. Predict ();
Print (Accuracy (i), Confusion-Matrix,Classfication-report);
End.

a) **Support Vector Machine (SVM):** In comparison to other supervised Machine Learning algorithms the SVM principle is simple. SVM is a Machine Learning algorithm that is supervised. It is however commonly used in classification methods. The hyper plane is separated in SVM to describe the data. The goal is to find a plane with the greatest margin, i.e. the greatest distance between data points from both classes. SVM is a kernel-based algorithm that transforms an input statistical space into the appropriate formats. It increases the power, flexibility and accuracy of SVM[13]. The main purpose is to isolate the dataset in the most efficient way possible. The margin is defined as the distance between the two closest points.

b) **Random Forest (RF):** RF is a method for supervised learning. It creates was made up of decision trees that are usually trained using the "wrapping" technique. The "bagging" principle's overall motivation is that a collection of learning models creates the ultimate result. It is a group of models that operate together as an ensemble, as the title implies. The knowledge of the people is a core idea in RF; each model forecasts an outcome, and the majority decides in the end. It has been shown to be effective in the literature for diabetic prediction. The RF classifier iterates B times by picking samples with replacement by fitting a tree to the training examples, given a collection of training examples X x1, x2,..., xm and their respective targets Y y1, y2,..., ym.

i) Sample n training instances from X and Y with replacement for b 1...B.

ii) On Xb and Yb, train a classification tree fb.

c) **XGBoost:** Extreme Gradient Boosting (XGBoost) is one of the most popular gradient boosting (ensemble) approaches in tree-based Machine Learning algorithms, with better and faster execution. The boosting method set is represented by XGBoost in the collection of ensemble learning methods. Ensemble learning is a notion that describes a set of classifiers that are a composite of various models that are utilized to give higher classification performance. XGBoost is a convincing distributed Machine Learning platform for scaling tree boosting methods as well as an efficient and easy deployment of the Gradient Boosted Trees algorithm. The classier is well configured and responsibility to solve in a distributed environment for a rapid parallel tree structure. It combines a single node with tens of millions of samples and billions of distributed software samples, allowing it to expand to record levels [14].XGBoost is a Machine Learning method that has recently controlled Kaggle competitions for structured data. Boosting is a high-speed and high-performance implementation of gradient boosted decision trees [15].

IV. RESULT

Machine learning techniques have been created to predict diabetes at an earlier phase. Comparing our model against current predictive models and common classification techniques can reveal accuracy rate. While using 10 fold cross validation, the performance was increased to 90.36 percent. In comparing to other research papers and to several classical classification methods, our Type 2 Diabetes model achieves a higher precision in Random Forest.

V. CONCLUSION AND FUTURE SCOPE

Various MLT and their applications have been investigated or evaluated. Machine learning algorithms were used on a variety of medical data sets, including Machine Learning data. Machine Learning methods have varying

degrees of power in different data sets. This study compares individual algorithms and the suggested technique using a 390-record diabetes data set collected from UCI. In this research, the proposed technique gave high accuracy with a value of 90.36 percent in RF, XGBoost gives the accuracy of 86.72 percent, while SVM produced lower accuracy with an accuracy value of 83.72 percent as shown in fig.2 As a result, RF outperforms the single method in terms of prediction accuracy. We mainly focused on type2 diabetes in this study, but this concept might be applied to other disorders in the future. This study only used a small sample of data. It can be used to process large amounts of data in order to expand in the future. Because only a single data set was used in this study, other data sets can be used in the future for prediction. Only a limited base classifier was employed in this study. In the future, alternative base classifiers such as ANN, Nave Bayes, KNN and others may be used.

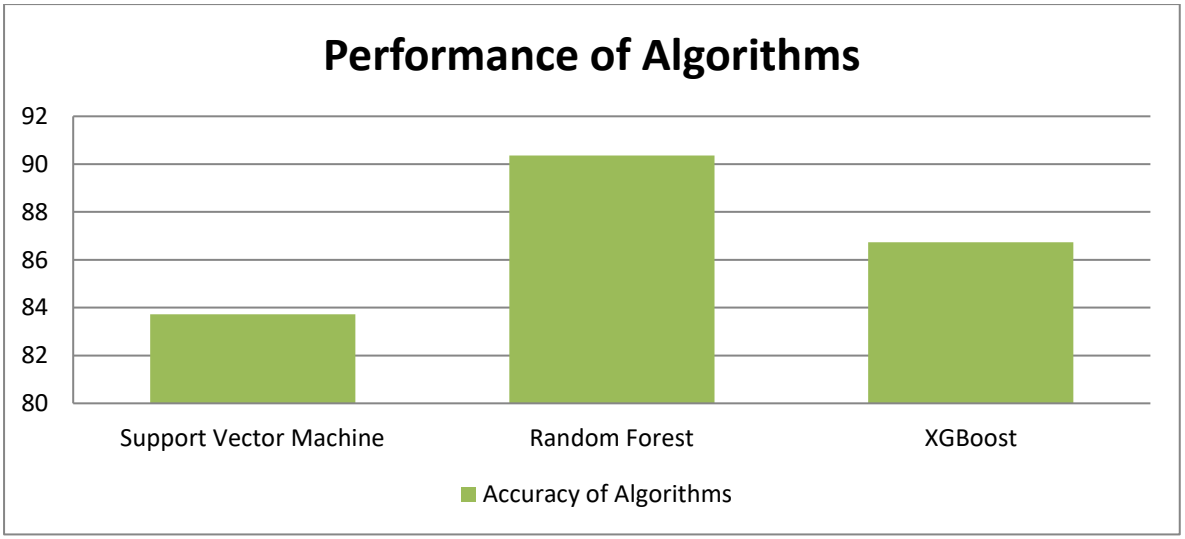


Fig.2 Represents the accuracy of Algorithms

VI. REFERENCES

[1]. Agrawal, Siddarth, Sebastian Makuch, Mateusz Dróżdż, Tomasz Dudzik, Igor Doman ski, Rafał Poręba, and Grzegorz Mazur. "The Impact of Hypoglycemia on Patients with Diabetes Mellitus: A Cross-Sectional Analysis." Journal of Clinical Medicine 11, no. 3 (2022): 626.

[2]. Ardestani, Amin, and Kathrin Maedler. "MST1 deletion protects β-cells in a mouse model of diabetes." Nutrition & Diabetes 12, no. 1 (2022): 1-5.

[3]. Leheny, Shelby. "What Are the Best Drugs to Treat Diabetes?." (2020).

[4]. Inoue, Ryota, Kuniyuki Nishiyama, Jinghe Li, Daisuke Miyashita, Masato Ono, Yasuo Terauchi, and Jun Shirakawa. "The Feasibility and Applicability of Stem Cell Therapy for the Cure of Type 1 Diabetes" ,Cells 10, no. 7 (2021): 1589.

[5]. Carullo, Gabriele, Sarah Mazzotta, Margarita Vega-Holm, Fernando Iglesias-Guerra, José Manuel Vega-Pérez, Francesca Aiello, and Antonella Brizzi. "GPR120/FFAR4 Pharmacology: Focus on Agonists in Type 2 Diabetes Mellitus Drug Discovery." Journal of Medicinal Chemistry 64, no. 8 (2021): 4312-4332.

[6]. Kieu, Alexander, Romona Devi Govender, Linda Östlundh, and Jeffrey King. "Benefits of the addition of continuous or flash glucose monitoring versus standard practice using self-monitored blood glucose and

hemoglobin A1c in the primary care of Diabetes Mellitus: a systematic review protocol." BMJ open 11, no. 8 (2021): e050027.

[7]. Moreira, Mário WL, Joel JPC Rodrigues, Neeraj Kumar, Jalal Al-Muhtadi, and Valeriy Korotaev. "Evolutionary radial basis function network for gestational diabetes data analytics" Journal of computational science 27 (2018): 410-417.

[8]. Taher, Kazi Abu, Billal Mohammed Yasin Jisan, and Md Mahbubur Rahman. "Network intrusion detection using supervised machine learning technique with feature selection" In 2019 International conference on robotics, electrical and signal processing techniques (ICREST), pp. 643-646,IEEE 2019.

[9]. Gadekallu, Thippa Reddy, Neelu Khare, Sweta Bhattacharya, Saurabh Singh, Praveen Kumar Reddy Maddikunta, In-Ho Ra, and Mamoun Alazab. "Early detection of diabetic retinopathy using PCA-firefly based deep learning model." Electronics 9, no. 2 (2020): 274.

[10]. Kumari, Saloni, Deepika Kumar, and Mamta Mittal. "An ensemble approach for classification and prediction of Diabetes Mellitus using soft voting classifier." International Journal of Cognitive Computing in Engineering 2 (2021): 40-46.

[11]. Zhong, Junda, Peng Liu, Shuang Li, Xiaomin Huang, Qunhui Zhang, Jianyu Huang, Yan Guo et al. "A comparison of three-dimensional speckle tracking echocardiography parameters in predicting left ventricular remodeling" Journal of healthcare engineering 2020 (2020).

[12]. Shafi, Salliah, and Gufran Ahmad Ansari "Early Prediction of Diabetes Disease & Classification of Algorithms Using Machine Learning Approach," Available at SSRN 3852590 (2021).

[13]. Adegboye A", AJOSR Vol. 3, Issue 2, 2021 Adegboye and Adegoke".

[14]. Kourtellis, Nicolas, Gianmarco De Francisci Morales, Albert Bifet, and Arinto Murdopo. "Vht: Vertical hoeffding tree." In 2016 IEEE International conference on big data (big data), pp. 915-922, IEEE, 2016.

[15]. Bhat, Salliah Shafi, and Gufran Ahmad Ansari, "Predictions of Diabetes and Diet Recommendation System for Diabetic Patients using Machine Learning Techniques" In 2021 2nd International Conference for Emerging Technology (INCET), pp. 1-5, IEEE, 2021.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Smart Lock Device

Dev Thakkar[1], Vaibhav More[1], Aryan Rathod[1], Prof. Deepali Sonawane[2]
[1]School of Computer, MIT-WPU, Pune, Maharashtra, India
[2]Assistant Professor, School of Computer Science, MIT-WPU, Pune, Maharashtra, India

ABSTRACT

This Project includes smart lock enhanced with biometric which includes fingerprint as well as voice recognition system.

This Device will have its own dedicated app and website.

For implementing this project, we will be using a fingerprint sensor, microcontroller, microphone, Gsm Module, Motors and necessary hardware components. Smart Lock will not be only restricted to main door locking system but also have other models which will be suitable to lock doors, cabinets, wardrobe(sliding, openable) and also aldrop!. The lock will be designed according to known hardware synopsis.

The purpose of introducing this smart lock is to give more security to the user which will not bound only to specific doors.

Smart Lock Device will have integrated fingerprint sensor with mic. The purpose of introducing microphone with fingerprint sensor is to ensure more security to the user. Fingerprint Sensor will be associated with number of invalid fingerprint attempts.

The software system of this lock device will be designed in such a way that user has to sign-up initially with their contact number as well as email id. Once the user has logged-in successfully they'll have to pair their Smart Lock Device with their phone. If Someone has exhausted number of Invalid fingerprint trials. The user will immediately receive notification that someone is trying to Breach The lock System with an option if they want to enhance security, if user allows that option, the lock will immediately turn on voice recognition and will unlock only when user Speaks as well as Place Finger on the sensor. The Purpose of Collecting Contact Number & mail id is when user is offline, user will receive a text message on their given phone number as well as on given mail id. In Software update, we can introduce the feature of adding contact info of neighbors as well, so that neighbors can also receive pop-up notification, if user wishes to inform them.

Keywords- Biometric, Lock, Breach, Security, Voice.

I. INTRODUCTION

A. Traditional vs Smart Lock

What are traditional locks?

The term 'traditional locks' is not something that many people are used to hearing. Granted, there are many different types of regular locks that are not automated, but up until smart locks carved out space for themselves, these old locks were just called locks. There are many variations of traditional locks, which can be used for a plethora of purposes. The term is essentially referring to locks that are not automated and locks that have to be manually engaged in order for the locking mechanism to be operated.

B. How do traditional locks work?

The majority of traditional locks work when a key is used to activate the locking mechanism, which will give it the ability to lock or unlock. Some very common examples of these traditional locks are pin tumbler locks, rim locks, and mortise locks. Let's take a look at the pin-tumbler lock for example.

Pin-Tumbler locks are some of the most common locks used within residential properties. The locking mechanism in these locks features a series of spring-loaded pins that are in turn loaded into cylinders. The cylinders consist of a set of pins that are designated as the key pins and the driver pins. When the correct key is inserted into the locking mechanism the key pins are elevated, which pushes the driver pins upward.

Once the proper key is inserted into the lock, the driver pins and key pins align at the shear line. Then the key can be turned in the lock, to unlock, and sometimes lock, the mechanism. If the wrong key is used, the misalignment of the pins will block the key from being turned because the pins will be bound at the shear line.

C. How secure are traditional locks?

This is not an easy question to answer, and that is due to the number of lock variations that homeowners utilize. The security levels that these locks give homeowners varies. For instance, the deadbolt is one of the most common exterior residential locks. There are usually two main types of deadbolts, single cylinder deadbolts, and double cylinder deadbolts. These locks are known to provide maximum security for homeowners but only if the right ones are used and if they are used in the right way.

Deadbolts are grouped according to grades that determine their relative strength. These grades are usually based on the relative strength, longevity, and durability of these locks. They range from 3 to 1, with 3 being the lowest grade and 1 being the highest grade. ANSI (American National Standards Institute) Grade 1 deadbolts provide homeowners with the maximum security for their residential locks. However, the thing that allows these locks to be as secure as they are, are the additions that can be made to ensure that they are as secure as possible.

D. What are smart locks?

In their simplest form, smart locks are automated versions of traditional locks. In most cases, a smart lock will make use of the traditional lock mechanism, but the lock mechanism can be engaged electronically or remotely. These locks are different because they require a different interaction (between the user and the lock) than traditional locks. The name 'smart locks' also stems from their ability to be controlled and operated by smart phones, as well as their ability to integrate with other smart devices.

These locks allow homeowners to control and monitor their locks in a way that traditional locks do not. If the smart locks are working the way it is intended to, it provides unparalleled ease of access and comfort. However, this does not always mean it is the most secure option. Smart lock manufacturers tend to focus more on the efficiency and added features that the lock brings to the table, which makes them skimp on the security factors that have made locks a hallmark for every home.

E. How do smart locks work?

Smart locks, much like traditional locks, require a lock and a key in order to work properly. A smart lock has to receive its operational instructions from a pre-authorized device, as well as a cryptographic key in order for it to perform its locking and unlocking process. In addition to this, smart locks are also able to monitor the status of the lock and send pertinent alerts to authorized devices. In most cases, this would be the homeowner's smart phone. These locks are considered to be a huge part of the smart home, and they are capable of integration with many other smart devices and products.

The key for smart locks is not a physical key as it is for traditional locks. These keys are either special key fobs or a set of instructions issued by home automation protocol, which will authenticate that it is the proper key for the

lock. Some smart locks also have the ability to hand out temporary keys to third parties, and these temporary keys function as spare keys.

F. How secure are smart locks?

The security of smart locks has been in question since before their inception. It did not become apparent to many people that this was even an issue until after homeowner's started to acquire smart locks. This might have been because smart locks were not necessarily advertised for their security capabilities, but they were marketed by talking about all the new and cool things that a smart lock could do for an individual's home. For instance, some smart locks give homeowners the ability to remotely monitor the status of their locks, as well as remotely operate their locks. These features are some of the things that make a smart lock truly unique and the reasons why some people flocked to them.

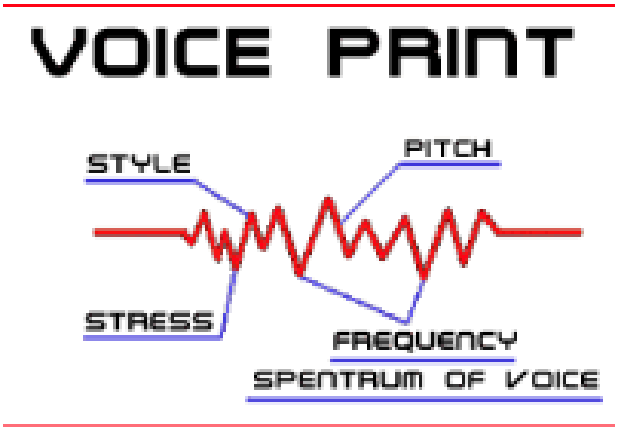
However, the issue of smart lock security was one that gradually made its way to the foreground of the conversation. Smart locks made little architectural improvements to the basic design and components of traditional locks, so they each essentially start out on the same security threshold (in most cases). In this sense, most people would think that their smart locks are better than their traditional locks because they are being afforded the same level of security with added features, but this isn't always the case.

Most smart locks will work with an existing deadbolt, which does imply that they are offering a much more secure lock than if you were to use a Euro Cylinder lock on your front door. Though this might be better, there is a drawback to this. Due to the specific nature in which smart locks are designed, it is hard to make additions to them. A perfect example is the August Smart Lock, which can only work with thumb turn deadbolts and will not work with double cylinder deadbolts. Another example is the Kevo Kwikset, which comes with its own hardware (lock cylinder, interior set up, etc.) and is meant to replace whatever hardware a homeowner had in place.

II. METHODOLOGY

Optical fingerprint sensor can be used, as it captures a photo of our finger ridges since ridges and patterns are very important in the analysis of fingerprints as no two fingerprints have been shown to be identical, and it uses certain algorithms to match it with the stored data, connections can be done for the power, data as well as with hardware bolt to lock & unlock whenever needed. Desired finger impressions can be enrolled in Scanner Module and stored in the IC registers of the Microcontroller. With the interfacing method, fingerprints can be used to create secure and impenetrable lock. Interfacing can be done by developing communication between Microcontroller and Interface. Motors are used for locking and unlocking the door.

However, if an unauthorized person tries to breach lock, beeping sound takes place after number of trials are expired, also designated app will send a continuous pop-up to registered user in the app as well as leave a SMS, incase user is offline. This Pop-Up Notification will be having an option, if user wants to lock the door/system with high level security which will be delivered via app as well as SMS(can be enabled using desired numbers, for example 1,2,etc). This high level security will be triggering voice recognition system to take place. Voice recognition will take voice input from the user whose identity needs to be stored in the device. The voiceprint is made with the use of software that splits voice input statement into various frequencies. The prints are stored in databases to identify later and acknowledge users.

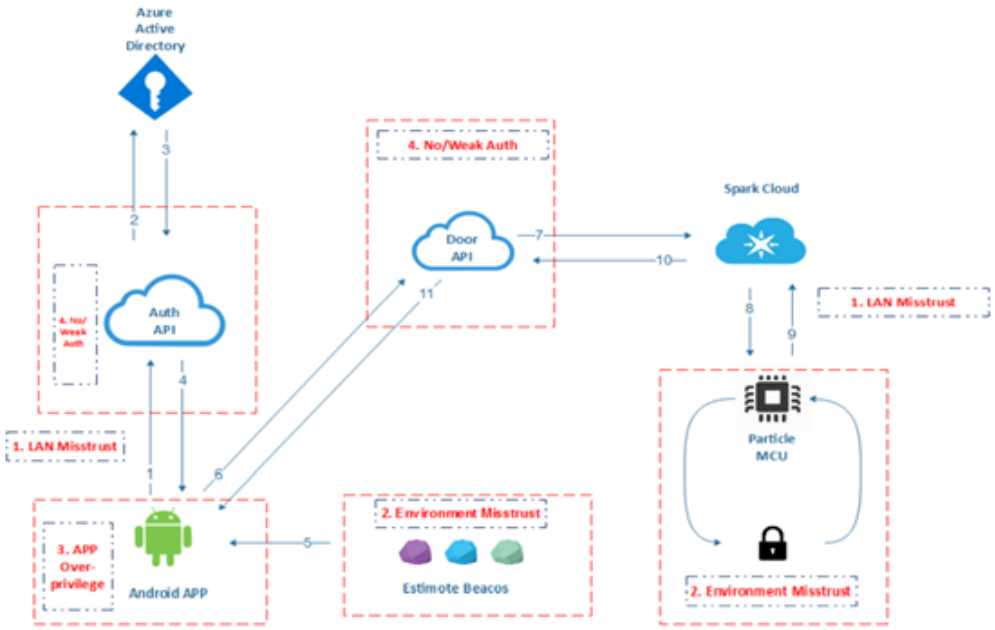


Adding this feature will add security, as system now can be only unlocked when user uses finger impression as well as input voice. However, if someone tries to harm microphone or finger impression sensor, system will send an appropriate message accordingly. Incase, internal parts are damaged system can be unlocked using Customer-Care Service where user has to provide their product's primary key (different for everyone), which will allow executive to unlock the system. As earlier mentioned, locking system will not be only restricted for the main door but it will have different product(smart padlock, smart sliding lock, etc) according to price range and user's need.

III. ANDROID BASED APPLICATION

An extensive and user friendly Android application has been developed to control and monitor the status of biometric door locks. The communication between application and server was achieved by Apache HTTP Client. For data exchange between client and server JSON was employed. The user has to get registered to the device before using the application, providing personal details. On a single android phone only one user can be registered though one user can login on multiple phones. After successful registration and login, user can insert, delete or edit door locks along with the desired features to be attached with each door (doorbell detection, door knock detection, suspicious person). After login user selects a door and views the activity tab of that door with images of visitors and time of arrival, action tab on which he/she can see all the unlocking actions performed by users of that door, status of different doors (open/closed) and unlock the door by putting his/her finger on the fingerprint sensor of the door if it fails the number of trials then it will give a notification on the app and then the user will immediately receive a notification that someone is trying to Breach The lock System with an option if they want to enhance security, if user allows that option, the lock will immediately turn on voice recognition and will unlock only when user Speaks as well as Place Finger on the sensor. The user guides of how to use application

and how to use the device are also available. Moreover a single android device can make only one account on server fortifying the security. Notification is received on android application whenever any activity is occurred or action is performed. On opening notification, application allows user to unlock door after biometric or voice is verified. The Purpose of Collecting Contact Number & mail id is when user is offline, user will receive a text message on their given phone number as well as on given mail id. In Software update, we can introduce the feature of adding contact info of neighbors as well, so that neighbors can also receive pop-up notification, if user wishes to inform them.



1. Android Application asks for authentication by sending username and password via HTTPS.
2. "Auth API" ask for an access token from Azure AD with provided user credentials, resourceID, and clientID.
3. If the information sent with the request is valid the Azure AD responds with an access token valid for 2 hours.
4. The token is sent back to the Android Application via HTTPS. The Android client can now make authenticated calls to the Door API.
5. The Android application will start listening for registered beacons. When a Beacon transmission is received, the application will confirm that the beacons are from a valid source.
6. The Android will request to open the door if the beacon(or biometric /voice) validation is successful. Access token and the function name is provided in the HTTPS call.
7. The door will send a new HTTPS request to the particle if the received request is authenticated and authorized. The request to Spark Cloud will contain the unique access token and deviceID for the Particle device.
8. Spark will send the specific function call (in this case "open door") to the device with the correct deviceID.
9. The Photon device will return a specific value of the function called was executed correctly or not.
10. Spark Cloud will send an HTTPS response back to door API containing information about the status of the request.
11. Door API sends a response back to Android telling the application if the request was successful or not.

A. What is REST API?

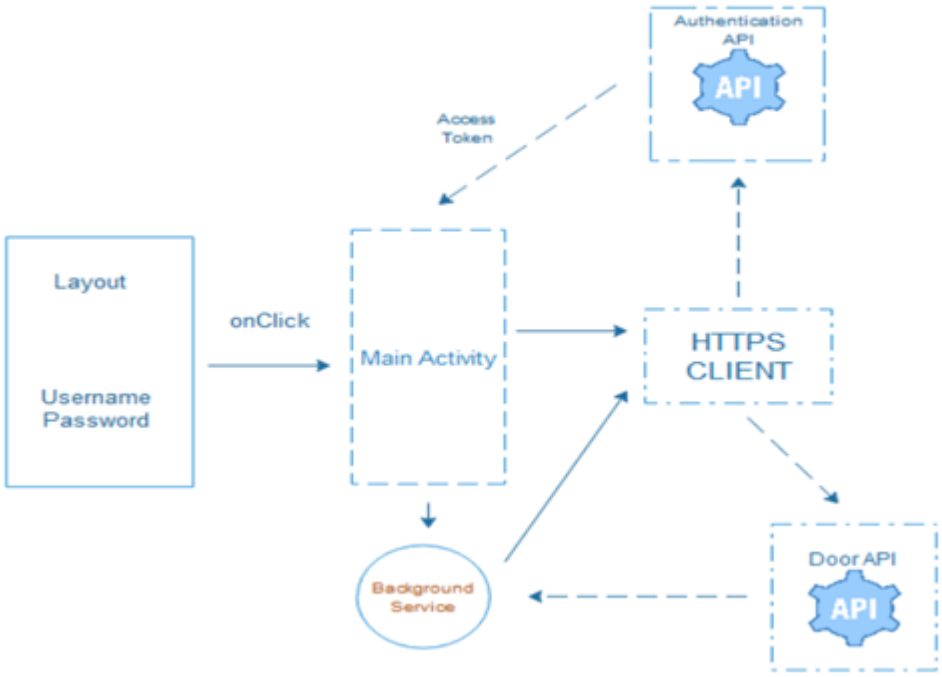
Representational state transfer technology (REST) is a software architectural approach and procedure used for the goal of communication in web-based services. REST is an API that uses HTTP requests to get, post, put and delete data. This API uses HTTP paradigms. REST API uses GET function to regain a resource; PUT function to change the nature of/update a resource, which can be a block of information or a file; POST function to create a resource and DELETE function to remove it. This API structure is important to minimize the coupling between the client and server components in a distributed application. REST is an interface between systems using HTTP to obtain data and generate operations on these data in all possible formats (e.g XML and JSON).

B. Communicating to and from the REST API

To make different calls via the internet can be dangerous from a security perspective but is in our cause definitely necessary. The Particle door device needs to be fed different tasks as door unlocking to be able to perform in a wanted manner. When transmitting data via the web the sender has no control over which path it chooses takes to reach the receiver. This means that nodes on the internet can intercept the data and read it if it is not encrypted in some kind of way. The most standard protocol for receiving or requesting data over the web is HTTP (Hypertext Transfer Protocol). The standard HTTP protocol comes in various forms and has all the functionality needed for calling our web APIs. However, there is one major problem; the HTTP sends data via plain text. This is a large issue as anyone interacting the HTTP request on its path the response can easily read or intercept data without us ever knowing. This will make all the security measures we implement useless and unnecessary as an attacker simply can read all the communication within the system. extracting sensitive data as username, passwords, or tokens. Fortunately, there is a simple solution to this problem called SSL (Secure Sockets Layer). By combining these two protocols you get a safe and secure protocol with all the functionality of the HTTP, this protocol is called HTTPS. HTTPS relies on asymmetric and symmetric cryptography and all the data send between two nodes a completely encrypted.

C. Application Overview: -

The SDL app will be requiring the user to enter the login credentials (username, password). Clicking on the login button will activate the onClick() method that in turn will go to our MainActivity and trigger an HTTPS request through the HTTPS client. The credentials will be sent in a scrambled message with an agreed code between the sender and the receiver (Authenticate API in our case) and transferred on a Secure Sockets Layer where no one can read the message. The user's credentials are authenticated in API, when the Authentication process is completed and succeed, the Access Token is sent back to the MainActivity in the SDL app. At this point, the app is ready to start the Background service and begin to scan for beacons. When a valid beacon is found, an authenticated request is sent (containing the acquired Access Token) through the HTTPS client to the Door API where the validity of the token is determined. A proper response is then sent from the Door API telling the application if the request was successful.



D. App Prototype Link

https://thegraphicgallery0.wixsite.com/website

IV. RESULT

- As a conclusion, Now keys can be optional! also locking systems will be more secured.
- The lock device will be available in number of variants & customisation according to price range as well as consumer's needs.
- Purpose to Introduce this Smart Lock is to give more security to the user which will not bound only to specific doors.
- Breaching the lock will automatically lead to activation of high security(Voice and Finger Impression)
- Due to this technology high security will be assured in Cabinates, Lock Safe's, Sliding Wardrobes, Padlocks, etc.
- Designated app and Contact Registraion will keep you notified in every situation.
- User Friendly App, which will allow user to manage their multiple locking systems through one app.
- Each Locking Product will come with Primary Id which will be known to user and will help to unlock their locking system via co-ordinating with 24x7 Customer Care Service.
- Minimise the breaching of locks as Neighbours can be notified as per user's virtue.
- User can always add, delete and update Voice Prints, as well Finger Impressions through their app.
- So Many Options to Lock and Unlock with High Level of Security

V. ACKNOWLEDGMENT

This paper and the research behind it would not have been possible without my enthusiastic team, and our mentor, Prof. Deepali Sonawane, her guidance, knowledge and attention towards detailing have been an inspiration and kept our work on the track. Also, my colleagues Vaibhav More and Aryan Rathod contributed their valuable support and knowledge to bring most out of this topic. I will also be grateful for the comments offered by anonymous peer reviewers at National Research Conference. The generosity and expertise of one and all will definitely encourage me to do more better in future. We are also immensely grateful for the comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of esteemed persons.

VI. REFERENCES

[1]. https://www.diva-portal.org/smash/get/diva2:1216681/FULLTEXT01.pdf
[2]. https://www.claysys.com/blog/voice-biometric-authentication/
[3]. Smart Door Lock Using Fingerprint Sensor Piash Paul, Md. Abdullah Al Achib, Hazrat Sauda Hossain, Md. Kaviul Hossain

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Automated Parking Systems using Digital Image Processing and Deep Learning

Simran Dubey, Advait Chaudhari, Shambhavi Jilkar
School of Computer Science, Dr. Vishwanath Karad's MIT World Peace University Pune, Maharashtra, India

ABSTRACT
Using the power of Deep Learning to implement the concepts of Digital Image Processing & OpenCV, we aim to achieve an Automated parking system. This system is proposed to specifically benefit those places that require high security and frequent identification of parking spaces. This paper will throw some light on how we can achieve efficient parking facilities, not just in public spaces, but also in various Institutes, Universities, Government Facilities, Societies, Corporate workplaces, etc.

Keywords— Automated parking system, Deep Learning, OpenCV, Mask R-CNN, Digital Image Processing, ALPR

I. INTRODUCTION

This paper aims at improving existing parking facilities in India, by the implementation of image processing to create an Intelligent Parking System. Image processing is very useful in identifying parking availability. Combining this with a system to identify number plates will reduce human labour and increase the security and flexibility. This will also help in utilising the parking space efficiently. In this system, we use a camera mounted at the entrance for admittance of verified vehicles. It will automatically take continuous video footage. The images captured by this camera will be run through the Automatic License Plate Recognition (ALPR) algorithm using OpenCV to help identify the license plate number of the vehicle. This will then be searched through the database. Inability to find a match will allow the security personnel in charge to either restrict the vehicle from entering or create a new registration. Constant video monitoring of the parking lot will provide continuous video that is analysed to identify vacant and occupied parking space in real time.

This can be achieved by the robust Mask R - Convolutional Neural Networks (CNNs) algorithm mainly used for image recognition tasks. Initially the user needs to provide their details to be stored in a MySQL database, so that the system can detect and allow them easily.

Research into this algorithm for image detection has proved to be effective and robust to light condition changes, presence of shadows, and partial occlusions. The detection is strong and reliable even if viewpoints are different for the training and test images. [9]

With the constant increase in population and urbanisation, congestion and shortage of parking spaces are becoming noteworthy issues in many countries, especially India. The absence of proper facilities for parking along with poor management contribute towards congestion and increased fuel consumption. From University campuses to movie theatres, parking is a troublesome transportation problem faced by all. Automatically providing information about the vacant spaces in the parking lot will reduce traffic congestion and utilisation of fuel besides providing ease, convenience, and value for time. This will also ultimately lead to a decrease in pollution. A system to prevent the entry of intruders by using License Plate detection, will provide increased security to parking lots which is a helpful factor for a variety of businesses.

II. LITERATURE REVIEW

K. Malarvizhi, A. Kayathiri and K. G. Subadra in their research paper published in 2017 have proposed a system to detect a vehicle parking system using Internet of things which we used as a reference here.In their research paper they focused on how they will utilise ultrasonic and proximity sensors for parking lot detection. Their methodology consists of three stages: parking slot detection, parking slot display and parking lot reservation.
In their proposed system they are going to use GSM communication network to display the vacancy details and unavailable slots on LED Screen. Also, the slots can be reserved through the person's mobile phone [10]. Similarly, another author namly C. Shi, J. Liu and C. Miao in their paper focused on analysing video on how we can detect the parking spaces as well as detect the license plate number. The Authors here are analysing location of parking spaces in a video which combines detecting license plate along with detecting parking spaces. In this they used grey level method to determine occupancy of the vehicle when the vehicle is sheltered by pedestrian. They also mentioned a guidance system for the vehicle so that when it enters the parking space the guidance system can a lot a parking space to them. Although a similar concept has been focused in our research paper, the implementation and algorithm is different and better than the one proposed above [11].
J. Ahmad, Z. Lewis, P. Duraisamy and T. Mcdonald in their paper published in 2019 highlighted the issue with regards to parking spots especially in urban areas where people rush to work and meetings during busy hours and they have to drive to multiple parking lots hoping that they will find one unoccupied spot successfully, so driving around to find one such spot wastes their time in blindly looking for one. The Authors of this paper proposed a solution for it by using MRCNN (Mask Region- based Convolutional Neural Networks) which will help the people in finding an available parking slot easily without having to drive and check through all of them hence saving their time.[13].Also Researchers E. J. Sen et.al in their paper proposed a system of Advanced license plate recognition system for car parking that consists of two sections: Radio frequency identification(RFID) based reserved car parking system and number plate recognition by using Open Computer Vision(CV). The solution of their paper provides high security and there is no necessity for a guard as it only permits Authorised vehicles to enter the parking area if some conditions are met. Those conditions are an Authorised vehicle should have a valid RFID tag number as well as a standardised license plate. The RFID reader will be installed in the parking lot that will read the particular RFID tag in that vehicle and grant access to it only if its data is stored in the database.
Open CV will be used to detect license plate of the vehicle. By this solution it makes it easy and saves time to get a parking slot, also it's safe as it only accepts valid vehicle entry.[14]
There has been an increase in the usage of parking spaces at industrial buildings, universities etc where unlike residential complexes, the parking spaces are not priorly appointed to the driver. So, with the help of our system

when the driver enters the premises the ALPR algorithm will capture the license plate number. This will be verified in the database. If that user is registered, the system will provide an available parking spot with the help of Mask R- CNN. If not, it will be notified to the security personnel.

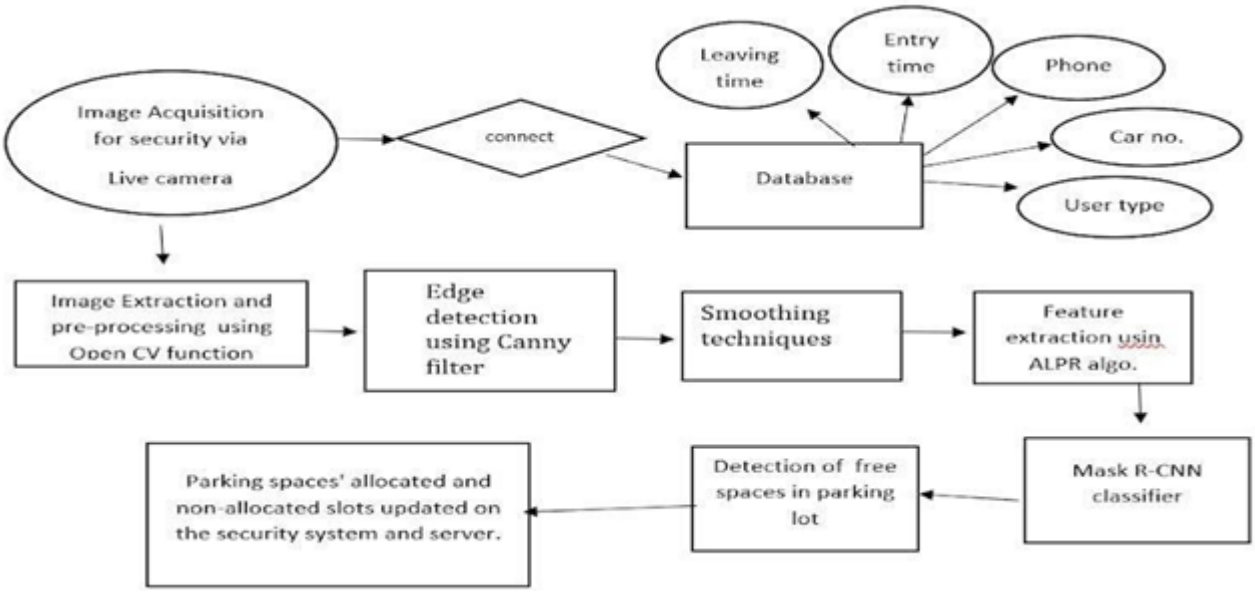
The combination of license plate verification and parking space detection using deep learning helps enhance security and enable state of the art parking facilities at workplaces, universities, etc. and sets the ground for improvement of the theories proposed by the aforementioned research papers.

III. OBJECTIVES

When the vehicle is parked and retrieved without human intervention, congestion in the parking area will be reduced. This will help enhance the security by tracking entry and exit of cars in parking lots. Efficient number plate tracing system which will trace the car number plate and ensure security by letting in either the verified or the authorised vehicles only. The surface space available will also be utilised efficiently and a fully automated system with low cost can be achieved

IV. METHODOLOGY

Once the image and video footage are acquired by the camera, the images are extracted and processed using the OpenCV function. The edge canny filter in OpenCV helps us identify the edges of the car which help differentiate the car from its background. Smoothing techniques help identify the available parking lot. Feature extraction using OpenCV is used to identify the license plate and check the number. Finally deep learning is implemented by using a Mask R-CNN classifier to detect the free parking spaces which are then allocated and then updated in the security system and server. The flow diagram below describes this process.



4.1 DATASET

The dataset involved sample images used for the implementation of this problem statement. The dataset has been taken from an online database. [15]. Given below are examples of the kind of images that were used in the dataset.

4.2 SYSTEM SPECIFICATIONS AND REQUIREMENTS:

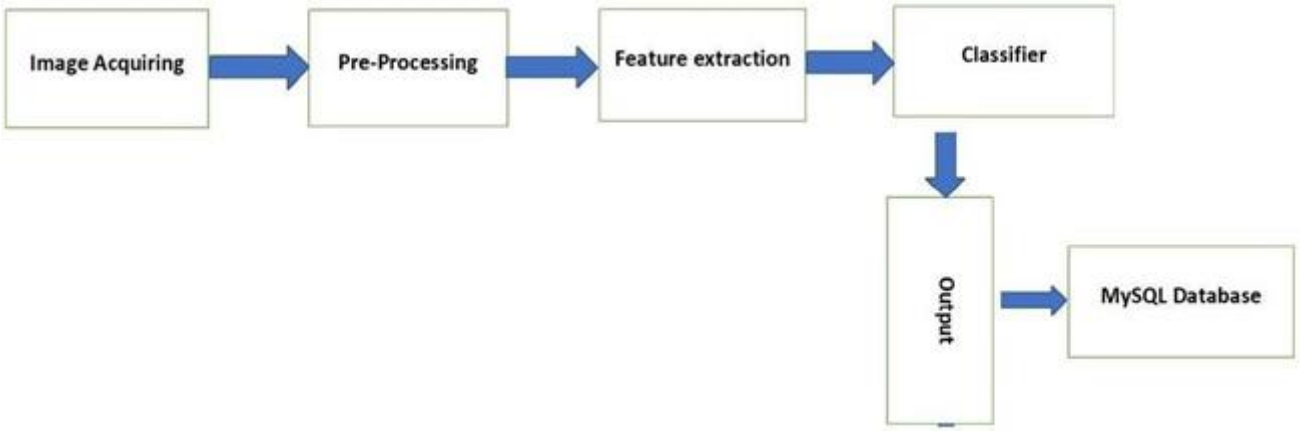
The particular system specifications and requirements for this project involve the following: Python3 installed in the system with any IDLE supporting it, Windows/Ubuntu OS, ALPR For Image processing, MongoDB for database, Seven- Segment display.

4.3 SYSTEM ALGORITHM

This block diagram describes the way the images are processed from acquisition to output. It shows the steps involved in the system algorithm which is as follows:

1. First the image is acquired from the database.
2. Next, image Pre-processing is done using OpenCV followed by Feature extraction i.e., Number plate detection using ALPR.
3. We then use the Mask R-CNN classifier to detect free/occupied parking slots.
4. The output as license number will be notified to the security personnel and if allowed to enter, available slots will be notified to the vehicle owner.
5. The video footage of the real-time allocated and non-allotted parking slots will be available to the security person.
6. The data of entry time and leaving time, along with the vehicle owners' details will be saved using MongoDB/ MySQL in the database for security reasons.

The diagram below shows the flow of the images in their process from acquisition tor output as described above.



4.4 SUB MODULE ALGORITHM

The steps involved in License Plate Recognition using OpenCV are as follows.

1. License Plate Detection: The first approach is to detect the License plate of the vehicle. For that in OpenCV we have a contour option to detect for rectangular objects i.e to find the license plate from the vehicle. The image capture and detection algorithms are trained based on the position of the camera which is set at 45-degree angle.
2. Character Segmentation: After we have detected the License Plate using OpenCV, we have to trim the license plate out and save it as a new image.
3. Character Recognition. The new image that we have of the license plate by the previous step now is that we can perform OCR (Optical Character Recognition) to detect the Number/Alphabet.

4.5 TECHNOLOGIES USED

OpenCV:

It is used to develop real-time computer vision applications. OpenCV mainly focuses on image processing, video capturing and analyzes features like object detection and face detection.

OpenCV's functionality extends to Image/video I/O, processing, display; object/feature detection; geometry-based monocular or stereo computer vision; computational photography; machine learning & clustering.

Mask R-CNN:

Mask R-CNN is an extension of Faster R- CNN. It is widely used for object detection tasks. For a given image/video, it returns the class label and bounding box coordinates for each object in the image/video.

The input to this model can be a video stream from a normal webcam capturing the whole parking lot from the top and detecting if the parking space is available or not.

Segmentation:

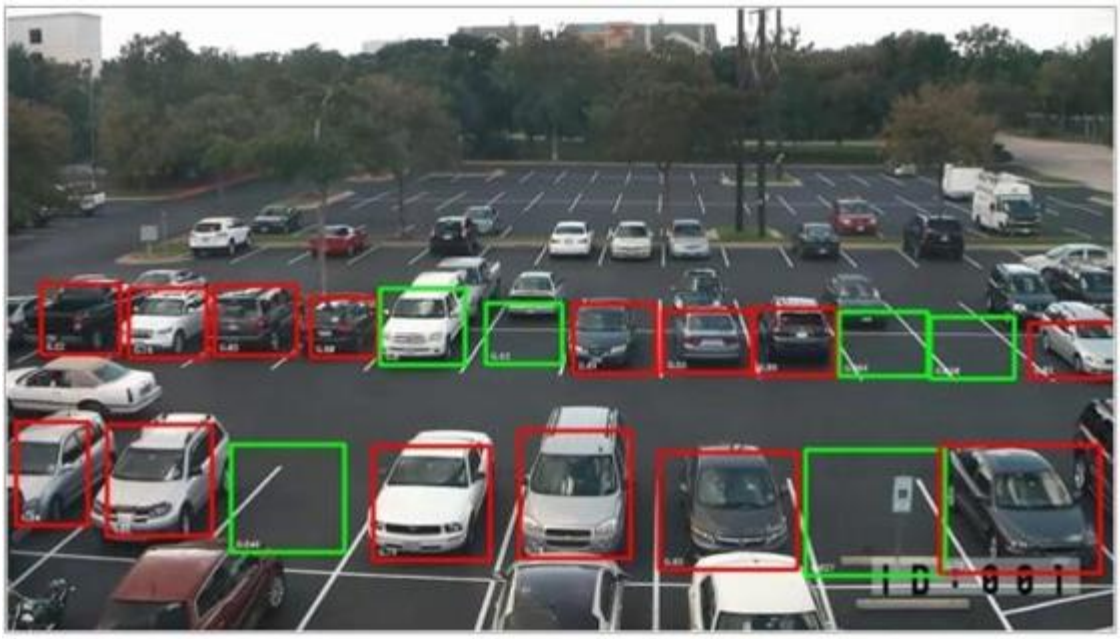
As the car enters the parking space, the instance segmentation process will be triggered by the Mask R-CNN classifier. Canny filter will smoothen the image and the classifier will parallelly put bounding boxes to specify grids which are allocated and unallocated and give the count of it. Allocated and unallocated slots would be specified by two different colours.

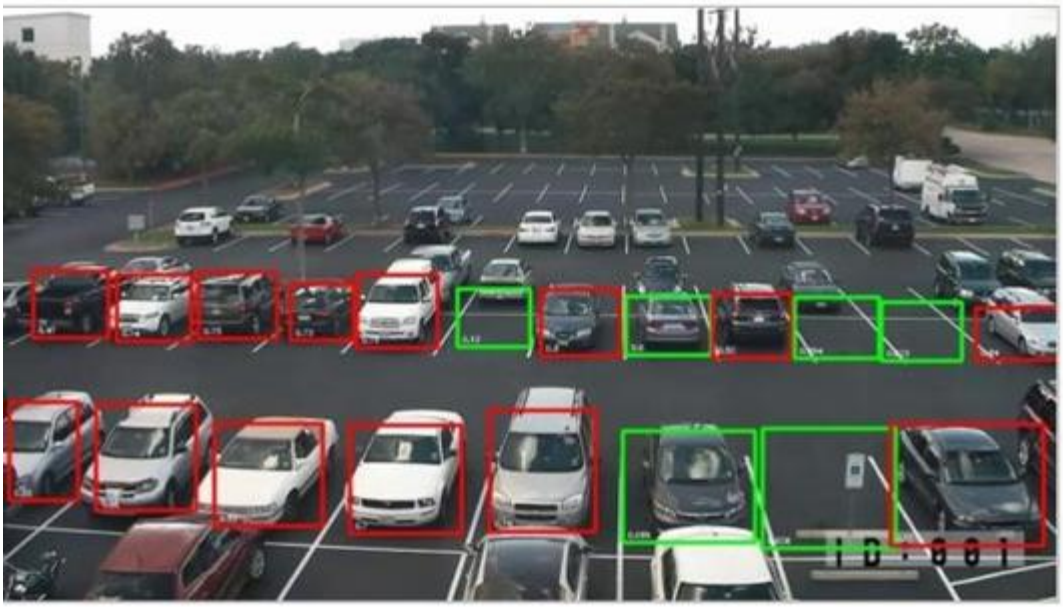
V. RESULT

```
new_image = cv2.bitwise_and(img,img,mask=mask)

(x, y) = np.where(mask == 255)
(topx, topy) = (np.min(x), np.min(y))
(bottomx, bottomy) = (np.max(x), np.max(y))
Cropped = gray[topx:bottomx+1, topy:bottomy+1]

text = pytesseract.image_to_string(Cropped, config='--psm 11')
print("Detected license plate Number is:",text)

for i in valid :
    if text == i:
        print("ALLOW US TO FIND YOU A PARKING SPACE!")
    else :
        print("SORRY, YOU DO NOT HAVE ACCESS TO THIS COLLEGE.")

cv2.waitKey(0)
cv2.destroyAllWindows()
```

```
Detected license plate Number is: HR 26 DA 2330!

SORRY, YOU DO NOT HAVE ACCESS TO THIS COLLEGE.
```


```
Detected license plate Number is: HR 26 DA 2330!

SORRY, YOU DO NOT HAVE ACCESS TO THIS COLLEGE.
```





Enhanced security is provided using License Plate Recognition (ALPR).

The Guidance information is displayed in Seven Segment Display to provide useful real time parking lot information.

There is identification of vacant parking spaces in real time. Robust image processing using OpenCV combined with Mask R-CNN allows for feasible and efficient detection with high accuracy.

VI. FUTURE SCOPE

There is score for adding functionality in the app for getting a parking slot and reserving a slot before reaching the destination.

Another aspect that could be implemented is to verify the student /staff through a mobile number or Mail by providing OTP (One time password). We could also allow for functionality of registered members to be able to add vehicles of their family members or friends to allow direct access without intervention of security. For security purposes we can generate logs of entry and exit of vehicles and also track any suspicious activity in parking space.

VII. CONCLUSION

A convenient and automated way to park a vehicle is proposed through the system. Using recent technologies of deep learning and digital image processing we can achieve state of the art functionality and results very efficiently and easily. Enhancing the security is also achieved by tracking entry and exit of cars in parking lots, apart from verifying the license number plate at entry.

VIII. REFERENCES

[1]. A. Kanáliková and E. Bubeníková, "Parking system with image processing," 2019 IEEE 17th World Symposium on Applied Machine Intelligence and Informatics (SAMI), Herlany, Slovakia, 2019, pp. 281-286, doi: 10.1109/SAMI.2019.8782760

[2]. T. Thomas and T. Bhatt, "Smart Car Parking System Using Convolutional Neural Network," 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, 2018, pp. 172-174, doi: 10.1109/ICIRCA.2018.8597227.

[3]. R. Rajathilagam, K. Sivamani, R. Seetharaman and D. Nedumaran, "Neural Network based Vehicle Number Plate Recognition System," 2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC), Chennai, India, 2019, pp. 102-104, doi:10.1109/ICPEDC47771.2019.9036497.

[4]. M. Tschentscher, B. Pruß and D. Horn, "A simulated car-park environment for the evaluation of video-based on-site parking guidance systems," 2017 IEEE Intelligent Vehicles Symposium (IV), Los Angeles, CA, 2017, pp. 1571-1576, doi: 10.1109/IVS.2017.7995933.

[5]. M. Antoni Suwignyo, I. Setyawan and B. Wirawan Yohanes, "Parking Space Detection Using Quaternionic Local Ranking Binary Pattern," 2018 International Seminar on Application for Technology of Information and Communication, Semarang, 2018, pp. 351-355, doi: 10.1109/ISEMANTIC.2018.8549756.

[6]. G. Amato, F. Carrara, F. Falchi, C. Gennaro and C. Vairo, "Car parking occupancy detection using smart camera networks and Deep Learning," 2016 IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 2016, pp. 1212-1217, doi: 10.1109/ISCC.2016.7543901.

[7]. S. Banerjee, P. Choudekar and M. K. Muju, "Real time car parking system using image processing," 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, India, 2011, pp. 99- 103, doi: 10.1109/ICECTECH.2011.5941663.

[8]. R. Vîlceanu, M. Oniţa and A. Ternauciuc, "Analysing parking lots vacancy detection algorithms using Mask R-CNN implementations," 2020 International Symposium on Electronics and Telecommunications (ISETC), Timişoara, Romania, 2020, pp. 1-4, doi: 10.1109/ISETC50328.2020.9301141.

[9]. B. Sairam, A. Agrawal, G. Krishna and S.P. Sahu, "Automated Vehicle Parking Slot Detection System Using Deep Learning," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2020, pp. 750-755, doi: 10.1109/ICCMC48092.2020.ICCMC-000140.

[10]. K. Malarvizhi, A. Kayathiri and K. G.Subadra, "Survey paper on vehicle parking slot detection using internet of things," 2017 International Conference on Computation of Power, Energy Information and Communication (ICCPEIC), Melmaruvathur, India, 2017, pp. 279-282, doi: 10.1109/ICCPEIC.2017.8290377.

[11]. C. Shi, J. Liu and C. Miao, "Study on parking spaces analysing and guiding system based on video," 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, 2017, pp. 1-5, doi: 10.23919/IConAC.2017.8082071.

[12]. M. Karakaya and F. C. Akıncı, "Parking space occupancy detection using deep learning methods," 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, Turkey, 2018, pp. 1-4, doi: 10.1109/SIU.2018.8404749.

[13]. J. Ahmad, Z. Lewis, P. Duraisamy and T. Mcdonald, "Parking Lot Monitoring using MRCNN," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-4, doi: 10.1109/ICCCNT45670.2019.8944394.

[14]. E. J. Sen et al., "Advanced license plate recognition system for car parking," 2014 International Conference on Embedded Systems (ICES), Coimbatore, India, 2014, pp. 162-165, doi:10.1109/EmbeddedSys.2014.6953109.

[15]. https://cocodataset.org/#download

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Literature Review on Presentation Attack Detection using Deep Learning

Mayank Tiwari, Dhananjay Thomble, Atharva Thite, Digvijay Kapurkar, Pranav Surve, Dr. C H Patil
School of Computer Science, Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India

ABSTRACT

With the advent of facial recognition systems which are mostly used for authentication and authorization purposes, the main system that it acts on becomes vulnerable to different face presentation attacks that not only threaten the face recognition paradigm, but also the security and the integrity of the entire system as a whole. Presentation attack detection (PAD) which incorporate deep learning methods, have emerged as an effective measure to counter face presentation attacks. PAD deals with distinguishing between a real/live image and a spoof attack that come in various forms of graphical as well as digital media display like a still image, videos, etc. presented via mobile phones or any such devices. Implementation of neural networks, which make use of deep learning, that can be designed to specifically detect the liveness of an image based on various parameters that are absent in presented media such as body temperature or changing micro expressions, is an efficient way of implementing a face presentation attack detection system. Thus, a well-trained PAD system reinforces the deployed face recognition system, and also vastly minimizes the breach of security of the entire system from such methods.

Keywords—Presentation Attack Detection, Deep learning, Facial Recognition System, Spoofing mitigation.

I. INTRODUCTION

With the increasing popularity of facial recognition systems (FRS) as a preferred way of implementing biometric-based authentication, the risk and techniques of breaking such systems has increased as well. Face presentation attacks are the way to break FRSs. The objective of a presentation attack is to fool the FRS using a facial biometric artifact. A printed photo, the electronic display of a facial photo, replaying video using an electronic display, and 3D face masks are among the most common face biometric artifacts. As a measure to counter such sophisticated attacks, presentation attack detection (PAD) algorithms have emerged. PAD algorithms often are implemented by using deep learning techniques that carefully distinguish between a live image and a presented image. This is done via sophisticated methods like liveness detection, micro expression detection and analysis, etc. PAD algorithms do well to significantly increase the security of FRSs.

II. WHAT ARE PRESENTATION ATTACKS

A. Presentation Attacks

Presentation Attack is the act of presenting a document or data containing biometric characteristics or biometric synthetic patterns to the biometric data capture subsystem of a system or a device that takes biometric inputs through sensors [2]. The goal of such an attack is to interfere with the operation of the system and often threaten the integrity and security overall as well. Presentation attacks are often carried out with intentions of malpractice.

B. Domain of presentation attacks

Usually presentation attacks occur in facial recognition systems where the face or facial features of a particular individual are used for the authentication as well as for authorization purposes. Face presentation attacks are carried out by imitating a particular individual's face or facial features through various forms and methods and artifacts. Face presentation attacks aim to breach the face recognition system's security through means of imposture and tricking the recognition system by exploiting one of an FRSs many vulnerabilities.

C. General vulnerabilities of a face recognition system

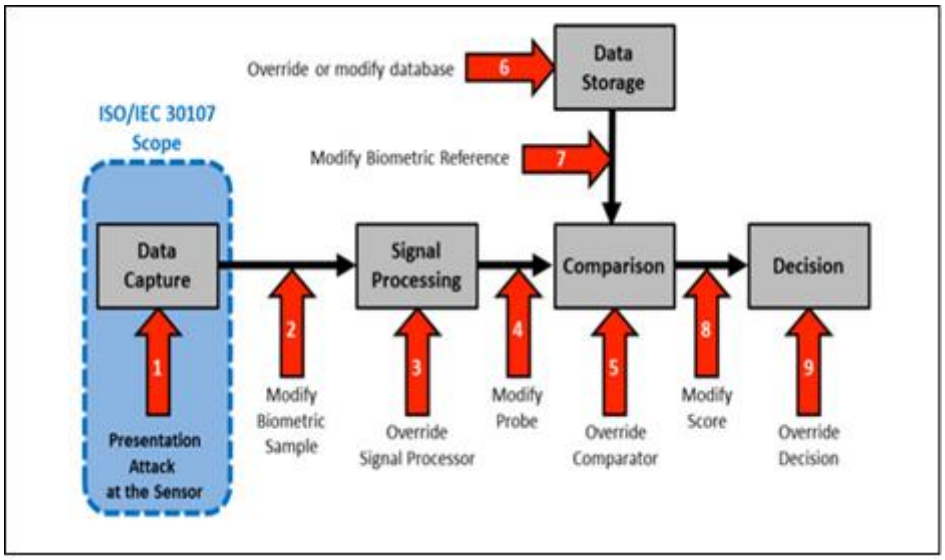


Fig 1. Vulnerabilities of an FRS. (image taken from ISO/IEC 30107-1)

Out of all the above depicted vulnerabilities, presentation attacks are usually targeted at the sensor. This is done conveniently by using a face biometric artifact of the target victim as an input to the sensor. Other attacks on the rest of the parts and subsystems of an FRS and the corresponding weaknesses in its defences are related to the integrity of the overall system. But since the point of input itself is sabotaged by the attackers, it can be said that just a sensor attack – that is, a presentation attack – is enough to compromise the integrity of the system.

D. Types of Presentation Attacks [2]

Presentation attacks can be divided into two types: active imposter presentation attack and concealer presentation attack.

- Active imposter attack: An active imposter attack is the presentation attack in which the attacker intends to be recognized as the target victim.
- Concealer presentation attack: A concealer presentation attack is the presentation attack in which the data capture intends to conceal his identity totally. The subject tries to not be recognized as any individual that might be stored in the system's database of known/recognized individuals.

E. Types of face presentation artifacts [2]

Face presentation artifacts are those objects or materials that are used to carry out/initiate the presentation attack. Depending on their application and method of working, face presentation artifacts are divided into two types: artificial and human characteristic artifacts.

- Artificial artifacts: Artificial artifacts are those artifacts that use artificial methods to generate the artifacts/objects, like a graphical or electronic print or a video.
- Human characteristic artifacts: Human artifacts are those artifacts that make use of humans to generate the artifact/object. They can be lifeless, altered, nonconformant, or conformant.

Out of these artifacts, artificial artifacts are the most widely used artifacts to generate the objects since they are extremely simple to generate, cost less and largely go undetected under the common eye, seem harmless and do not involve much hassle as compared to human characteristic artifacts which largely involve committing crimes of very high orders and seem very suspicious right from the beginning.

III. DIFFERENT APPROACHES TO CARRYING OUT FACE PRESENTATION ATTACKS

A. Face presentation attacks via Artificial artifacts

As mentioned earlier, the primary way of carrying out any face presentation attack (FPA) is by tricking the data capture subsystem at the sensor level through means of imposture. This is done with the help of various artifacts discussed earlier. Each of these artifacts or Presentation Attack Instruments (PAI) have their own approaches to carrying out an FPA.

1) FPA via Artificial artifacts

Artificial artifacts are those that are generated through artificial means. Depending on whether the generated artifact is a video, or an image, or a 2D/3D printed mask, artificial artifacts take two approaches.

- Complete approach: This refers to the complete generation of an artifact like a 2D/3D printed mask or a video, wherein the complete facial features of the targeted individual are processed and captured by the data capture subsystem (DCS).
- Partial approach: This refers to the partial generation of an artifact like a partially covered mask, a photo in which the targeted individual is wearing glasses, etc. This approach aims to restrict the number of facial features that are captured and processed. This often leads to occlusion of the target individual's face that hampers the recognition quality of the FRS and thus, makes it easy to bypass via an FPA.

2) FPA via Human characteristic artifacts

Human characteristic artifacts that involve using humans as the artifact or PAI have completely different and direct approaches. Human characteristic artifacts always ensure near-to-live or actual live detection of the facial

features of the targeted individual. Human characteristic artifacts are always employed through means of imposture.

- Lifeless approach: This involves using certain parts of the human body, usually in a lifeless state, like the cadaver part of the face. This ensures live detection of the exact facial features of the target individual as though he himself were standing in front of the DCS.
- Altered approach: This involves the alteration of some of the facial features of an imposter, through plastic and cosmetic surgical means. This can also be achieved through mutation of the faces via surgical methods. Another way of achieving this is through disguise.
- Nonconformant approach: This involves the usage of facial expressions that are manipulated to better appear like having similar facial features as that of the targeted individual.
- Coerced approach: This approach involves the actual presence of the target individual at the DCS. The individual is either forced or threatened to be there, or coerced into some activities that lead to him being taken advantage of. The latter usually ends up in the individual being in either a drugged state or straight up unconscious
- Conformant approach: This is the simplest approach that involves zero-effort impostor attempts. This can be carried out by people who look strikingly similar to the target individual like their twins.

IV. PRESENTATION ATTACK DETECTION

Presentation attack detection (PAD) is the activity of distinguishing between a live image/Bonafide image and a presented image/spoof attack [3], [4]. PAD is done to protect the system from various presentation attacks that it might be susceptible to, and is vulnerable to. PAD has been one of the most important topics in the facial recognition scientific community due to the increasing number of threats that FPAs pose. PAD has been in research and development since not that long ago. With that being said, research for implementing PAD in efficient and quicker ways has been undergoing with some incredible results. The idea behind PAD is simple: to detect human features that are otherwise absent in common presentation attack methodologies. There are several ways to achieve this.

A. PAD methods and state-of-the-art algortihms

With various forms and types of artifacts paving way to various approaches in carrying out presentation attacks, it becomes extremely important to develop systems that mitigate the risks of such approaches and artifacts. PAD systems are designed for this exact same purpose. There are a number of methods to implement PAD systems. Following is the classification of PAD methodologies and algorithms.

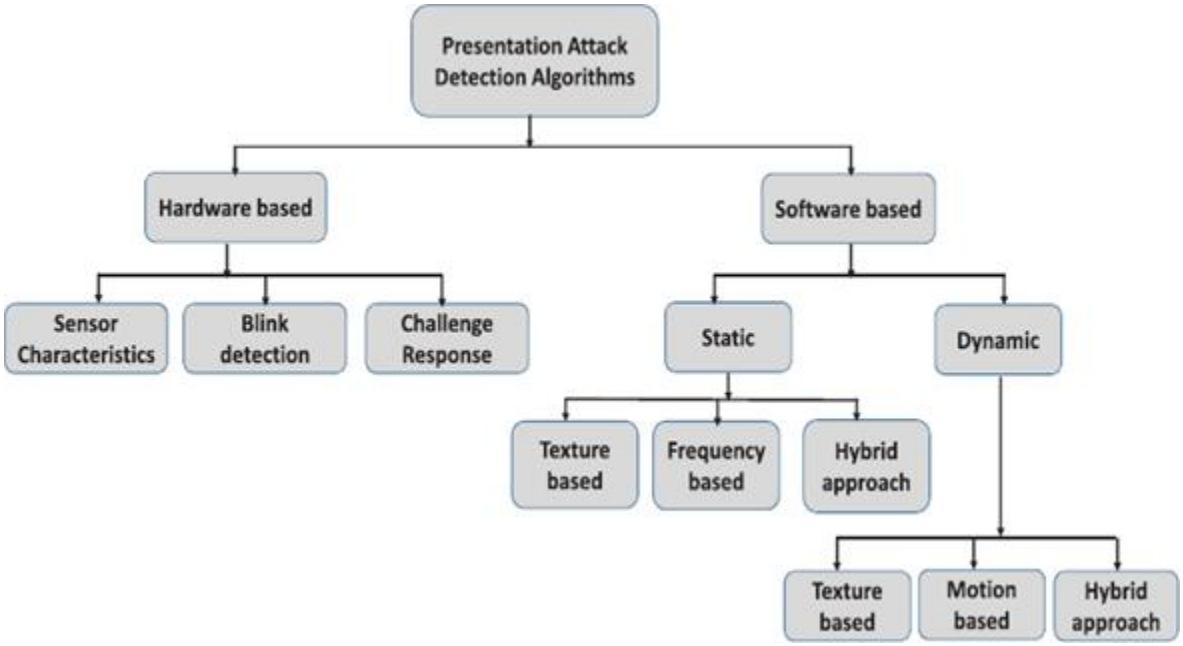


Fig 2. Classification of PAD methodologies and algorithms

1) Hardware based [1], [4]

Hardware-based methods explore the features of the human face (also called as facial components) using dedicated additional hardware components that work in conjunction with the face recognition sensor. These methods may also require an interaction with the hardware or a face capture sensor (such as eye blinking), which will also use software internally to process the captured face data [2]. The hardware-based methods can be widely classified into three types: sensor characteristics, blink detection, and challenge response.

- Sensor: The techniques developed in this method are based on exploring the features of the camera (or sensor) used to capture the face image (or video). The features of the sensor explored depend on the type of sensor used to capture the[2] face data, for example, measuring the variation of the focus with a light field camera (LFC) or measuring the reflectance from a near-infrared/thermal/multispectral face sensor or measuring the reflectance in a 3D scan.
- Blink detection: Blink detection is a commonly used liveness measure to mitigate spoofing attempts against face recognition systems. The idea behind blink detection is to continuously track the spontaneous action of eye blinks that are performed unconsciously. Blink detection can be carried out either using dedicated hardware or a software-based technique.
- Challenge response: The idea behind challenge-response-based presentation attack detection is to provide a separate user interface in which the response to a challenge is recorded and processed to identify a Bonafide presentation, for example, by tracking the gaze of the user toward a predefined stimulus.

2) Software-based [4]

Unlike hardware-based face PAD methods, which always require additional hardware components or user interaction, software-based methods are comparatively more efficient with low cost. This is achieved by designing an algorithm to distinguish between a real face and a spoofed image (or video). These schemes do not require any kind of user interaction and have better accuracy. Some popular software-based methods are discussed below.

- Texture-based: This kind of approach is very successful in detecting face presentation attacks, mainly because it can efficiently discriminate the artifact characteristics such as the presence of pigments (due to

printing defects), shade deformation (due to a display attack), and specular reflection (by the spoof medium) [4]. It makes use of one of the most popular algorithms, Local Binary Patterns (LBP), to detect those shades.

- Dynamic methods: Dynamic methods exploit the temporal information from videos to detect the relative motion across frames. One motion pattern occurs due to the intra-face variations, such as subconscious eye blinking, head rotation, and facial muscles movements [4].
- Hybrid methods: This kind of method fuses different features at the feature level or score level to further improve the detection performance. Combining different texture features is one direct way for feature fusion [4]. One such combination proved to be that of algorithms LBP and local shape features for printed photo attack detection. Another such hybrid measure was the fusion of LBP and color moments (effective for image quality analysis).

Most of the time, software-based PAD techniques are employed due to their cost effectiveness, efficiency and accuracy. Research done so far consists majorly on 2D presentation attacks, viz. Photo prints, video replays, etc.

V. CHALLENGES IN PAD TECHNIQUES

Although various techniques, methodologies and algorithms for PAD have been implemented successfully to great extents, they still have certain challenges in either their implementation or the working conditions.

A. Hardware-based PAD techniques challenges [2]

The following table describes the various challenges faced in the various implementations of hardware-based techniques, where the success of the system depends largely on the type and quality of the hardware used.

TABLE 1. HARDWARE BASED CHALLENGES

Methods	Advantages	Limitations
Sensor Characteristics	-Good generalizability	-Moderate computation cost -High sensor cost
Blink Detection	-Effective for display photo attack	-Computation overhead -Not effective for video replay and mask attacks
Challenge response	-Generalizability -Effective for both photo and display attacks	-High computation cost -User inconvenience -Not effective for replay

B. Software-based PAD techniques challenges [4]:

To generalize the challenges faced in software-based PAD techniques, there come up three major points, which are described below:

1) Lack of quantitative evaluation

Most existing surveys compare different algorithms by simply listing the reported results, without carrying out a quantitative evaluation on a common ground. Therefore, based on the results on different databases with different protocols, it is still difficult to understand how differently the existing methods can perform and which methods perform better for common 2D presentation attacks [4].

2) Limited algorithms and results [4]

Most competitions and the surveys presented a common evaluation framework for comparing different detection methods on the same face spoofing database. However, the gathered methods and results on only one database are limited and not thoroughly analyzed.

3) Lack of generalization ability evaluation

These surveys or competitions, and some existing detection schemes [4] as well, pay more attention to PAD performance based on certain testing or controlled environments. The robustness and generalization ability have not been carefully evaluated to show how well the state-of-the-art methods can perform in more challenging conditions, such as mobile scenarios or cross-database testing scenarios, which can reflect the real-world applications by providing high-resolution images and diverse attacks [4].

VI. CHALLENGES IN PAD TECHNIQUES

This chapter will be focusing on presentation attack detection techniques and methods that have been developed in the sphere of deep learning methodologies.

A. Deep Learning

Deep learning or deep learning methodologies is a derived, more complex and vastly extensive family of machine learning methodologies. Deep learning deals with the construction, training and implementation of the trained artificial neural networks to smartly work for the intended purposes it was designed for. The logic behind these artificial neural networks (ANN) is the same implication and working of a real human neural network. ANNs aim to work in the same way the neural networks function in a human body in conjunction with the brain, to carry out any tasks or activities.

ANNs are trained extensively over datasets using various learning approaches and principles established in machine learning. Over the course of the learning of an ANN, it undergoes evolution as the data fed to it increases. This causes the ANN to evolve over a number of generations to reach to the point where the ANN is fully trained under supervision, and any data fed to it – which is mostly dynamic and real-time – will be efficiently processed to give the desired results.

The whole process is quite akin to the learning, growth, development and evolution of a human which undergoes a similar process. The difference, though, is that a trained ANN tends to be static and symbolic, in that, it is only able to perform tasks and activities, no matter how dynamic, that fall in the range and domain of the data and purpose it was trained for. In comparison, a human or any biological brain works dynamically and is not restricted as an ANN would normally be. However, the tasks performed by an ANN is significantly efficient, better and of much higher orders as compared to that of the biological brain.

An ANN consists of a group of interconnected processing units called artificial neurons (analogous to biological neurons in a biological brain). Each connection between neurons can transmit a signal to another neuron. This output functionality is similar to a synapse in the biological brain. The receiving neuron can process the signal(s), which now acts as an input, and then signal downstream neurons connected to it. Neurons and synapses may also have a weight, which is the connection to the signal, that varies as learning proceeds, which can increase or decrease the strength of the signal that it sends downstream. A typical ANN architecture consists of an input layer, hidden layer (which comprises of a collection of neurons between the input and output layers), and an output layer. The layers may perform appropriate transformations on the incoming input signals. Signals travel

first from the input layer, then to the hidden layers (if any), and finally to the output layer, possibly after traversing the layers multiple times.

B. Popular Deep Learning Architectures

With the increasing efficiency of deep learning (DL) methodologies and the advancement of artificial neural networks, certain architectures were subsequently developed better suited to certain applications, and then expanded to several others more. Some popular DL architectures are discussed below:

1) Deep Neural Networks

A deep neural network (DNN) is a type of a neural network with multiple layers between the input and output layers [11]. In order to turn the input into the output, DNN tries to find the relationship whether linear or not [11]. The network moves through the layers calculating the probability of each output [7]. Since this type of neural network has many hidden layers, it has, therefore, been classified as a "deep" neural network. Compared to a shallow network (single layer), the extra layers of the DNN facilitate modeling of complex data with fewer units by composing features from the lower layers.

2) Convolutional Neural Networks

Convolutional neural networks (CNN) are also called as shift invariant or space invariant artificial neural networks [8]. They are based on shared weights architecture [9], [10] and make use of the principles of convolution in mathematics. CNNs are most commonly used in visually analyzing images and pictures. The hidden layers of a CNN typically consist of a series of convolutional layers that convolve with a multiplication or other dot product [12].

3) Recurrent Neural Networks

Recurrent neural networks (RNNs) are a superset of feedforward neural networks, and possess the ability to selectively pass information across sequence steps, while processing sequential data one element at a time [13]. Thus, they can model input and (or output) consisting of sequences of elements that are not independent. Additionally, recurrent neural networks can simultaneously model sequential and time dependencies on multiple scales [13].

4) PAD with Deep Learning

Presentation attack detection can be efficiently performed, to a great extent, by making use of deep learning methodologies and classification algorithms. Since convolutional neural networks have applications in analyzing images, a deep learning model that makes use of CNNs can be implemented to serve as PAD subsystem in an FRS [1], [3].

A deep CNN architecture for PAD can be in the following way [1]. A preprocessing stage including face detection and facial components detection is used before feeding the images to the CNN [3]. Once the CNN is trained, the feature representation obtained from CNN is used to train a support vector machine (SVM) classifier and used for final PAD task.

An FRS will be used to extract the local binary features of the face detected. These extracted features are then used to learn linear regressors in each cascade. The CNN is more capable of learning discriminative features from backgrounds [1]. In the convolutional layers, response normalization layers are used for the outputs of the first and second convolutional layers [1]. The max-pooling layers are plug to process the outputs of the first, second and the last convolutional layers [1].

After the learning of extracted features, a classifier, e.g. an SVM will then be used for the classification purpose to learn and be used for PAD or anti-spoofing measures. Thus, a CNN can be used to detect a spoofing attempt carried out on the DCS of an FRS – in principle.

VII. CONCLUSION

With presentation attacks on the rise thanks to modern technology, and the ways to carry it out getting even more sophisticated, the implementation of presentation attack detection systems is the way to counter them. Several challenges associated with hardware-based PAD systems, most notably the cost of installation as well as maintenance, software-based PAD systems that implement deep learning-based CNNs is the logical way forward. Although CNNs are not yet completely fool proof as there does not yet exist an all-solving CNN to tackle every kind of 2D and 3D PAD under every condition, they have proved to be very effective against PAs. This seminar has successfully discussed the several types of PAs, approaches, different ways of countering them and how AI or CNN can be used for the same.

VIII. REFERENCES

[1]. Jianwei Yang, Zhen Lei and Stan Z. Li, “Learn Convolutional Neural Network for Face AntiSpoofing", arXiv.org, 2014.

[2]. Raghavendra Ramachandra and Christoph Busch, “Presentation attack detection methods for face recognition systems: A comprehensive survey”, ACM Computer Surveys, 2017.

[3]. Anjith George, Zohreh Mostaani, David Geissenbuhler, Olegs Nikisins, Andre Anjos ´ and Sebastien Marcel, “Biometric Face Presentation Attack Detection with Multi-Channel Convolutional Neural Network”, arXiv.org, 2019.

[4]. Shan Jiaa, Guodong Guob, Zhengquan Xua, Qiangchang Wangb, “Face presentation attack detection in mobile scenarios: A comprehensive evaluation”, Elsevier, 2019.

[5]. Guohao Ju, Xin Qi, Hongcai Ma, and Changxiang Yan, “Feature-based phase retrieval wavefront sensing approach using machine learning”, Optic Express, Vol. 26, Issue 24, pp. 31767-31783 (2018).

[6]. Avi Baum, Or Danon, Mark Grobman, and Hadar Zeitlin, “Artificial neural network incorporating emphasis and focus techniques”, United States Patent, Patent No. : US 10 , 387 , 298 B2, Aug . 20 , 2019.

[7]. Mrs. R.A.Fadnavis, “Application of Machine Learning For Survival Analysis- A Review”, IOSR Journal of Engineering (IOSRJEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719, Vol. 09, Issue 5 (May. 2019), ||S (XI) || PP 56-60.

[8]. Valueva, M.V.; Nagornov, N.N.; Lyakhov, P.A.; Valuev, G.V.; Chervyakov, N.I. (2020). "Application of the residue number system to reduce hardware costs of the convolutional neural network implementation". Mathematics and Computers in Simulation. Elsevier BV. 177: 232–243. doi:10.1016/j.matcom.2020.04.031. ISSN 0378-4754. S2CID 218955622. Convolutional neural networks are a promising tool for solving the problem of pattern recognition.

[9]. Zhang, Wei (1988). "Shift-invariant pattern recognition neural network and its optical architecture", Proceedings of Annual Conference of the Japan Society of Applied Physics.

[10].Zhang, Wei (1990). "Parallel distributed processing model with local space-invariant interconnections and its optical architecture". Applied Optics. 29 (32): 4790–7. Bibcode:1990ApOpt..29.4790Z. doi:10.1364/AO.29.004790. PMID 20577468

[11].Handan Kulan, Tamer Dag, "In silico identification of critical proteins associated with learning process and immune system for Down syndrome", PLoS ONE 14(1):e0210954, DOI:10.1371/journal.pone.0210954, January 2019

[12].Subhana T B, Prof. Shamna A R, "Detailed Investigation on Convolutional Neural Network in Deep Learning", International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-7, Issue-8, August 2021, ISSN: 2395-3470

[13].Zachary C.Lipton, John Berkowitz, Charles Elkan, "A Critical Review of Recurrent Neural Networks For Sequence", arXiv:1506.00019v4 [cs.LG] 17 Oct 2015.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Recognize Human Emotion from Speech using Neural Network

Bhoomi Rajeeep[1], Hardik B. Patel[2], Sailesh Iyer[3]

[1]MTech Student, Department of Computer Science Engineering, Rai School of Engineering, Rai University, Ahmedabad, Gujarat, India

[2]Assistant Professor, Department of Computer Science Engineering, Rai School of Engineering, Rai University, Ahmedabad, Gujarat, India

[3]Professor, Department of Computer Science Engineering, Rai School of Engineering, Rai University, Ahmedabad, Gujarat, India

ABSTRACT

Mood and behaviour detection with the help of the voice analysis helps detect the mood of the speaker by analysing the frequency of the voice. This paper aims to study the various states of the mood such as the happy, sad as well as the detection of the behaviour using Machine Learning algorithms and Artificial Intelligence. Proposed model is able to detect the frequency of the voice with the help of training data and machine learning algorithm. Algorithm is able to detect the frequency and help identify the mood of the speaker as well as the behaviour. Behaviour can be identified in terms of positive or the negative. Proposed model helps to avoid the health issues related to the mental situation also used in the application of the medical as well as gaming. It is a challenging task to identify the mood of the speaker by analysis of the voice frequency because many factors affect the analysis. Proposed model consists various machine learning as well as Natural language processing tasks and the data visualization tools to analyse the outcome.

Keywords — Detection of voice, Feature Extraction, Optimization, Classification, Speech analysis, Log-Mel Spectrogram

I. INTRODUCTION

We are able to detect the mood of any person by just seating with him or her even if we don't know him or we meet him or her first time by simply analysing the frequency of the tone of a particular person [1]. Past study of the voice analysis suggests that the by analysing the frequency of the voice model is able to predict the sentiment as well as emotion associated with the voice [2]. Research also proves that by defining the perception of the voice, model is able to detect the state of the mind for a particular person [3].

Research study based on the information retravel of the voice suggest that with the help of analysing the voice of a person, model is able to distinguish the perception of the person as well as also able to classify the perception

such as the affirmative or the defeatist which helps model to further classify the exact felling associated behind the voice [4].

Analysis of the sentiment with the help of the person's voice make it possible to recognize the feeling associated with the speech as well as non-lexical sentiment analysis helps to analyse the signal in an accurate manner. With the help of the speech signal, model is able to retrieve the

Information related to the state of the person. With the help of linguistic analysis, model is able to identify the affection of the person. Conceptual knowledge helps to identify the perception of the person's state and many research suggest that lexical based analysis helps model to analyse the sentiment associated with the speech or voice. Vocal split of the particular language helps to identify the emotions associated with the voice [5].

II. PROPOSED MODEL

To implement the proposed model, various research work in the field of the voice analysis is taken into account and major problems associated with the methods in the current system is identified. Solutions towards the problems are designed by either developing a new method or by modifying the existing algorithm to improve the overall accuracy of the prediction.

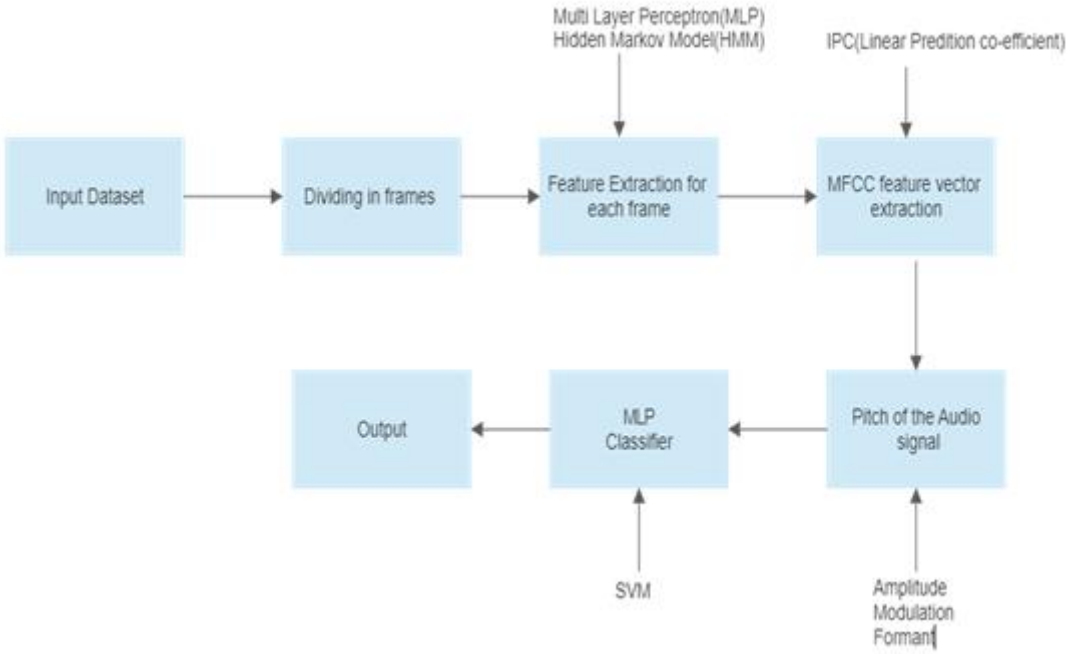


Fig 1. Illustration of the proposed system

System consists following modules, which are listed below.

- Selection of the database
- Conversion of the data into the collection of frames
- Feature extraction from the collection of the frames
- Extraction of the frame with the help of MFCC method
- Identifying the pitch of the audio signal
- Classification with the help of the MLP
- Generation of the output with the help of python

Following section describes the important modules needed to implement the system and also describes the proposed solution needed to improve the previous methods in a brief manner.

Feature Extraction

During the study of the research work, major problems associated with the feature extraction method are identified which are given below.

Multi Layer Perceptron uses a initial parameter in an multiplicative order which increases the number of layers required and generate many redundant data. Process consumes lots of thime and performance of the model decreases. MLP model uses a geographical data which are spatial by nature and it is hard to process the spatial data [6].Many reseach work uses hidden markov model to identify the hidden state of the data and suffer from the following disadvantage.

In Hidden Markove model, parameters are unstructured in the nature which leads the system to unstable stage because there are lots of dependencies in between the hidden states [7].

To overcome the problem, proposed model implement the unique solution with the help of the discrete fourier transform and Mel Frequency Wrapping technique which are illustrated in the following figure.

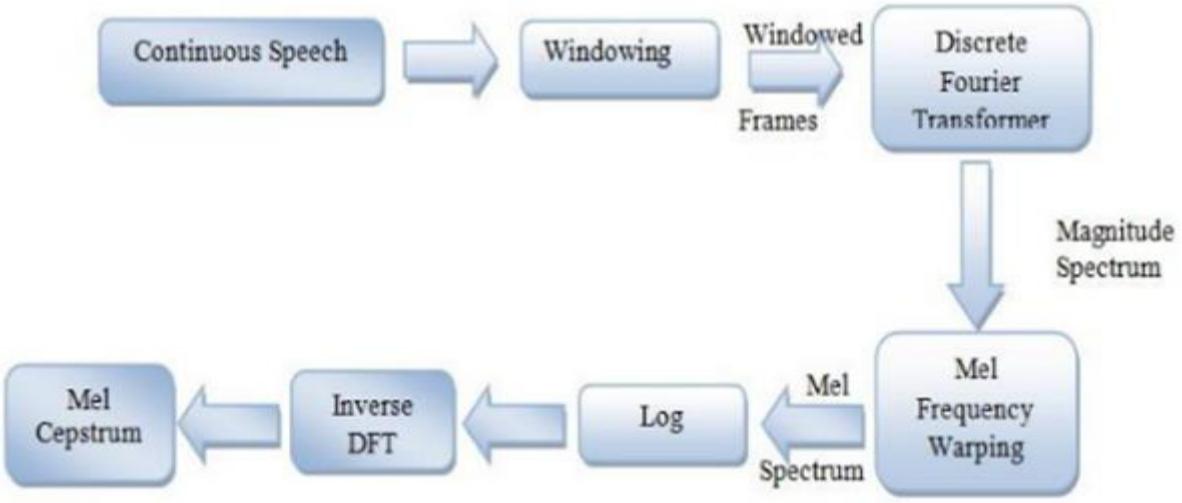


Fig 2 : Use of Discrete Fourier Transform for the extraction of the feature

By using the Discrete Fourier Transform, loss less transformation of the data can be achieved as well as it also provides utilization of all the parameters associated with the signal such as the amplitude of the signal, phase of the signal, as well as the nature of the signal which helps the conversion of the signal from into the frequency domain [8].

MFCC Feature Vector Extraction

Model used for the implementation of the speech as well as filtering has been studied and brief literature review carried out on the same. Coefficient used for the designing the predictive linear model is also studied and this section describes the problems associated with the methods that are previously used in the research work along with the appropriate solution proposed by the current model.

Quality of the signal decreases drastically while bitrates of the signal consist low quality. Also, when distance is longer linear predictive coefficient suffers from the lossy compression. With the help of the MFCC feature vector extraction process it is possible to implement the Quantum Neural Network which provides the parallel computation and reduce the time of the processing. IPSOQNN technique is useful for the fast recognition of the signal and QNN trained with the help of the IPSO technique which provides a greater accuracy of the prediction

and also provides a global optimization. With the help of the MFCC feature extraction technique complexity of the model can be reduced [9].

Pitch of the Audio Signal

In the literature study of the amplitude modulation technique, problems are identified such as amplitude modulation works well only with the higher bandwidth and requires original signal with the higher bandwidth. In the amplitude modulation technique detectors are very sensitive towards the noise when signal consist larger portion of the noise it is very difficult to recognize the signal [10].

To deal with these problems pitch detection method is used in the proposed model which is able to distinguish the human voice and instrumental voice in an effective manner. With the help of the pitch detection method, it is feasible to identify the gender of the human. Timestamp can be track with the help of the pitch detection method. At last pitch detection method is also capable to identify the age of the person in an effective manner [11].

MLP classifier

In the literature review phase Support Vector Machine has been studied and problems associated with this method is identified such as SVM underperforms when dataset is large. SVM overlap the target class when signal has more noise and at last if there are more features are available in the training set then it is not possible to identify the feature in an accurate manner [12].

To resolve these problems Multi-Layer Perceptron based classification is used in the proposed model which provides efficient results in case of data set is large in the size. MLP is also capable to manage the thousands of the data without eliminating the data or reducing the size of the dataset. MLP considers all the parameters available in the dataset and considers each parameter during the classification phase [13].

III. IMPLEMENTATION OF THE MODEL

Model consist various phases which are described in below section.

Dataset

RAVDESS (Ryerson Audio-Visual Database of Emotional Speech and Song dataset) is utilized to train the model which consist more than 7356 files and rated based on the emotional validity as well as intensity and genuineness.

Preparation of Data

From the dataset emotion label are extracted by implementing the function named as glob (). This function is able to create a path which helps to define a path at which data are stored.

Feature Extraction

Mel spectrogram is used for the feature extraction with the help of the library called Librosa. Log-Mel spectrogram of the audio is assigned to the model and average of the available values is calculated. After the calculation of the average, this value is again converted into the data frames. With the help of the following code this process is implemented.

```
def extract_feature (file_name, mfcc,
chroma, mel):
   with soundfile.SoundFile(file_name) as
sound_file:
      X = sound_file.read(dtype="float32")
      sample_rate=sound_file.samplerate
      if chroma:
        stft=np.abs(librosa.stft(X))
      result=np. array ([])
      if mfcc:
mfccs=np.mean(librosa.feature.mfcc(y=X,
sr=sample_rate, n_mfcc=40).T, axis=0)
      result=np.hstack((result, mfccs))
    if chroma:

chroma=np.mean(librosa.feature.chroma_stft
(S=stft, sr=sample_rate).T,axis=0)
      result=np.hstack((result, chroma))
if mel:

mel=np.mean(librosa.feature.melspectrogra
m(X, sr=sample_rate).T,axis=0)
      result=np.hstack((result, mel))
return result
```

With the help of the Librosa library absolute value is calculated from the available element. MFCC is applied to represent the information related to the voice. There are 13 different coefficients are used to represent the feature and envelop it into the spectra. Higher dimension of the features is eliminated to simplify the spectra. MFCC identify the different types of the phonemes using difference between the features.

Outcome is transferred to the stack with the help of the hstack () function which is capable to store the data in a one - dimensional array in the form of a single dimension.

Signals

Model used a bandwidth of the 44.1KHz signal which are collected from the various samples of the air pressure with respect to the time and measures it into data per second.

Fourier Transform

Fourier Transform is used to convert the amplitude which are collected from the various samples into the frequency with the help of the mathematical equations. With the help of the Fourier Transform model is able to convert the signal from the frequency domain to the time domain and output is known as the spectrum.

Spectrogram

Speech signals are known as non-periodical signals because it varies with respect to the time. With the help of the spectrogram, it is possible to represent the signal over a time domain and Short-Time Fourier Transform is

used to define a spectrogram. FFT is performed on the voice signal to convert it into the spectrum by dividing whole window into the small segments of the signal.

Male Scale

It is used to define the unit of the pitch, which is represented by the equal distances in the pitch with respect to the distance of the listener. Reference scale is considered between the 1000 mels to the 1000 Hz tone.

MLP for the classification

MLPClassifier is a type of the feed forward neural network which is used for the classification of the data or voice or images.

Accuracy score function is utilize to check the accuracy of the model with the help of the SKLearn library and following code is used to implement the MLP classifier.

model=MLPClassifier (alpha=0.01, batch_size=256, hidden_layer_sizes= (300,), learning_rate='adaptive')

IV. CONCLUSION

Proposed model utilizes various methods such as the Mel Scale, Multi-Layer Perceptron, feature extraction to improve the predictive accuracy of the model. Also, research identify the problems associated with the previous research work and try to improve or solve the problems associated with the methods or the techniques.

V. REFERENCES

[1]. Parlak, "Emotion recognition from the human voice," 2013.
[2]. Gong, "A Research of Speech Emotion Recognition Based on Deep Belief Network and SVM," Hindawi, pp. 1-16, 2014.
[3]. S. An, "Study on Method of Feature Selection in Speech.," (IJACSA) International Journal of Advanced Computer Science and Applications, pp. 1-5, 2014.
[4]. Belin, "Understanding Voice Perception.," British journal of psychology, pp. 1-15, 2011.
[5]. Jurek, "Improved lexicon-based sentiment analysis for social media analytics," Springer, pp. 1-9, 2015.
[6]. Salhi, "Voice Disorders Identification Using Multilayer Neural Network," International Arab Journal of Information Technology, pp. 177-185, 2010.
[7]. "An introduction to hidden Markov models," IEEE, vol. 3, no. 1, pp. 4-16, 1986.
[8]. Thyagarajan, "Discrete Fourier Transform," in Introduction to Digital Signal Processing Using MATLAB with Application to Digital Communications, 2019, pp. 151-188.
[9]. Hossan, "A novel approach for MFCC feature extraction," in Signal Processing and Communication Systems, 2011.
[10]. Kuwalek, "AM Modulation Signal Estimation Allowing Further Research on Sources of Voltage Fluctuations," IEEE Transactions on Industrial Electronics, vol. 67, no. 8, pp. 6937-6945, 2019.
[11]. Bartošek, "Comparing Pitch Detection Algorithms for Voice," Department of Circuit Theory, FEE CTU in Prague, 2007.
[12]. Aida-zade, "Speech recognition using Support Vector Machines," in IEEE 10th International Conference on Application of Information and Communication Technologies (AICT), 2016.
[13]. Chi, "MLP classifiers: overtraining and solutions," in International Conference on Neural Networks, 2002.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Honeypot - An Overall Overview

Mihir Sharma[1], Pranay Ranjan[1], Divya Jangid[1]
[1]MCA, Department of Computer Science, MITWPU, Pune, Maharashtra, India

ABSTRACT
The objective of this review paper is to show how Honeypot Helps Hackers or Intruders to infiltrate a system and some other aspects using honeypot like using it with IOT and Cloud. The paper also talks about how it is beneficial and its different types. Honeypots are used in many scenarios when the let the intruder attack and then inform the system.
Keywords: Honeypot, Honeyd, Cloud, Dynamic Configuration, Intruders, Security

I. INTRODUCTION

There is Classic security paradigm which is protect, detect and react where first is related to protect the network then detect failures in that defense and how to react on those mechanisms. In this honeypot acts as a trap for the intruders and bait them based on the purpose of that trap with the primary purpose to gather information of the intruders without compromising our security. This security mechanism was discovered way back in 1980s. Then main attempt of the hacker being to find out any vulnerabilities in the system and exploiting them. Honeypots also help to find if the security of the particular database or software is in threat example being if the intruder somehow reaches the honeypot that means the security is in danger. Also detecting if the attack is from inside if the employee has some malicious intents. We can even place more than one honey pot into the system creating a group called Honeynet
honeynet (honeywall).
a honeypot is placed behind a honeywall so that the hackers cannot reach a sole honeypot and hacking it to attack out system. the most crucial thing being able to control data and capture the data honeypot does a really good job at protecting a user. Honeypot is used in many corporative networks. They mostly propagate to the nearest address. As the internet era grew the main purpose was to do research about networking and its security aspects .it is an intrusion detection system also known as IDS used to exploit the vulnerabilities. An experiment was carried out in Rio Grande do sun in Brazil with the objective to measure the unusual traffic result being more than 65 thousand hosts were being emulated. IDS is used to detect the malicious activities where it runs in the background and causes no disturbance and if some malicious activity is detected then a notification is sent to the admin of the network. Another experiment was carried out in 1999 where a host was kept open and within only 15 minutes it was compromised where after he erased the logs of the system.

Malware poses an increased threat to information security. According to GData the number of malwares in 2014 are increasing by 2.3 times which resulted into 59,98,685 as the total number of recorded malwares. Due to the spread of this computer malware, organizations have started to combine the security system devices such as firewall and IDS which helps to track the activity of attacker and thereby protect their resources but then too it becomes difficult for them to identify the virus or worms or the new methods that are used by the attackers. So Honey pot is used to detect the malware in which suspicious packages are being trapped using machine learning. Honeypot is designed to be unsafe to entice Raiders because its purpose is to understand the techniques or methods used by the attackers. Honeypot also uses classification algorithms such as decision tree and support vector machine (SVM).

The use of honeypot is best working under Ubuntu OS. With the increase in the development of computers and technology there are people who want to access information and use it many different ways .SSH or security shell is a protocol that allows us to access and remotely control a personal computer by encrypting the data between the server and the client. honeypot works as a trap as discussed but here are some important facts about malicious attacks and what can be the counter measure. Here are some most common login id and passwords.

TABLE I COMMON LOGINS

№	Login
1	admin
2	root
3	master
4	login
5	user

TABLE II COMMON PASSWORDS

№	Password	Percentage of use
1	123456	0.38%
2	password	0.18%
3	qwerty	0.1%
4	root	0.08%
5	test	0.06%

II. BENEFITS

It can collect highly valuable data which can be useful against the attackers on the move. It also allows the white hat community in studying that what the intruders are doing so that they are not exploited and Honeypots provide deterrence honeypots are placed just to know the activity about the hackers through the log files. honeypots are place to capture the specific pattern of data. honeypots also capture the tools of the hackers. honeypot gets the information about the attacks which are newly found. Honeypot is placed with firewall that is before firewall or after firewall because these are the ways hacker can get into system. and then we can get maximum amount of information from hacker's activity. we can get to know about their tools and then we can secure our system against their tools.

III. TYPES

Honeypots are a wide stream and can be classified based on their deployment and based on their level of involvement. Based on deployment, honeypots may be classified as:

1. Production honeypots
2. Research honeypots

1) Production honeypots

These are easy to use, capture only limited information, and are used primarily by companies or corporations. Production honeypots are placed inside the production network with other production servers by an organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypots do.

2) Research honeypots

They are run to gather information about the motives and tactics of the Black hat community targeting different networks. These honeypots do not add direct value to a specific organization, instead, they are used to research the threats organizations face and to learn how to better protect against those threats. Research honeypots are complex to deploy and maintain, capture extensive information and are used primarily by research, military, or government organizations.

Based on design criteria, honeypots can be classified as

1. Low-interaction honeypots
2. Medium-interaction honeypots
3. High-interaction honeypots

a) Low-Interaction Honeypots

In low interaction we let hackers access the limited system for the limited time so hackers cannot hack the system and we'll got to know about their activities and we are securing our system about knowing little things about hackers. this interaction is used in companies. It gathers information with little risks being placed on the safe side in a network and collecting logs

Medium-interaction honeypots

The medium interaction honeypot combines both low and high interaction honeypots with giving the necessary information and also looking out for malware.

High-interaction honeypots

The motive of this interaction is to give hackers access of whole system and get maximum information of it. this technique is for researchers, who wants to know about new techniques of the hackers. it lets the intruder to fully interact with the system and there may be chances where the security is compromised with the result being they provide maximum security.

IV. HONEYPOT FOR IOT

There has been an exponential increase in the number of devices operating in the realm of Internet of Things(IOT). These devices operate over weak operating systems and limited network resources. This paradigm makes these devices extremely susceptible to malicious cyber-attacks.

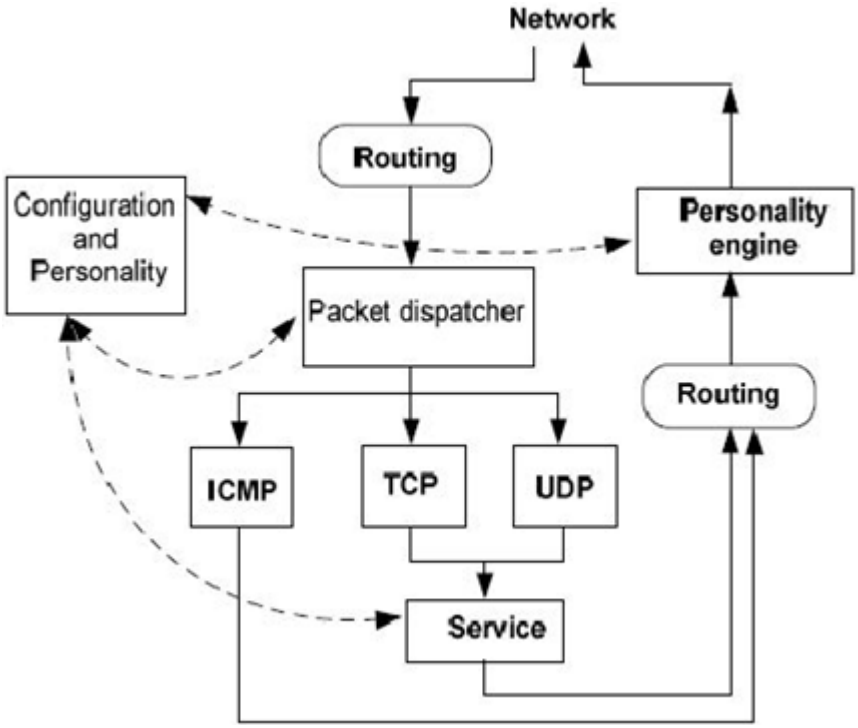
Honeypot can prove to be an effective tool in guarding IoT devices against malicious attacks.

According to a recent report, the number of devices operating as IoT devices across the globe has crossed 11 billion mark. Effective protective measures become imperative to ensure these devices are not exploited, especially when it has been constantly reported that these devices are continuously unfiltered and exploited as they have limited to absolutely null security constraints. According to a report, an unethical hacker junta defiled thousands of IoT devices in 2019. This time they used an effective malicious attack called "Distributed Denial of Service Attack(DDoS)" which is a sub class of "Denial of Service" Attack(DoS). On a different occasion, malicious codes were injected into thousands of IoT devices. A botnet named Hide N Seek(HNS) was effectively used to execute these attacks through several remote commands. IoT devices are mostly sensor based systems with limited abilities, this makes it difficult to implement sandbox and other security protection technologies on these devices.

Monitoring the suspicious behavior of the IoT devices and effectively identifying the threats are of prime importance to protect IoT devices. Studying characteristics of data and thorough analysis of malicious behavior along with study of nature of attacks is of utmost importance.

This requires us to collect malicious samples of IoT first. This is where Honeypot comes to risqué. It proves to be an effective method of capturing malicious requests and collecting malicious behavior samples. Honeypot lures the attacker by putting up some proxy hosts and network services. Then it captures the attack behavior and analyses the tools and methods adopted by the attacker. Finally, it deduces the intention and motivation of the attacker. Hence, honeypot has ability to enhance the security protection capability of real time systems and can effectively help defense party to understand the security threats. Recently, a Situational Awareness Model was deployed with MYSQL database to effectively store and study the data. After 6 months of data collection. an analysis was performed. The outcome was impressive as the system efficiently detected malicious activities such as botnet scanning as well as outbreak of worms. Honeypot is capable of detecting and recording myriad of attacks which might prove impossible manually. Some researchers even proposed that implementing data mining techniques to analyze and study recorded traffic and extracting useful information will further reinforce the security.

Prominent security expert, Neil Provo, proposed a seminal honeypot based framework "Honeyd". Honeyd has the capability to simulate real computers under the network layer. It comprises several components such as protocol processing units, traffic allocation units and fingerprint matching units. The protocol processing unit has the capability to impersonate Internet Control Message Protocol(ICMPD), User Datagram Protocol(UDP), Transmission Control Protocol(TCP). The traffic allocation unit sends data packet to established honeypot. The current network's IP address is assumed to be virtual address of honeypot. A single host has the capability to deploy several honeypots.



V. FIVE YEARS OF DATA ANALYSIS

Ransomware attacks are the most reported types of attacks and it is producing most damages. Ransomware attack is like hacking into the system then take the access and hack all the data from the targeted machine after that decrypt the data for the money. now we'll talk about 5 years of results.

First Year – 2014

The first year was dedicated to research for the setup of first honeypot at the places. After a minute of first honeypot was live attackers were ready to attack to the systems and the first ones were trapped. most of the attackers tried to install the rootkit and they realized they are dealing with honeypot. they tried the most tried passwords and got into the system but they did not get anything of the data.

Second Year - 2015

second year lots of tests were done to understand if some of the data are valid or not. here automization technique was done and after that analysis of that data was happened which was to filter automatic scanners of the human hackers.

Third year- 2016

This year we characterized the most amount of attacks hacking data was collected. that time 2 more honeypots were placed. the grade of difficulty was increased but still we were having more attacks. this year because of the number of honeypots placed we were facing problems in maintaining and analyzing it.

Fourth Year – 2017

This year one honeypot was shut down because it was having least amount of traffic and also there was duplication of attacks this year. some attackers understood it is honeypot and they launched a service against it. but in the company's data was collected daily so we were changing the IP of the VPS used.

Fifth Year - 2018

This year the goal was to analyze and scan the source code for the algorithm that might be used inside ransomware tools. The focus was not to gain number of attackers but to get the output control for the system using the data of algorithms we got from source code.so we can stop the hackers before the system get damaged.

VI. BUILDING HONEYPOT ON CLOUD

we know about local honeypots which are placed at local domain. these honeypots are most common in companies that doesn't use cloud services at all. now we'll talk about cloud honeypots. This type of honeypots are installed in the cloud with so many advantages as well as restrictions. they are used only in the companies which have part of their system located in the cloud. honeypots also come with major advantages that they easy to install, deploy fast and can be restored easily if corrupted. how we can implement honeypot into the cloud. if we want to implement honeypot then the easiest way is to implement it in the cloud for testing without being worried about the security of our system. for e.g. we will use cloud VPS loaded with Ubuntu 14.4 LTS. and for the honeypot software we will use easiest way to implement it is a KIPPO honeypot. KIPPO is able to do SSH service which is able to listen and log all the login activities. Now we will know about the things which hackers follow at the time of hacking

1)Reconnaissance and Scanning:

most of the times hackers target the system but sometimes they are searching for the weak servers so they can make proxies of them and hack the system. for this search they use scanning tools which are available for free.

2)exploiting phase:

after the hackers have the information of the IP's of the hosts which are live om the internet, they will go the next phase they will try to grab the weakest point of the victim that is the mostly used passwords which is also called as dictionary attacks.

3)Maintaining access and hiding tracks:

The hackers manage to hack the system, so when he hacks the system that time he will try to remove the log files to hide his track and he will also try to left a backdoor so next time he can hack the system easily.

Some important aspects of implementation.

Kippo honeypot will be installed into the Ubuntu vps in the cloud and the SSH will be open because the most hackers search for the default open SSH port, we will assign this port to the kippo.

we need to keep our servers up to date so the attacks can be avoided. Modify the SSH configuration by running few commands. Before installing kippo we have to make sure that we have downloaded two dependencies that is python dependency (because Kippo is a python script) and second is to install a subversion to install kippo because our vps is Ubuntu vps creating the kippo user. Now we have to change the kippo server port so that attacker will see the port as normal one. Download the kippo and configure it and after downloading change the default hostname because an experienced hacker is aware of characteristics of kippo and hacker will understand that it is honeypot. Start the kippo now all the login details will be in the log files that is kippo.log. file. here we'll be able to understand the also able to read from the date and time, combinations of passwords or user tried. from the kippo graph we can get the real values of data interpretation.

VII. CONCLUSION

With the increase in number of intruders/hackers trying to infiltrate a system, honeypot plays a major role if stopping and even trapping them. Not only trapping but collecting logs and information is a key factor that gives honeypots an upper hand. Even though intruders are stopped from attacking but they will keep on trying to attack a system and in some or the other way the honeypot are also receiving minor upgrades.
Working with/on cloud and IOT its performs some good work managing the hackers.

VIII. REFERENCES

[1]. Shaik Bhanu, Girish Khilari, Varun Kumar: Analysis of SSH attacks of Darknet using Honeypots Computer Science, Veltech University (CDAC) IT Network & Systems, CDAC, Pune.India 3Computer Science, Veltech University, Chennai, India. 2004
[2]. ROMAN JASEK, MARTIN KOLARIK, TOMAS VYMOLA: APT detection system using honeypots. CZECH REPUBLIC.
[3]. Robert Koch, Mario Golling and Gabi Dreo: Attracting Sophisticated Attacks to Secure Systems: A new Honeypot Architecture. Robert Koch, Mario Golling and Gabi Dreo Universitat der Bundeswehr M ¨ unchen ¨ Department of Computer Science 85577 Neubiberg, Germany (2013)
[4]. Seema Sharma: Detection and Analysis of Network & Application layer Attacks using Maya Honeypot. Computer Science and Engineering Amity University Uttar Pradesh Noida, India (2016)
[5]. Honeypot in Network Security: A Survey
[6]. Marius Lihet, Pr.Dr. Vasile Dadarlat : Honeypot in the cloud
[7]. Stephen Brown, Rebecca Lam, Shishir Prasad, Sivasubramanian Ramasubramanian, and Josh Slauson: Honeypots in the Cloud. University of Wisconsin – Madison 2012
[8]. Marius Alin Lihet, vasile Dadarlat: How to build a honeypot system in cloud, IEEE 2015
[9]. Arash Barfar, Shahriar Mohammadi: Honeypots: Intrusion deception, Research Gate 2017
[10]. Émerson Salvadori Virti, Liane Tarouco, Lisandro Z. Granville: Honeypots as a Security Mechanism , Computer Science Institute, Universidade Federal do Rio Grande do Sul - UFRGS Porto Alegre, Brazil (2006)
[11]. Vinu V Das: Honeypot Scheme for Distributed Denial-of-Service Attack, SAINTGITS College of Engineering, Kottayam.
[12]. K.R. Sekar, V. Gayathri, Gollapudi Anisha, K.S. Ravichandran, R. Manikandan: Dynamic Honeypot Configuration for Intrusion Detection School of Computing, SASTRA University, India (2018)
[13]. Mr. Kartik Chawda, Mr. Ankit D. Patel: Dynamic & Hybrid Honeypot Model for Scalable Network Monitoring, Parul Institute of Engineering and Technology, Limda, Waghodia, Vadodara, ICICES2014
[14]. Development and Implementation of a Honeypot-Trap, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) Moscow, Russia
[15]. Iik Muhamad Malik Matin, Budi Rahardjo: Malware Detection Using Honeypot and Machine Learning. School of Electrical Engineering and Informatics, Bandung Institute of Technology (2019)
[16]. Weizhe Zhang, Bin Zhang, Ying Zhou, Hui He, Zeyu Ding: An IoT Honeynet based on Multi-Port Honeypots for Capturing IoT attacks
[17]. Ateeq Ahmad, Muhammad Ali, and Jamshed Mustafa: Benefits of Honeypots in Education Sector

[18].Artem Taran1, Dmitry S. Silnov Institute of cybernetic intellectual systems: Research of Attacks on MySQL Servers Using Honeypot Technology
[19].Li Li, Hua Sun, Zhenyu Zhang: The Research and Design of Honeypot System Applied in the LAN Security
[20].Anjali Sardana and R. C. Joshiu: Honeypot Based Routing to Mitigate DDoS Attacks on Servers at ISP Level
[21].Aleksey A. Egupov1, Sergey V. Zareshin2, Igor M. Yadikin3, Dmitry S. Silnov: Development and Implementation of a Honeypot-Trap
[22].Mr. Kartik Chawda, Mr. Ankit D. Patel Computer Science and Engineering Department: Dynamic & Hybrid Honeypot Model for Scalable Network Monitoring
[23].K.R. Sekar, V. Gayathri, Gollapudi Anisha, K.S. Ravichandran, R. Manikandan School of Computing, SASTRA University, India: Dynamic Honeypot Configuration for Intrusion Detection.
[24].Vinu V Das, Assistant Professor, Department of Computer Science and Engineering: Honeypot Scheme for Distributed Denial-of-Service Attack
[25].Emerson Virti, Universidade Federal do Rio Grande do Sul: Honeypots as a security mechanism

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Farming as a Service (FaaS) Through IoT Based Indo Green Agri Drone

Mr. Shubham Kaundinya[1], Miss Vaishnavi Pande[1], Dr. Ankush Kudale[2]
[1]Student, MCA-III, Sinhgad Institute of Management, Pune, Maharashtra, India
[2]Assistant Professor, MCA, Sinhgad Institute of Management, Pune, Maharashtra, India

ABSTRACT
This paper describes the problems may be caused by poor management and organization within the scheme and poor technology usage in the agriculture. Latest technology developments have turned present-day unmanned systems into realistic alternatives to traditional water supply survey methods. Technological Solution: Flying robot suitable for monitoring water leakages to canal system of irrigation. We describe the technical requirements for each of these monitoring types and discuss the operational aspects. The selection of a specific sensor/platform combination depends critically on the target species and its behavior. The technical specifications of unmanned platforms and sensors also need to be selected based on the surrounding conditions of a particular project, such as the area of interest, the survey requirements and operational constraints.
Keywords: Sensors, Remote control, Motor, Electronic speed control, battery, Radio transmitter and receiver.

I. INTRODUCTION

This document is completing as from my winter 2021 distributed research experience as a postgraduate student. We will promote the product as per the identified customers and will make sure that sufficient research has been done in identifying the needs of the customers. Since, this product will be a unique product in the market, we will make sure that customers are satisfied by the facts we present before them, and so we will do the best for identifying and presenting the best part of the product. It can applicable to drip irrigation agriculture farming also.

II. BACKGROUND AND LITERATURE REVIEW

Complexities in water distribution for the use of Agriculture through irrigation canal. effecting in water wastage and farmers crises against water distribution authority. The objectives of this project is as under -

- Identify leakages to canal of water supply.
- Measure the quantity of water supplied to agriculture farm and actual water received in farm.
- Billing of water supply at actual water received in farm.
- Quantify water consumption pattern by farm and by crop.

III. METHOD AND MATERIALS

A. About material:

1) Actuators and motors
2) Sensors
3) Software –Python
4) Remote control
5) Frame.
6) Motor
7) Electronic Speed Control (ESC)
8) Flight Control Board.
9) Radio transmitter and receiver.
10) Propeller (2 clockwise and 2 counter-clockwise)
11) Battery & Charge

Fig. 1 Agri Drones

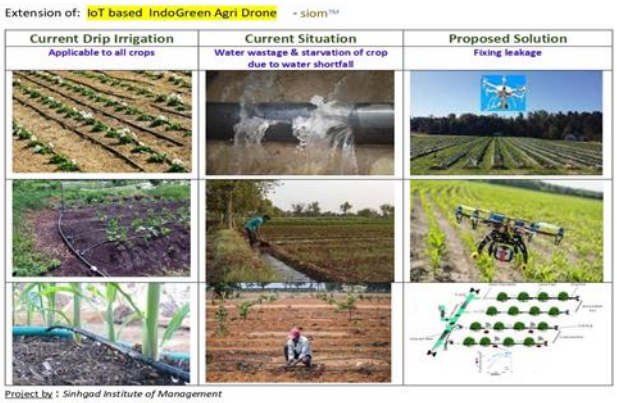


Fig. 2 Extension of Agri Drones

B) About method (Agriculture Drone system using GPS): In this device there are eleven content. We intend to protect your idea we will apply for provisional patent with prior art and claims to patent and trademarks office Govt. of India.

There is no any competitors for this in market. Technical specifications of this drone is as under a drone is bit more complex than the accepted definition of a thing in the IoT. The flying Drones can be considered as IoT. Drones are currently used in two standard agricultural applications tracking and distribution.Tracking (and subsequent analysis) is used in both plant and livestock agriculture and helps farmers understand the status, resources, and productivity of their farms. Distribution using drones involves physically moving resources across a farm, including spreading agricultural chemicals such as leakage of cannal water. The Agriculture Wonder Drone System is designed by making use of GPS where the automatically controlled drone based on aerial leakage of water cannel. Where the drone was behaved at required altitude, and then it is switch to altitude hold mode, which maintains the same altitude until it is switched back.

IV. MARKET AND SALES ANALYSIS

We have already developed device which has been published in IPR gazette of Govt. of India and team of researchers and students whom have experience of research projects and execution, implementation experience.

Our team capacities:

Sales: For sales we will contact irrigation department of government also for farmer's community.

Marketing: we will go for digital marketing as well as agricultural exhibition, news and media.

Operations: For development and implementation we have microcontroller development expert in industry and required peripherals we will import and assemble and also for software development we have MCA students and Alumni who will work on this project.

Technical Knowledge: In case of technical knowledge we will ask to incubation support and also industry experts for more technical details.

Finance: we are in process of searching the funding agency or interested business or startup who can help is for raising funds for developing this device.

V. GENERATE PYTHON-PACKAGE AND PYTHON-CODE

Setting Up the Path for Windows:

Assuming you have installed python in c:\Program Files\python\python32-37

Right-click on 'My Computer' and select 'Properties'.

Click the 'Environment variables' button under the 'Advanced' tab.

Now, alter the 'Path' variable so that it also contains the path to the python executable.

Example, if the path is currently set to 'C:\WINDOWS\SYSTEM32', then change your path to read 'C:\WINDOWS\SYSTEM32; c:\Program Files\python\python32-37

If you use bash as your shell, then you would add the following line to the end of your '.bashrc: export PATH=/path/to/python:$PATH'

Program:

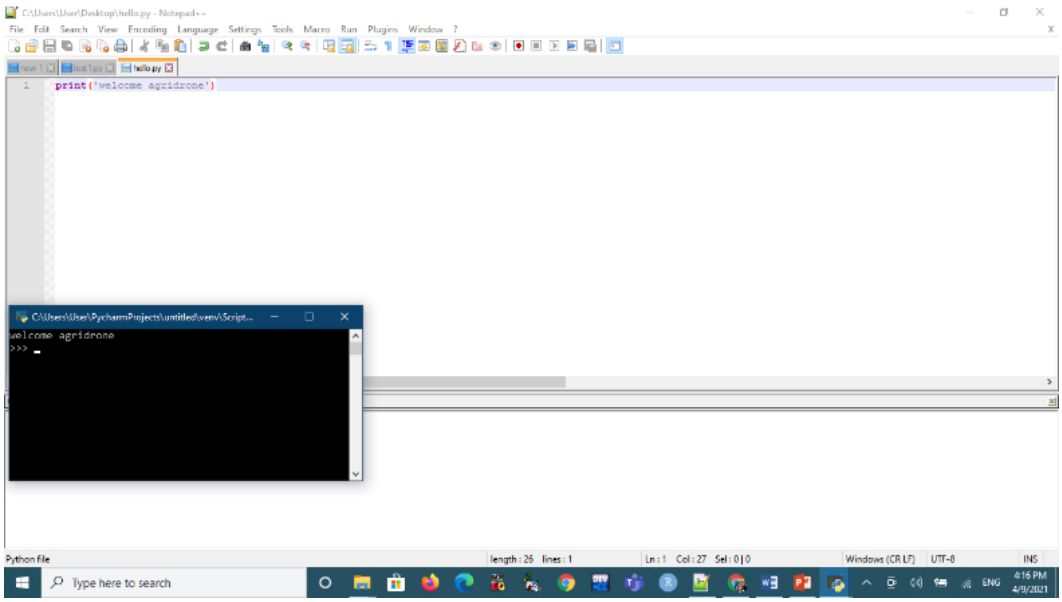


Fig. 3 Output: welcome Agridrone

VI. RESULT

The idea of execution is simple. A risk involved is mainly with the trust of customers. Flying Drone will designed and operationalized. Break-even point –No Loss no Profit –complete for social cause for initial 2 years.

After 2 years based on utility it has been estimated on 10% on manufacturing cost

For 1 flying Drone cost approx. 557000/- and initial we will develop one drone as a pilot project. Rs.500000/- (Rs. Five Lakh only) required from Funding agency/Incubation center as a support seed money. Balance fund will raise aprox.Rs.57000/- we will ask to other service providers and industry/business partners/vendors who are interested to contribute social as well funding agencies.

Below support required from incubator center apart from funds, Mentoring, Technical support for development, Government permissions, Peripherals space, IP protection.

Sr.	Particulars	Ist Year(Rs.)	2nd Year(Rs.)	Total(Rs.)
1	Drone peripherals	100000	100000	200000
2	Survey	5000	5000	10000
3	Assembly	25000	25000	50000
4	Legal permission	0	5000	5000
5	Software	25000	0	25000
6	Salaries:	70000	70000	140000
7	Supporting Technical Staff	60000	1000	61000
8	Expert	25000	25000	50000
9	Books	2000	2000	4000
10	Travel	5000	5000	10000
11	Other staff, if any	1000	1000	2000
	Total->	**318000**	**239000**	**557000**

Table 1 Estimation

VII. CONCLUSIONS

Our device is very important to our country and Government also because it has various techniques to handle their work. It has complex structure and Lightweight size. The device has been successfully Carry required work of area of fix customer problems. With the help of IoT they can access all information. In this manuscript different types of system useful for Agriculture wonder drone system using electronic speed-controller and Agriculture drone system using GPS were discussed. Mainly the paper focused on selection of best compatible design for Drone system for Agriculture purpose. Some of the exiting implementation was discussed with their advantages and disadvantages. In line to this the experimentation and expected result also discussed for further implementation.

VIII. ACKNOWLEDGMENT

I would like thank Dr. Ankush Kudale sir who guided us for completion of this idea for how to build and how to use of this device in future. I would also like thanks for my all faculty member and respective departments throughout the completion of this idea and how to develop more and more information will update for sensors and robotic device.

IX. REFERENCES

[1]. Prof. K. B. Korlahalli, Mazhar Ahmed Hangal, Nitin Jituri, Prakash Francis Rego, Sachin M. Raykar, "An Automatically Controlled Drone Based Aerial Pesticide Sprayer", Project Reference No.39S_BE_0564. [1][2]

[2]. S. R. Kurkute, C. Medhe, A. Revgade, A. Kshirsagar, "Automatic Ration Distribution System A Review". Intl. Conf on Computing for Sustainable Global Development, 2016. [2][3]

[3]. Vardhan, P. H., Dheepak, S., Aditya, P. T., & Arul, S. (2014) "Development of Automated Aerial Pesticide Sprayer." International Journal of Engineering Science and Research Technology, vol 3, issue 4.[1][2]

[4]. Aditya S. Natu., Kulkarni, S., C. (2016) "Adoption and Utilization of Drones for Advanced Precision Farming: A Review." published in International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169, Volume: 4 Issue: 5 PP.563 – 565[1[2]

[5]. https://www.geeksforgeeks.org/python-programming-language/[2[4]

[6]. https://en.wikipedia.org/wiki/Agricultural_drone [1]

[7]. https://www.engpaper.com/agriculture-drone.html[1]

[8]. Swapnil R. Kurkute, Dipak Patil, Priyanka V. Ahire, Pratikha D. Nandanvar, "NFC Based Vehicular Involuntary Communication System", International Journal of Advanced Research in Computer Science, ISSN No. 0976-5697 Volume 8, No. 5, May-June 2017.[1][2]

[9]. Abdullah Tanveer, Abhishek Choudhary, Divya Pal, Rajani Gupta, Farooq Husain, "Automated Farming using Microcontroller and Sensors". International Journal of Scientific Research and Management Studies (IJSRMS), ISSN: 2349371, Volume 2, Issue 1, Page No.-21-30[1][2]

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Literature Review on IOT Based COVID Detection System

Shashank Arya, Aishwarrya Shrivastava, Ragini Pandey, Prerna Shukla, Dr. C H Patil
School of Computer Science, MIT World Peace University, Pune, Maharashtra, India

ABSTRACT

The world is facing an ongoing pandemic caused by the novel coronavirus since 2019. This outbreak has placed the whole world's authorities in a difficult position. It posed various challenges in front of the world, the most important being "cutting the transmission" of the virus among others. Technologies have given a strong edge in confronting this pandemic. One such technology is IOT among others like Artificial Intelligence, Big data analytics etc. The Term IoT stands for Internet of Things. IOT is used for the purpose of connecting and exchanging data with different systems and devices on the internet that are embedded with sensors and different technologies. IoT is a vast network of appliances which have internet connection, these types of products are capable of gathering data and storing them in cloud or local storage. Gathered and stored data can be analyzed through various techniques that can be used for various things. Some examples of IoT devices are as follows: smart watch or band, smart helmet, etc. The exponential increase of the pandemic has wreaked disaster and increased the need for sudden reactions to ease down the effects. To settle the problems, researchers from all around the world with a variety of expertise have started understanding the problem. Artificial Intelligence is a very supportive technology around us, it has provided us effective ways to tackle the disease in appropriate ways. As we talk about the Covid-19, IoT-enabled devices or applications are doing a tremendous job, it is used to minimize the spread of the virus. In this pandemic situation where everyone is battling with coronavirus all around the globe, and searching for a way to win this battle these IoT devices can help us in many ways by gathering the data of the person's vital information like SpO2 and other information which will help the humanity in a better way. This paper surveys the role of IoT-based technologies in COVID-19 and reviews the platforms, applications, and industrial IoT-based solutions combating COVID-19 [1].

Keywords - IoT, Covid, COVID-19, Corona, Healthcare, Pandemic, Internet of Things.

I. INTRODUCTION

Internet of Things was first used by Kevin Ashton while he was giving a presentation about executing radio-frequency identification. It is a hi-tech technology that can be used to link with different things on the internet without any form of human interactions. In a simpler way, any application or system that is connected to the internet for observing and keeping a record of data can be called an IoT device. [2]

Recently, IoT has gained a persuasive research ground which is being used drastically for research purposes in different sectors such as academic and industrial directions but more importantly in healthcare. The IoT uprising has a big hand in mutating modern healthcare systems with the incorporation of technological, economic, and social surveys. It is expanding healthcare systems from traditional to more individualized healthcare systems through which patients can be diagnosed, treated, and recorded more easily. IoT is drastically becoming an important technology in healthcare systems where it can easily deliver better quality of services at a lower cost with leading user experiences. Because of its wide accomplishments including tracking identification and authentication with the collection of data, the sudden growth of IoT in healthcare is expected to rise from USD 72 billion in 2020 to USD 188 billion in 2025 [1].

Covid-19 is a contagious virus which belongs to the coronaviridae family of single-stranded, it affects the lungs, causing symptoms such as cough, fever, exhaustion, and shortness of breath. Origin of the virus is still not available, researchers did map the SARS-CoV-2 genomic information and discovered that it belongs to the coronavirus family's β-CoV genus, which is basically found in bats. In order to use the IoT device for gathering information on Covid we must have an IoT device which is designed in a way that can collect all the vital information of the person who is affected with the virus. The device will monitor the person and record all his/her activities in a log file which will be studied by the doctors and the scientists for the better knowledge of how this virus affects the person's body and immune system.

Healthcare in distant rural locations is harder to locate and provide, which is why new technologies such as Internet of Things (IoT)-based remote health supervision are proving useful.

The purpose of this research is to define the impact of IoT-based technologies in COVID-19 monitoring and controlling, as well as to examine the frameworks, applications, and operational IoT-based services that are being used to battle COVID-19.

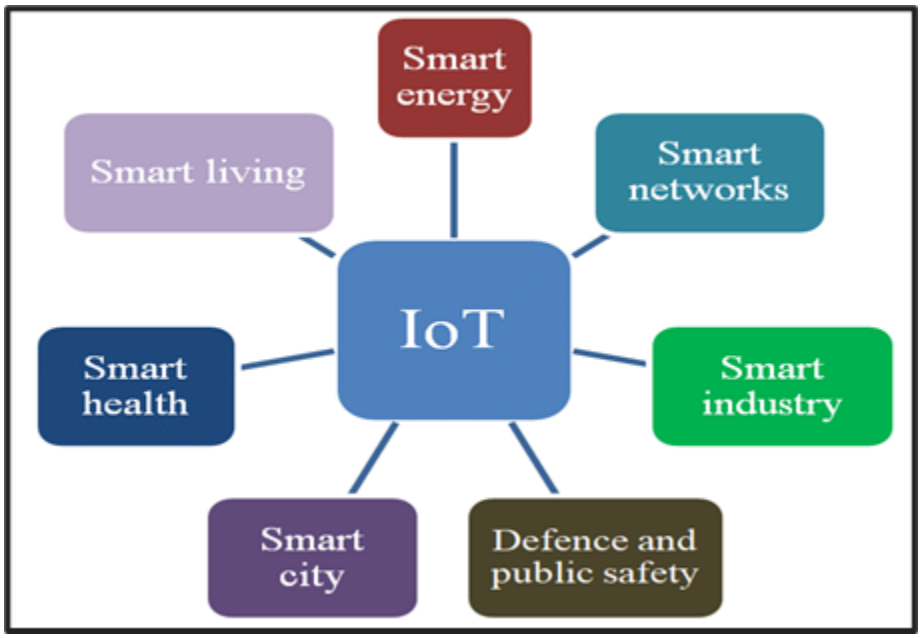
Early and accurate diagnosis can result in reduced infections and, in result of which, better health care for those who are affected. By segregating sick people from that around, quarantining proven or reported cases and implementing lockdowns can significantly reduce the number of COVID-19 occurrences. Following up on COVID-19 patients after they have been cured will aid in the observation of recurrence of symptoms and the infectivity of these recovered individuals. [2]

II. IMPORTANT ROLE OF IOT IN COVID-19

The globe has been battling the outbreak brought on by the novel severe respiratory syndrome coronavirus 2 by attempting to contain the virus's unexpected spread and create a vaccine. There was a strong demand for global surveillance of individuals with symptomatic and asymptomatic COVID-19 infection, as most efforts to identify a treatment or restrict the spread of the COVID-19 have yielded unsatisfactory results so far. In the past, IoT technology has gotten a lot of attention in the healthcare industry, where it plays a crucial role in various stages of infectious diseases. And, given the current pandemic's high COVID-19 unpredictability, it's critical for patients to be linked with and supervised by their doctors at all stages of the disease. [4]

III. LITERATURE REVIEW

Here, we portray small pertinence that will be encouraged by urban IoT measures that are of sensible concern within the city setting. Since that can envision a win-win circumstance of prospering quality and booming the applications bidded to civilians, bringing a proficient change for city organization to diminish in agent cost. A few regions that have been considered in this paper where IOT can be profited exceptionally regularly are Smart hospitals, Smart environment and Smart education service. [3]



IV. CLASSIFICATION OF IoT DEVICE

Basically, an IoT consists of three main things that are constrained devices, gateways or routers and the cloud platform. We can divide IoT into two types of high-level architecture that are constrained devices and gateway-like devices.

A) GATEWAY- LIKE DEVICE

These devices use powerful processors and extendable memories and also there are no constraints on power sources. They basically store all the data on the cloud servers and hence there is very less possibility of network latencies. They usually run-on Linux operating System. [4]

B) CONSTRAINED DEVICES

These devices are end nodes with sensors/actuators that can handle a specific application purpose. They are typically connected to gateway-like devices. They have a low power lossy network and in turn communicate with the IoT cloud platforms. They basically communicate through low power wireless protocols like 802.15.4, BLE, LPWAN and are mostly battery to powered with low data rate. There are some constraints for these devices as follows: Code Complexity (ROM/Flash), Available power source and that has limits on reachability over time, if battery powered. [5]

V. WEARABLE SMART IOT DEVICES FOR QUICK DIAGNOSIS IN COVID-19 PANDEMIC

Wearable technologies can be defined as the combination of electronics with anything that is able to be worn. Some examples of wearable IoT are as follows: Smart Bands or Watches, Smart Helmets, Smart Glasses etc. Utilising wearable gadgets is considered an effective way to respond to the need for early diagnosis amid this widespread disease. Creating these gadgets has had a momentous effect on the early discovery of infections [1]. For example, a wearable IoT gadget can affirm whether respiratory signs of a persistent are typical or not. With this information, the patient can notice any changes in his or her health circumstance and after that choose to create a medical appointment before any other symptoms show up. In reality, the COVID-19 widespread could be less demanding to battle utilizing suitable wearable devices. [4]

A) Smart Helmet

Wearable smart helmets with a thermal camera proved to be safer than an infrared thermometer gun during the COVID-19 epidemic due to less human contacts. When a high temperature is detected by the thermal camera on the smart helmet, an optical camera records the location and image of the individual's face. Then, with an alarm, they are sent to the allotted mobile device, allowing hospital personnel to identify the infected person and officials to take action. Furthermore, after detection, Google Location History can be used in conjunction with the smart helmet to locate the sites travelled by the culprit. This wearable device has been adopted in countries such as China, the United Arab Emirates, and Italy to monitor crowds within 2 metre of passers-by. Remarkably, this approach has produced positive outcomes. For example, the KC N901 is a smart helmet made in China that detects excessive body temperatures with a 96 percent efficiency. [3]

B) Smart Bands/Watches

Wearable devices like fitness trackers and smartwatches can give us new perspectives on our health and well-being. Wearable technology ensures consistent immediate access to physiological parameters, unlike typical testing in what seems like a clinical setting, which can be done repeatedly yearly (or less frequently). You can see how far an individual deviates from the "average" baseline in this way. This is a completely different approach to healthcare than existing procedures, which primarily match physiological data to vital records. The prospect for wearable healthcare technologies is becoming increasingly obvious during the 2019 coronavirus illness pandemic. [7]

Pre-symptomatic cases of covid-19 can be detected using smartwatches data, heart rate, number of steps walked in a day and sleep duration. [5]

C) Smart Thermometers

To acquire consistent measures of body temperatures, a broad range of IoT smart thermometers has been developed. These low-expense, accurate, and simple-to-use devices can be worn underneath garments or stick to the skin. They are commonly available in a variety of formats, including touch, patch, and radiometric. The usage of these gadgets can be quite beneficial in detecting questionable instances early on. [5]Furthermore, because the use of infrared thermometers for collecting temperature of the body may increase the spread of illness due to the close proximity of people and healthcare personnel, smart thermometers are strongly recommended. Kinsa's thermometers have been widely utilised in homes, and the manufacturer can now anticipate the most suspect regions in each state of the United States based on people's reported temperatures. Tempdrop, Ran's Night, iFever, and iSense are examples of smart thermometers that can send temperature of the body to a smartphone at any time. The use of these gadgets in people's daily life can increase the likelihood of early diagnosis of new patients. [7]

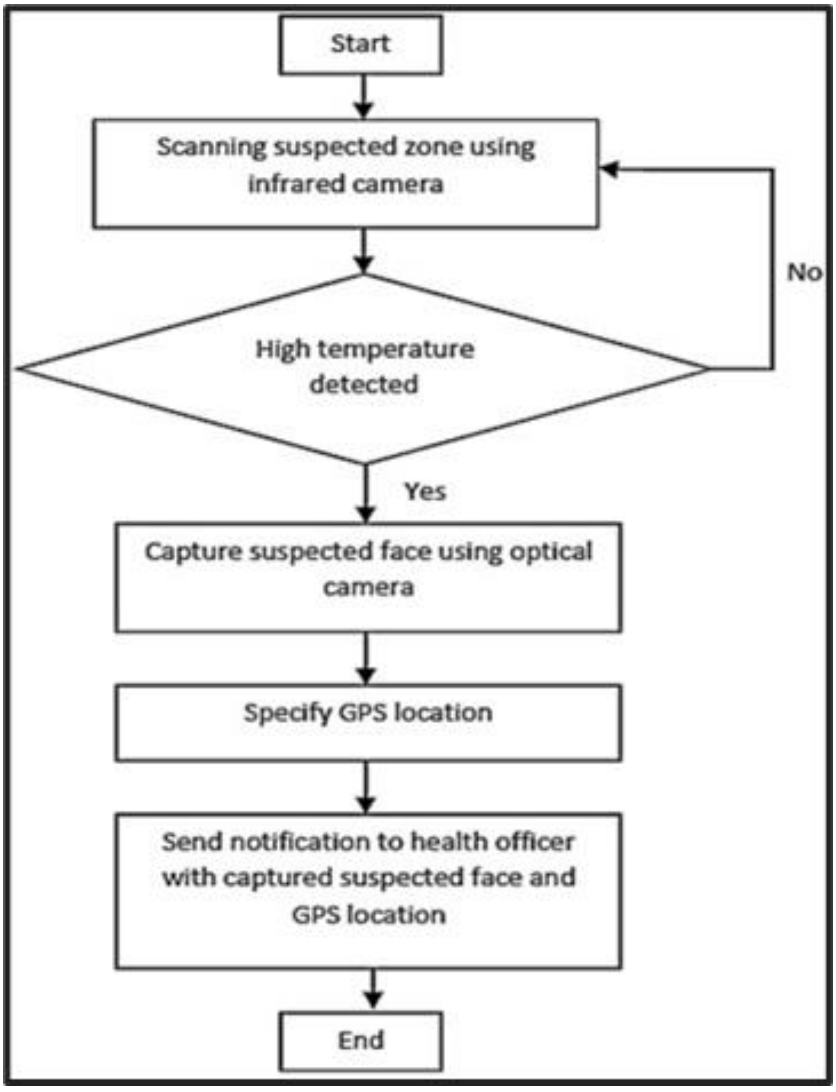


Fig: Work flow of IOT smart thermometer

D) SMART GLASSES

The COVID-19 outbreak is reshaping the healthcare sector, with telecommunication, or digital health, as one of the main drivers. Smart glasses have just lately been made available to the general public, but they have already piqued the curiosity of health care providers, as seen by their initial implementation in hospitals across the country. Smart glasses, compared to thermometer guns, have fewer human interactions. Smart glasses with optical and infrared cameras have been utilized to watch masses, and the integrated face recognition technology makes the monitoring method easier after worrisome cases are detected. In reality, this enables for the detection of the questionable case's identity or a person with a high temperature. Furthermore, by recording the locations travelled by the questionable case, Google Location History can enable more reliable actions in the future. [5]Rokid, a pair of smart glasses with sensors, can keep track of approximately 200 individuals. The combination of Vuzix smart glasses with the Onsight Cube thermal camera is another type of this device. These sensors collaborate to keep an eye on masses and detect persons, according to the Journal of Healthcare Informatics Research. With high temps, the smart helmet uses a thermal and optical camera to record temperature changes and transmit the data to medical facilities or officials. [3]

VI. NON-WEARABLE EXISTING DEVICES FOR DETECTION AND TREATMENT.

These are devices that exist in physical form and are instilled with sensors and actuators and are responsible for doing required functions via communicating with other devices over the internet.

A) Drones

In specific terms, Drones also known as Unmanned Aerial Vehicles (UAVs) are aircraft without any human pilot on board working in coordination with ground-based controllers and communication systems fitted with cameras, GPS etc. These drones are mainly associated with defense, image capturing, distribution etc. But these have played an important role in curbing the pandemic and providing aid to the crowds and villages in isolation, hence cutting the transmission and also lowering the amount of human power required for such jobs. These have helped in reaching hard-to-access, far flung places. [5]

This technology has helped in maintaining isolation from contaminated people and reducing human interactions. Drones with thermal imaging act as a magic combination in detection of people with high temperature/fever from the crowds and in data collection. It works on the concept of infrared radiation i.e. The amount of infrared radiation that a body emits is proportional to the amount of thermal energy it emits and maps it with washed out hotspots in the images. [4]

B) Panic Buttons

Panic buttons were designed for elderly people as a handy measure to access emergency medical help and alerting families which is a programmable device connected with the cloud through wireless communication. Other functions it includes is that one can ask for repetitive tasks just by pressing this button.

In 2018, Athma Foundation launched 'Aathma Panic Button,' a waterproof device for senior citizens that is meant to help them in emergencies. [2]

The moment a person presses the panic button, a pre-recorded voicemail about him/her is sent as three messages — to the 108 ambulance, a neighbour and an immediate relative.

In combating the current pandemic, Visionstate, a Canadian software firm produced Wanda QuickTouch was deployed as a cleaning alert system in hospitals. They are designed for alerting authorities in case of any concerns related to essential sanitation or public safety. [2]

C) No- contact Temperature Sensor

No contact Temperature sensor came into being with the necessity of the implementation of social distancing in order to detect the temperature with no physical contact and prevent the spread of the virus. [4]

These include devices with thermal imaging systems, no contact infrared thermometers which measure the body's temperature rapidly when placed 5-10 cm from the surface of the body and are non-invasive in procedure. [1]

There are several benefits of these thermometers when compared to traditional ones, these are:

- Non-contact approach may reduce the risk of spreading disease between people being evaluated
- Easy to use
- Easy to clean and disinfect
- Measures temperature and displays a reading rapidly
- Provides ability to retake a temperature quickly [3]

In the current scenario, as different establishments such as businesses, transportation systems, community organizations plan to resume their normal phased operations and public usage places and services like malls, restaurants are reopening, these no contact infrared thermometers along with sanitizers are mandatorily being operated manually at the entrance gates. [1]

D) Pulse Rate Sensor

The use of the sensor is to measure the amount of haemoglobin saturated with oxygen as it is an indicative measure of overall health of a person. The virus infection reduces the level of oxygen flow in the blood and decreases the percentage of respiratory distress. It can be termed that the healthy person has a 96–100% level and it decreases as the spread of infection increases. To further understand pulse oximetry, usually, a patient's body lung is filled with liquids and inflamed material. This restricts the lungs' ability to pass the Oxygen to the bloodstream. SpO2 Level range from 95% to 100% is considered a healthy scale, while 94% indicate a possible covid-19 infection where the patient must be admitted to ICU for very close monitoring. A SpO2 device is a need to regularly monitor the oxygen level of a possibly infected person and notify if there are any abnormal recordings. This factor defines the acuteness and progression of the disease to a severe stage. [5]

Pulse oximetry is basically a valuable non-invasive tool that provides data regarding the percentage of haemoglobin molecules loaded with oxygen in arterial blood in patients with normal oxygen-dissociation curves.

- The oximeter utilizes an electronic processor and a pair of small light-emitting diodes (LEDs) facing a photodiode through a translucent part of the patient's body, usually a fingertip or an earlobe.
- One LED is red, with a wavelength of 660 nm, and the other is infrared with a wavelength of 940 nm.
- Absorption of light at these wavelengths differs significantly between blood loaded with oxygen and blood lacking oxygen.
- Oxygenated haemoglobin absorbs more infrared light and allows more red light to pass through.
- Deoxygenated haemoglobin allows more infrared light to pass through and absorbs more red light. [5]

E) Mobile based Applications

A large number of mobile applications have been developed to curb and beat the ongoing pandemic. Mobile apps have been implemented for training, information sharing, risk assessment, self-management of symptoms, contact tracing, home monitoring, and decision making, rapidly offering effective and usable tools for managing the COVID-19 pandemic. [2]

Mobile apps are considered to be a valuable tool for citizens, health professionals, and decision makers in facing critical challenges imposed by the pandemic, such as reducing the burden on hospitals, providing access to credible information, tracking the symptoms and mental health of individuals, and discovering new predictors. [4]

Such mobile applications gather huge data for contact tracing and implement isolation and quarantine methods for infected persons and cut the transmission.

For example- Aarogya Setu

Aarogya Setu is a mobile application developed by the Government of India to connect essential health services with the people of India in our combined fight against COVID-19. The App is aimed at augmenting the initiatives of the Government of India, particularly the Department of Health, in proactively reaching out to and informing the users of the app regarding risks, best practices and relevant advisories pertaining to the containment of COVID-19. [3]

F) Mask Coverage Detectors

Masks are one of the most essential commodities. Since this virus spreads mostly because of the droplets produced by sneezing and coughing, it became essential for all to wear it all the time to prevent the spread of the virus. But people often don't wear it properly hence defeating the very purpose of masks. Mask coverage detectors are devices that convey the overall coverage of the mask in percentage, for example, for a person having his mask below nostrils, it will show the result and not allow entry. [3]

The model is fed with huge datasets for improved accuracy. Biometrics sensors used for face capturing and face detection, which faces from the nose, lips, eyebrow size, and eyes. Other parameters are tested like face surfaces, features, skin colors etc. Test cases are assessed based on the datasets and algorithm and the output is created. [5]

VII. IOT IN CURRENT PANDEMIC OF CORONAVIRUS DISEASE COVID-19

CoVID-19 is a global pandemic that is spreading at an exponential rate. To identify the suspected or quarantined people, some advancement has occurred with the development of data analytics and machine learning. Digital healthcare systems have developed on the top of cloud computing, mobile computing, artificial intelligence and the internet of things. The existing challenge of COVID-19 has affected all countries worldwide. Due to the devastating spread of global pandemic COVID-19, Internet of things (IoT) enabled devices are in trend. Early detection of contagious people is one of the main goals of all countries. During the first phase of COVID-19, which is early diagnosis, there is an essential need for faster diagnosis due to the high rate of contagiousness of COVID19 where even an asymptomatic patient can easily spread the virus to others. The sooner the patient is diagnosed, the better the spread of the virus can be controlled, and the patient can receive appropriate treatment. In fact, IoT devices can speed up the detection process by capturing information from patients. This can be implemented by capturing body temperatures using different devices, taking samples from suspicious cases, and so on. [7]

As the CoVID-19 carrier may spread this virus with an exponential rate in population. Thus, the detection of suspected people with different gadgets are proposed to detect various symptoms of patients. For healthcare industries, IoT devices are capable of providing sensor data that can be potentially processed as well as analysed in real-time. [6]

AI can be valuable in the treatment of COVID-19 and also for appropriate health monitoring. AI can also assist in formulation of treatment regimens, strategy of prevention and for the development of various drugs and vaccines. For example, for temperature detection thermometers are used. Further for detection of respiratory

systems a WHOOP's wrist -worn wearable health tracking system is proposed by central Queensland University Australia. They have proposed a self-identified system that will gather the patient's data, but this system is mainly dealing with an analysis of change in the respiratory system of patients. [4]

VIII. CONCLUSION

While the world is struggling with the COVID-19 pandemic, many technologies have been implemented to fight against this disease. One of these technologies is the Internet of Things (IoT), which has been widely used in the healthcare industry. During the COVID-19 pandemic, this technology has shown very encouraging results dealing with this disease. [6] For this paper, we conducted a survey on the recent proposed IoT devices aiming to assist healthcare workers and authorities during the COVID-19 pandemic. We reviewed the IoT-related technologies and their implementations in three phases, including "Early Diagnosis," "Quarantine Time," and "After Recovery." For each phase, we evaluated the role of IoT-enabled/linked technologies including wearables, drones, robots, IoT buttons, and smartphone applications in combating COVID-19. IoT technology can be extremely efficient for this pandemic, but it is also critical to consider the privacy of data. By implementing IoT technology properly in a secure way, more patients, with peace of mind, can participate in their treatment using IoT devices. As a result, authorities and healthcare workers can better respond to pandemics.[2] Consequently, the impact of these types of diseases, including infections, hospitalizations, and death rate, can be significantly reduced. The implementation of IoT requires energetic and hard attempts to handle. It seemingly conveys even a minor alter in the user's superiority of life. With a broadly shared, localized sophisticated scheme of intelligent devices, IoT has enabled improvements to significant facilities in utilities, hospitals, education and other areas, which gives a modern scheme to technology advancement. [5]

APPLICATION	FUNCTIONS
Aarogya Setu [1]	Track covid cases via Bluetooth and trace potential users who may have come in close proximity with Covid positive patients and linking them with health services.
Social Media -WhatsApp [6]	It can provide well-being and support to Covid-19 diagnosed patients at their fingertips without going to hospitals. Users can consult their problem online with the physician.
Social Monitoring [3]	It is used for tracking Covid positive patients. This application can be used to give access to user's personal information by the government.

CoWin [2]	This app is developed by the Indian Government for the benefit of Humanity, users can register themselves on the application for the covid vaccination hassle free. Government can use this data to figure out how much of the population is fully - vaccinated or partially vaccinated and on the basis of the result take the necessary further actions.
DetectaChem [4]	It is a USA based application which is used for taking COVID-19 tests at a low-cost by using a kit that is connected to a smartphone application.

IX. REFERENCES

[1]. A. H. S. M. Z. A. A. R. A. Muhammad Usman Ashraf, "Detection and Tracking Contagion using IoT-Edge Technologies: Confronting COVID-19 Pandemic," Springer Nature Switzerland AG 2020, 2020.

[2]. M. U. Ashraf, "Confronting COVID-19 Pandemic".

[3]. N. A. B. A. Z. S. A. G. Shaik Asif Hussain, "IoT based wearable device to monitor the signs of quarantined remote patients of COVID-19," Sustainable Cities and Society, 2021.

[4]. V. H. V. G. M. G. Vinay Chamola, "A Comprehensive Review of the COVID-19 Pandemic and the role of IOT," Digital Object Identifier, 2020.

[5]. A. K. Y. F. G. C. D. H. Ceren Ates, "Wearable devices for the detection of COVID-19," Nature Electronics, 2021.

[6]. I. H. K. Mohd Javaid, "Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic," PMC, 2021.

[7]. W. H. Organization, "Modes of Transmission of Virus Causing COVID-19: Implications for IPC Precaution Recommendations," Available: https://www.who.int/news-room/commentaries/detail/modes-of-transmission%-of-virus-causing-covid-19-implications-for-ipc-precaution-recommendations, 2020[Online].

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

IoT Device: 'DRIVE SAFE' A Road Safety Device

Shruti Mali[1], Sakshi Gaikwad[1], Kalyani Andhale[1], Ganesh Jadhav[2]
[1]Student, School of Design, Dr. Vishwanath Karad World Peace University, Kothrud, Pune- 411038, Maharashtra, India
[2]Assistant Professor, School of Design, Dr. Vishwanath Karad World Peace University, Kothrud, Pune- 411038, Maharashtra, India

ABSTRACT
Road safety is a major issue concerning development, the public health sector, and it is also a leading cause of deaths and injuries. Globally 1.35 million deaths are reported annually in the Road Safety 2018 Report with India being an 11% contributor to that number [2]. Animal - Vehicle Collision (AVC) remains to be one of the important road safety issues concerning animal safety. Stray animals wandering around the roads are one of the under recognized factors for AVC [1]. Globally on average, 5.5 million animals are killed every day due to AVC and thus annually it causes 2 million animal deaths [9]. To lessen these fatalities, concrete measures need to be taken into account in terms of technology and Awareness. Introducing technological advancements to vehicle owners (Cars, Scooty, Bikes, and Auto Rickshaw) that can be user-friendly, can help to curb these fatalities.
This paper explores different areas connected to road fatalities and their adverse effects. In this paper, we suggest a solution that is backed up by Artificial intelligence (AI) and Internet of things (IoT) -driven technology. In this paper, we use an IoT Device that detects pedestrians and animals in the path and alerts the driver beforehand to avoid a sudden encounter with them and avoid eventual accidents. The study includes Market research, Quantitative Survey, Material analysis, form analysis, and also its user-friendly behaviour.
Key words: Road traffic, Animal safety, Pedestrian safety, stray animals, road accident fatality, IOT, AI.

I. INTRODUCTION

Road traffic accidents are considered amongst the worst issues as it has serious health problems globally, mostly in developing countries like India where the increase in population has led to an increase in vehicles and road networks. Around 54% of deaths recorded globally are pedestrians and motorcyclists. [2]

Fig 2.1 Human injured in a car accident

The number of Animal Vehicle Collisions (AVCs) globally exceeded 1 million in the 90s.[27] In India, animals wander freely on the roads, this increases the risk of animal-vehicle collisions in rural areas. The NMC (National medical council) recorded 3,442 stray animals injured in road accidents in the year 2020-2021, while the injuries recorded was 4,262 in 2019-20. The NMC says that there might be more animal injuries because most of the people do not bother to tell the municipality or other civil bodies when there is an accident in which animals are injured or dead at the site.

Fig 2.2 Animal injured in a car accident

There were fewer accidents in 2020-21 because of restricted vehicular movement during the Covid-induced lockdown as compared to 2019-20. [7]

The table below shows the data of animal Vehicle collisions between the years 2014-2018. [4]

	2014	2015	2016	2017	2018
No. of deaths	239	338	425	416	318

Wildlife animals are becoming extinct day by day and domestic animals and pedestrians are at risk of being injured or killed. The major factors that contribute to accidents are Speed of the Vehicles, traffic, environmental factors like weather, a physical environment like people walking on roads instead of a footpath or no footpath at all, poorly timed signals, Pedestrian behaviour like consumption of alcohol, not paying attention to the signals, drivers being distracted by calls or drink and drive.[28] Various research papers suggest that combining different technologies for obstacle detection gives a more accurate representation of the driving environment, when looking at technological solutions for obstacle detection in extreme weather conditions (rain, snow, fog), and in some specific situations in urban areas (shadows, reflections, potholes, insufficient illumination), although already quite advanced, the current developments appear to be not sophisticated enough to guarantee 100% precision and accuracy, hence further valiant effort is needed.[1] This paper aims at reviewing all the above factors and proposing a solution backed up by Artificial Intelligence and IoT-driven technology to reduce these fatalities and make it a safe space for pedestrians and the animals. This design solution will detect the pedestrian or animals in the path and alert the driver so that the driver can take the necessary precautions to avoid any accidents.

II. METHODS

2.1. Field study:

The study population consists of the vehicle-driving citizens of India. During the study, a quantitative online survey was conducted to understand citizens' points of view on the topic, its severity, and their reaction to the problem. The sample size for this study was 50 participants with a minimum age of 18 years (Legal Driving age) and a gender-neutral ratio.

The topics discussed in the survey were:

- Occurrence of events that includes accidents that involve physical harm to animals or pedestrians in the participant's life.
- Their ability to follow measures to avoid accidents on the road.
- Their opinions about such accidents.
- Their opinion about the causes of such accidents.
- Their awareness about this issue.

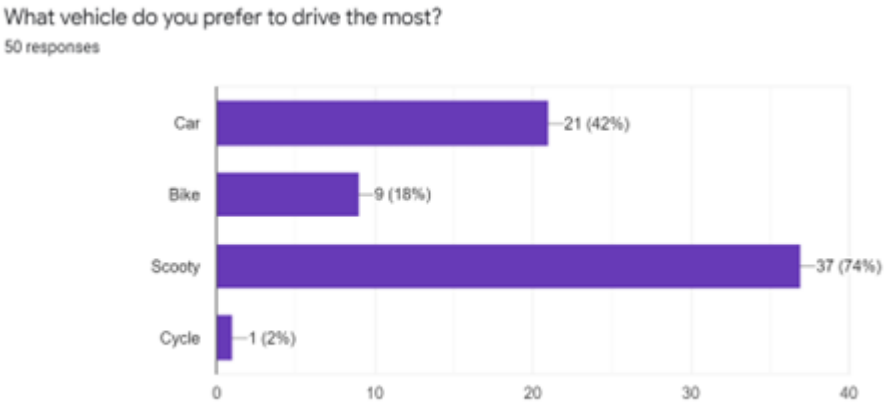
A total of 50 participants randomly agreed to participate in the study. They were uncompensated for their contributions to this study. Inclusive criteria for the study was the minimum Legal Driving Age in India (18 years) without medical issues. Participants' personal details (name, age, phone number, weight, height, education, etc.) were not collected to maintain anonymity in the study.

2.2. Results

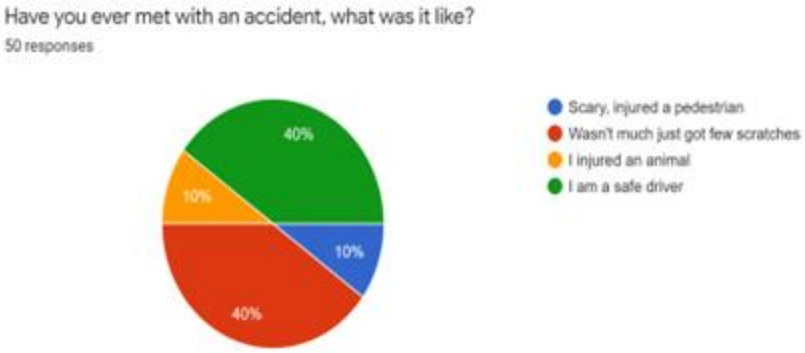
A total of 50 participants were selected at random to participate in this study. The collected data was analysed by using the Pie chart technique. The pie chart is a technique used to represent the statistical data collected in the study in a circular graph with percentage representations for understanding.

Formula used to calculate and represent the data is:

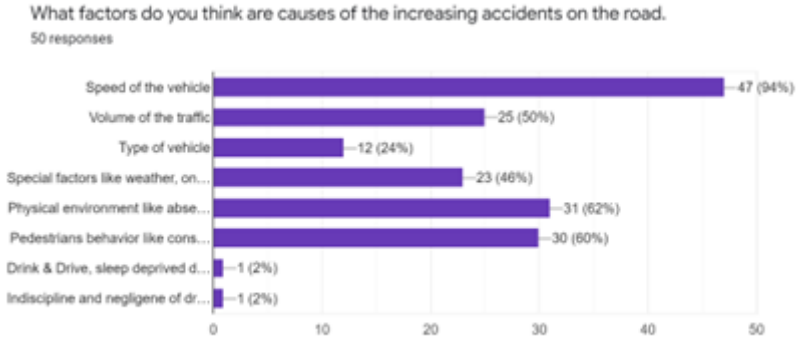
(Given Data / Total Data) multiplied by 360



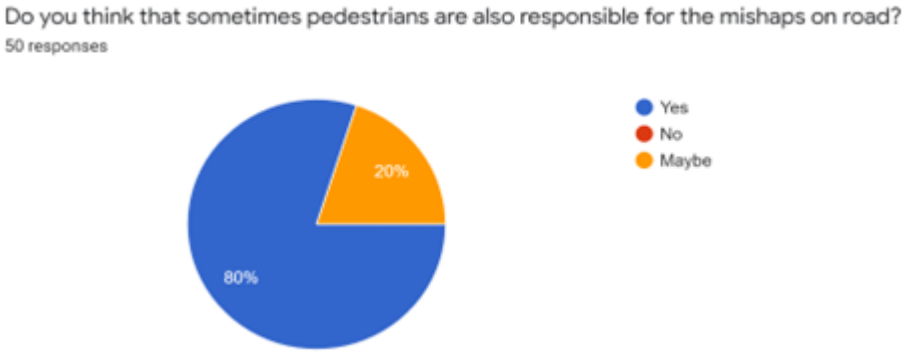
The study showed that almost 71% of the population preferred using two-wheeler commodities to travel and felt safe travelling at night.



Nearly 40% of participants have met with an accident and injured themselves while 10% have injured a fellow pedestrian or animal in the way.



Close to 92% of participants feel over speeding and unexpected movements on the road are vital factors causing these accidents.



80% of participants think pedestrians and animals are also responsible for causing such mishaps. Negligence, ignorance, and lack of attention are other factors that generate animal and pedestrian collisions with vehicles.

2.3. Existing Products in the market:

Some of the existing products or devices in the market are LIDAR, its full form is light detection and ranging, it is a method of depth perception which transmits a light source to either create multidimensional or ranging depth maps of the scene in front of the vehicle. [28] It does not work well in bad weather conditions like snow, fog or heavy rains as it uses lasers to measure the distance. It also requires more power and this decreases the car's driving range. These sensors do not look aesthetically pleasing when they are placed on top of the car.[29]

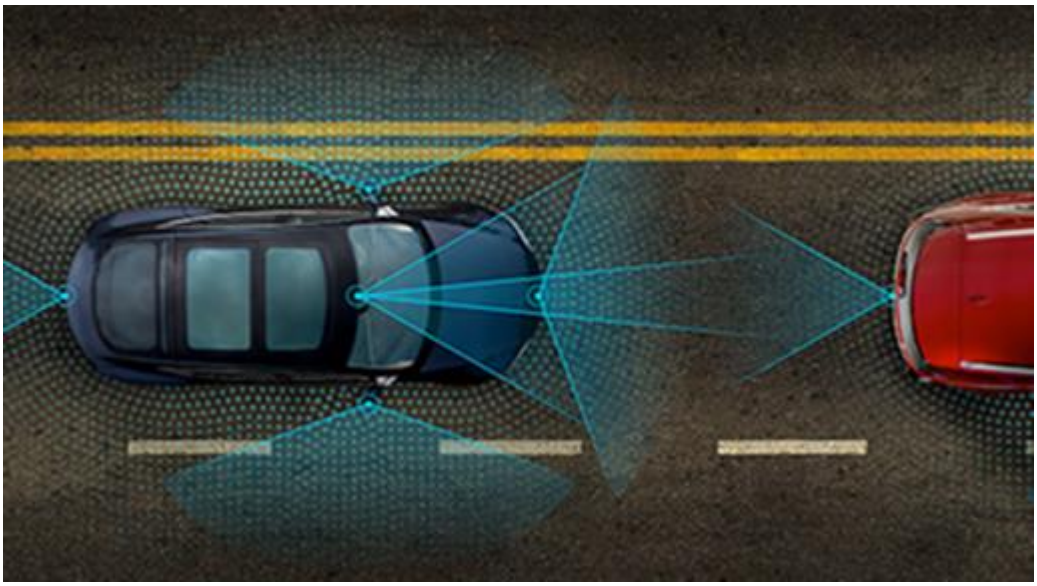


Fig 3.3.1 LIDAR System

There is an augmented reality driving app which is called as imagGinyze which aims to make it our safety companion. This app detects the obstacles in the path and notify the driver by displaying it on the screen. This design is in its prototype stage and yet to be in the market.[30]

Fig 3.3.2 Augmented reality Driving App

The ADAS, which stands for advanced driver assistance system is a technological advance feature which is designed to increase the safety while driving a vehicle. Logistfleet states that when these devices are designed properly this type of systems uses machines and humans to interact. This improves the ability of the driver to drive on the road and take necessary actions while driving. After installing and implementing these types of devices there is still an issue with some of the drivers who are at the learning stage. They do not use these devices to the fullest which will eventually reduce the risk of accidents [31]

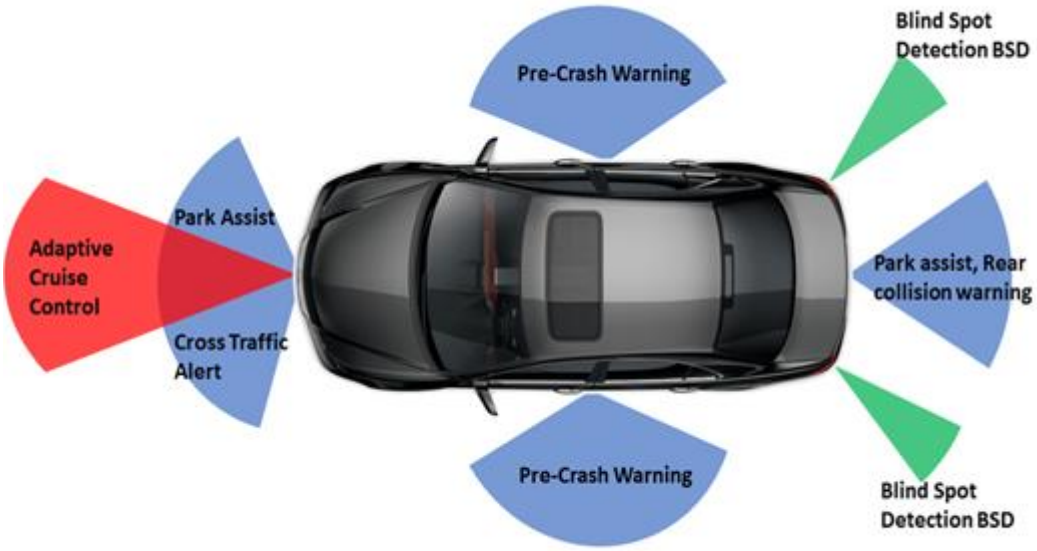


Fig 3.3.3 ADAS Device

Such devices should work well in all the conditions, especially in fog or heavy rains where road is not clearly visible but the LIDAR system does not work well in such conditions, the Augmented reality apps helps for

detecting the obstacles in the path but they are not yet tested so they are not available in the market. The ADAS device charges from vehicles main battery and at times it is distraction, triggering hazardous behaviour and confusing to use as it includes various features So all these devices have their drawbacks and hence there was a need to come up with a technological device that consider all the drawbacks and overcome them to make a drive safe device.

2.4. Proposed Design

The device proposed in this paper is an IOT Device that warns drivers of humans and impending animal crossing and is adaptable to most two wheeler and four wheeler vehicles. The 'Drive Safe' product has:

- 360 Degree detection radar
- can be connected to smartphones / smartwatches/ tablets through an App via Bluetooth is attachable to any vehicle irrespective of its size or shape
- Has an identifiable sound buzzer to alert the driver well in advance
- can detect animals as well as pedestrians
- works well in low light/dark conditions
- waterproof
- notify the path with no/less obstacle

It consists of basic components- ultrasonic sensor, Bluetooth module, Arduino pro mini, servo motor, DC motor and motor driver IC.

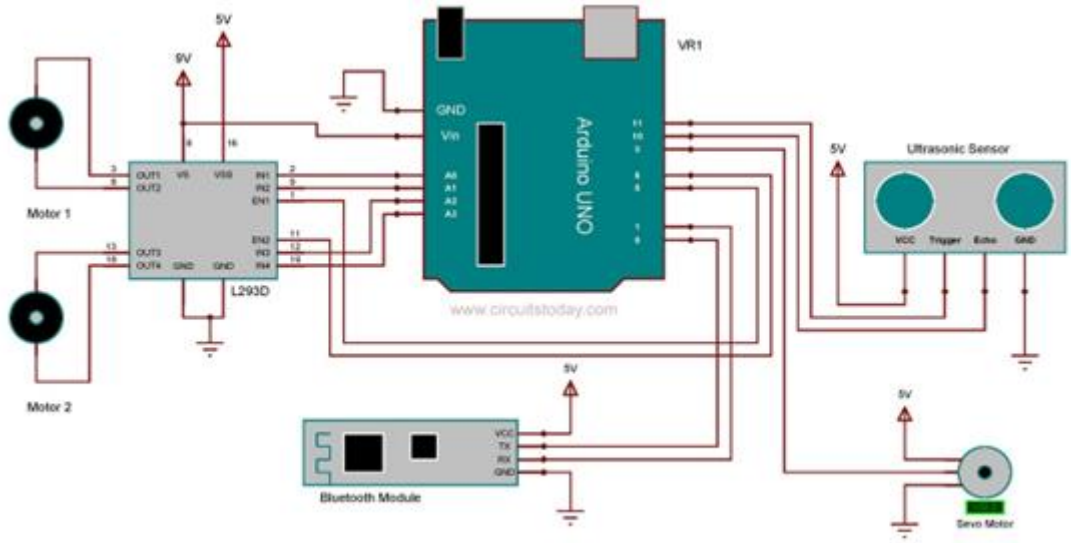


Fig. 3.4.1 Circuit Diagram of Drive Safe

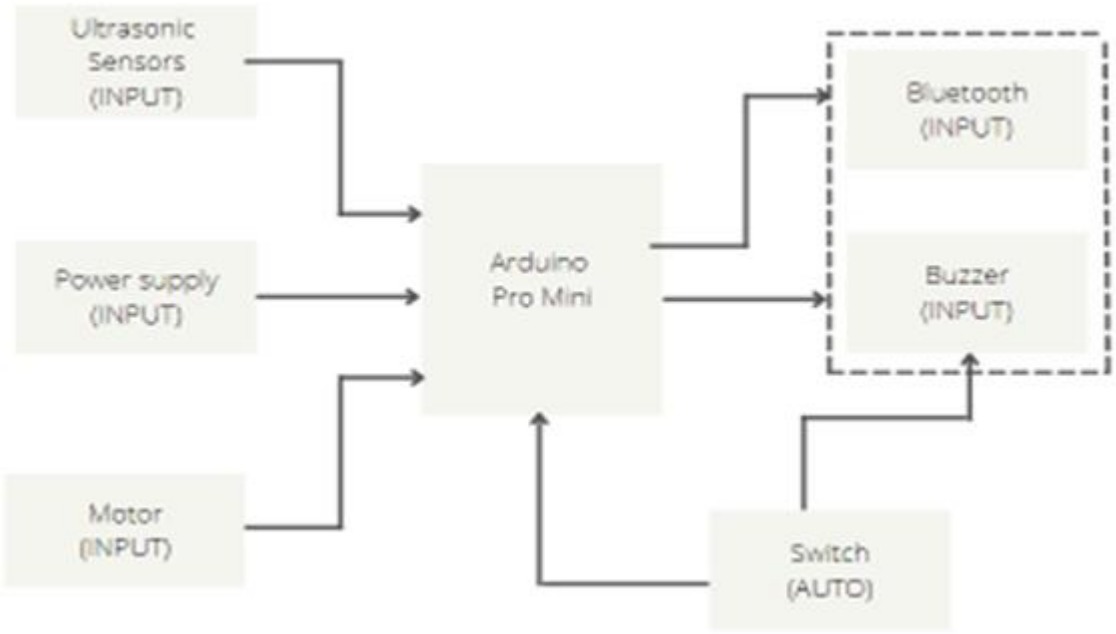


Fig. 3.4.2 Block Diagram of Drive Safe

Ultrasonic sensors are used to measure the distance between the objects. It uses ultrasonic waves. To measure the distance. It uses a transducer, which converts energy from one form to another to send and receive ultrasonic pulses that pass back information about an object that is in nearby proximity. These ultrasonic sensors act as an input for the safe drive device along with the power supply and the motor which helps the device to perform the necessary action to detect the objects. This information is passed on to Arduino pro mini which is a controller board that allows you to connect different sensors as an input to convert it to an output. The Bluetooth which works on a radio signal is the output for this device. When the data is processed with the help of sensors through Arduino pro mini it sends the signal to the user via Bluetooth which helps the driver understand that there is an obstacle in the path. The buzzer which is an audio signalling device adds extra help to the user via sound signals so that the users will be alerted.

The product dimensions are as follows:

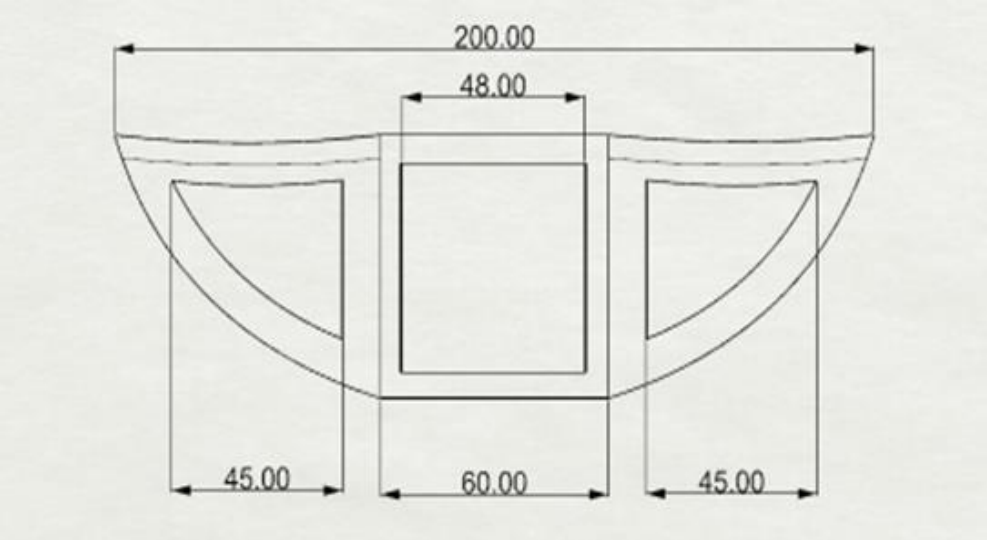


Fig. 3.4.3 Front view and top view of Drive Safe device

Fig. 3.4.5 Adhesives used for the interaction between the device and vehicle

This device will be attached on the car's bonnet or for the two wheelers it is attached on the front side. Snaps which are interlocking dicks are used to attach this device on the vehicle. Velcro can also be used to stick this on any vehicle.

2.5. Customer Feedback

Fig. 3.5.1 Reference for the customers

A Quantitative survey was conducted with the figure 3.5.1 as reference to introduce our concept idea with the customer base. A sample base of 20 was selected for this feedback round. They were the subset of our initial sample group that were studied for the initial research. The sample base was asked to give their opinion on the 'Drive Safe: An IoT Device' by giving them a product description flyer (figure 3.5.1) for reference. The opinions were asked on topics like functionality of the product, characteristics of the product, aesthetics of the products, additional features they would like to add in the concept of the device and also if they are willing to invest in it. In this feedback we understood that people are supportive of this concept and are willing to invest in a device like this. People are supportive and excited about the fact that it will be fully customizable to suit their vehicle's aesthetics. They are happy about its shape, size and aesthetics in general. They feel a device like this can help curb the accidents and also make them aware about the upcoming movements and situations on the road. The features the customers want to add were an inbuilt version of the device in the vehicle and an alternative to the buzzer sound that is a little calm and would not disturb the driver when driving. The existing version is completely accepted by the people and they are ready to experience the working model of this Drive safe device.

III. FINAL PROPOSED DESIGN

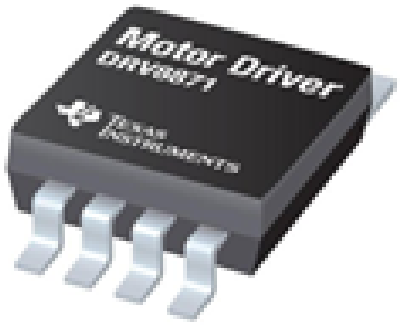
The device proposed in this paper is an IOT Device that warns drivers of humans and impending animal crossing and is adaptable to most two wheeler and four wheeler vehicles. The 'Drive Safe' product has:

- 360 Degree detection radar
- can be connected to smartphones / smartwatches/ tablets through an App via Bluetooth is attachable to any vehicle irrespective of its size or shape
- Has an identifiable sound buzzer to alert the driver well in advance
- can detect animals as well as pedestrians
- works well in low light/dark conditions
- waterproof
- notify the path with no/less obstacle

The internal components of the device consists of:

- Ultrasonic sensor- instrument that measures the distance to an object using ultrasonic sound waves.
- Bluetooth module- a hardware component that provides a wireless product to work with the computer or in some cases the Bluetooth may be an accessory or peripheral, or a wireless headphone or other product.
- Arduino pro mini- The Arduino pro mini is a microcontroller board based on the ATmega328.
- Servo motor- a rotary actuator or linear actuator that allows for precise control of angular or linear position, velocity and acceleration.
- DC motor- class of rotary electrical motors that converts direct current electrical energy into mechanical energy.
- Motor driver IC- an integrated circuit chip which is usually used to control; motors in autonomous robots.

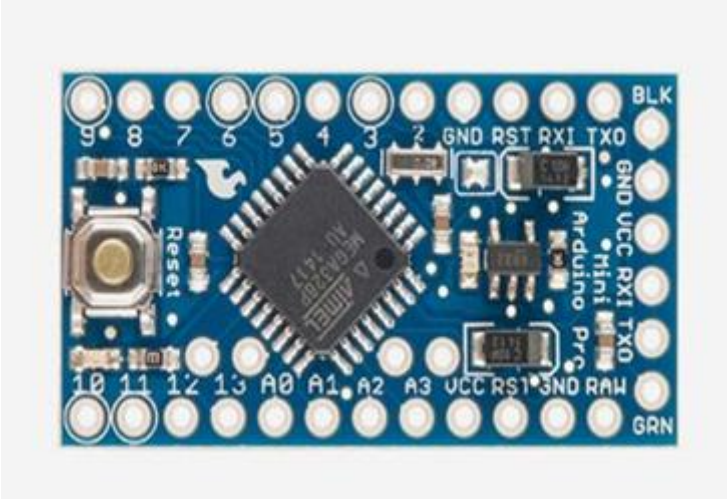
Interior components of the device-



Motor Driver IC

Bluetooth module

Ultrasonic sensor



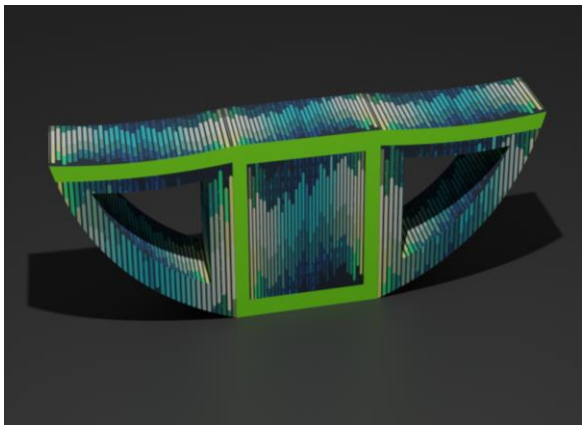
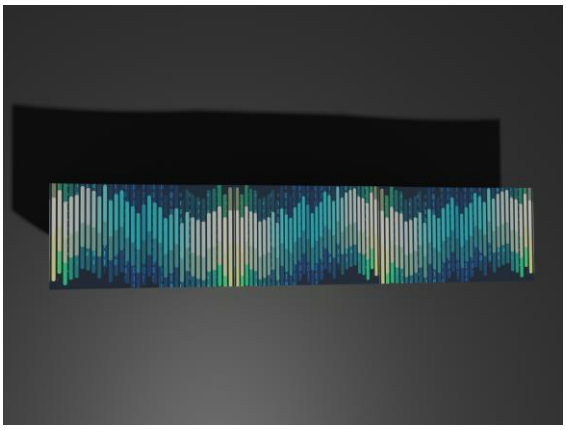
Arduino pro mini

DC Motor

Servo motor

Ultrasonic Sensor	25*7.4*3.2 mm	Max. Sensing Range: 450 cm Operating Voltage: 5 V
Bluetooth Module	3.5*3.5*1mm	Reference Distance: 40m/2Mbps Working Voltage: 1.8~3.6V
Arduino Pro Mini	33*18mm	Circuit Operating Voltage: 5V Microcontroller: ATmega328
Motor Driver IC	20*7*5mm	Voltage: 12-24 V Number Of Pins: 4
Servo Motor	32*12mm	Torque: 2.5kgf-cm 3.0kgf-cm Voltage: 4.8V-6.0V
DC Motor	25*15* 20 mm	Rated current (mA): ≤180. Rated power (W): 0.37. Rated Torque (N-cm): 16.3

The device can be attached to the vehicle using snaps or Velcro adhesives. It's detachable and can be used on other vehicles including 2 wheelers like bikes, scooter, etc. as per the need. All the interior components including the Arduino UNO, servo motor, ultrasonic sensor, Bluetooth module, motor driver IC, etc. fit in 200mm*60mm*30mmdimensional structure/package.

IV. DISCUSS

This project is designed to build a device that can warn us about the vehicle in the path and guide us so that we can drive safely. This device is built using Arduino UNO board and ultrasonic sensors to detect the obstacles. It uses 360 degree radar detection to detect the person or animal in the path. The LIDAR systems also use these features but that device does not look appealing on the vehicle and cannot work well in bad environmental conditions like fog or heavy rains [29]. So the device we have introduced can work well in low light or bad environmental conditions and it has water proof casing so that its functioning is not affected by environmental factors. This ultrasonic sensor keeps calculating the distance between the object and the vehicle and if the object is close to the vehicle it helps to detect the path which has less obstacles by using the servo motor so that the driver can take a different route and avoid any crashes. The augmented reality app called imagGinyze helps to notify and alert the driver by showing the distance between the object and the vehicle. [30] It does not notify any other route as it is virtual and has computer generated images so it does not have any sensor or motors like servo motors which can find the path that does not have a vehicle close by. The main feature that has been introduced is that it has an identifiable sound buzzer that is mild enough to alert the driver well in advance and

also not disturb him/her while driving, so that the driver can take the necessary precautions. A Bluetooth module is used in this device so that it can be connected to smartphones / smartwatches/ tablets through an App via Bluetooth and will notify using an app that will detect live objects on the road. The user has to download the app and connect it to the device so that the device can start functioning the moment it is connected.

V. CONCLUSION

The device starts working as soon as it detects a human, animal or object in its path.
It notifies the driver on phone/ tablet / smart watch via Bluetooth. The path with no/ less obstacles is notified to the driver so that the driver can take a safe route and avoid accidents, or hurting the pedestrians or animals in the way. This device works perfectly fine at night time and is waterproof to avoid any type of damage during unfavourable environmental conditions. It is detachable and can be used on other vehicles as well.

VI. ACKNOWLEDGEMENT

We would like to express our gratitude to Prof. Ganesh Jadhav for his helpful guidance, encouraging support and useful critics for this research paper. We would also like to thank our generous field study participant for providing us with valuable information. All the authors were relentlessly working towards betterment of this research paper. This paper has been read and approved by the authors.

VII. REFERENCES

[1]. Mohanty, C. R., Radhakrishnan, R. V., Jain, M., Sasmal, P. K., Hansda, U., Vuppala, S. K., & Doki, S. K. (2021). A study of the pattern of injuries sustained from road traffic accidents caused by impact with stray animals. Journal of Emergencies, Trauma, and Shock, 14(1), 23.
[2]. Untitled Road accidents in 2019
[3]. Combs, T. S., Sandt, L. S., Clamann, M. P., & McDonald, N. C. (2019). Automated vehicles and pedestrian safety: exploring the promise and limits of pedestrian detection. American journal of preventive medicine, 56(1), 1-7.
[4]. Sugumar, K., & Kumar, A. S. IoT Concept for Animal Detection Using ANN to Prevent Animal Vehicle Collision on Highways.
[5]. Muthusamy, A. P., Rajendran, M., Ramesh, K., & Sivaprakash, P. (2015). A review on road traffic accidents and related factors. International Journal of Applied Engineering Research, 10(11), 28177-28183.
[6]. Bartonička, T., Andrášik, R., Duľa, M., Sedoník, J., & Bíl, M. (2018). Identification of local factors causing clustering of animal-vehicle collisions. The Journal of Wildlife Management, 82(5), 940-947.
[7]. Nine stray animals injured in road accidents in Nagpur every day over 52 months | Nagpur News
[8]. https://ieeexplore.ieee.org/abstract/document/7792584/
[9]. Khan, M. A., Grivna, M., Nauman, J., Soteriades, E. S., Cevik, A. A., Hashim, M. J., ... & Al Azeezi, S. R. (2020). Global incidence and mortality patterns and forecast of Pedestrian Road Traffic Injuries by Socio-demographic Index Findings from the Global Burden of Diseases, Injuries, and Risk Factors 2017 Study.

[10].Yu, X., & Marinov, M. (2020). A study on recent developments and issues with obstacle detection systems for automated vehicles. Sustainability, 12(8), 3281.
[11].Singh, S. K., & Misra, A. (2004). Road accident analysis: A case study of Patna City. Urban Transport Journal, 2(2), 60-75.
[12].Harith, S. H., Mahmud, N., & Doulatabadi, M. (2019, March). Environmental factor and road accident: A review paper. In Proceedings of the International Conference on Industrial Engineering and Operations Management, Bangkok, Thailand (pp. 5-7).
[13].Novikov, A., Shevtsova, A., & Vasilieva, V. (2020). Development of approach to reduce number of accidents caused by drivers. Transportation research procedia, 50, 491-498.
[14].AI-powered tech system can help reduce road accidents in cities KV Kurmanath
[15].How Modern Technology has Helped Improve Road Safety
[16].Advanced Technology and Road Safety
[17].Technology for Road Safety
[18].Technology Has Significantly Improved Road Safety
[19].Technology Trends for Road User Safety in Public Sector
[20].UC Berkeley UC Berkeley Authors Raford, Noah Ragland, David R
[21].Combs, T. S., Sandt, L. S., Clamann, M. P., & McDonald, N. C. (2019). Automated vehicles and pedestrian safety: exploring the promise and limits of pedestrian detection. American journal of preventive medicine, 56(1), 1-7.
[22].Deb, S., Carruth, D. W., Sween, R., Strawderman, L., & Garrison, T. M. (2017). Efficacy of virtual reality in pedestrian safety research. Applied ergonomics, 65, 449-460.
[23].VARE, S., Huhta, M., & MARTIN, M. (2003). The facilities for animal movements across highways and roads. TIEHALLINNON SELVITYKSIA, FINNRA REPORTS, (36).
[24].Borkovcová, M., Mrtka, J., & Winkler, J. (2012). Factors affecting mortality of vertebrates on the roads in the Czech Republic. Transportation research part D: transport and environment, 17(1), 66-72.
[25].Joshi, S., Nair, G., Koch, I., Drysdale, M., & WA, M. R. Developing Proactive Solutions to Animal Strikes on Regional Roads.
[26].Heinonen, J. A., & Eck, J. E. (2007). Pedestrian injuries and fatalities (No. 51). Washington, DC: US Department of Justice, Office of Community Oriented Policing Services.
[27].Yang, X., Zou, Y., Wu, L., Zhong, X., Wang, Y., Ijaz, M., & Peng, Y. (2019). Comparative analysis of the reported animal-vehicle collisions data and carcass removal data for hotspot identification. Journal of advanced transportation, 2019.
[28].LIDAR Solutions | Analog Devices
[29].Why LiDAR is Doomed
[30].Augmented Reality iPhone Driving App Detects Obstacles In Real Time
[31].ADAS: Everything You Need to Know

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Study of IoT Advancements in Cybersecurity

Krishna Chaitanya Kotabhattara[1], Yogeshwari Makwana[2], Sailesh Iyer[3]

[1]B. Tech Student, Department of CSE, Rai School of Engineering, Rai University, Ahmedabad, Gujarat, India

[2]Assistant Professor, Department of CSE/IT, Rai School of Engineering, Rai University, Ahmedabad, Gujarat, India

[3]Professor, Department of Computer Science Engineering, Rai School of Engineering, Rai University, Ahmedabad, Gujarat, India

ABSTRACT

The Internet of Things (IoT) has emerged as a rapidly growing solution for automation problems. Digital Transactions have given rise to many cyber attacks thereby increasing threats considerably. This review paper provides a comprehensive survey on how to tackle and protect our data from attackers. A study of modus operandi used by Attackers has been presented and future dimensions and roadmap have been discussed in this paper.

Keywords: -Artificial Intelligence (AI), Cryptography, Cyberattack, Cybersecurity, Internet Of Things (IoT)

I. INTRODUCTION

IoT (Internet Of Things) has developed a lot in the last few years, from fitness trackers to our home automated assistants. Its use has been increased to more than 25% throughout the world, the analysis says that by the end of 2030, the number of users will exceed more than 100 million [1].

Many businesses and governments have invested in IoT, with this current covid pandemic, everyone's focus shifted to the healthcare sector and huge benefits were gained from patients wearables to direct receiving of information to doctors on their patient conditions, vitals, etc. on smartphones.

Research indicated that the productivity of IoT will increase up to more than 56% and over 15-12% of production will be contributed to the healthcare sector by the end of this decade.

With these many benefits, numbers, percentages, and increases in the development of IoT, Cybersecurity experts are concerned about its security. These numbers also give new opportunities to hackers/cybercriminals.

One can simply say that the detection of this network traffic is difficult to maintain. In this paper, Our goal is to present a deep analysis of how attackers approach.

II. COMPARATIVE ANALYSIS OF CYBERSECURITY

One of the concerns is the Application Programming Interface (API). API is like a gateway through which one can easily access the data and is frequently used a lot in IoT these days. Attackers can easily modify the network requests and cause changes in data, for example:-

Traffic Light Signals:-Attackers can easily access the wireless network and can modify the data to send a wrong response to the server. One of the examples is traffic lights, where an attacker can send invalid modified data to a server which will cause invalid traffic lights and will lead to road accidents.

Surveillance cameras:-This is one of the most common attacks, attackers can simply exploit and get into any cameras easily to spy or access personal data.

Petrenko et. al.[1] have explored various methods of paying Big Data Analytics in the Cybersecurity domain. Andrade et. al. [2] have exhaustively discussed Cybersecurity using IoT in the Smart Cities domain. Andrade et. al.[2] have explained how Bayesian Model can help us to counter and lower cyberattacks in smart cities(IoT). However, there are some gaps in that, and have promised to present a working model on it in the future.

So basically any network-based IoT can be penetrated by modifying the HTTP request data. With these many vulnerabilities, one can simply ask themselves there is any proper security for this?

Yes, there is, Rate limiting the requests and using cloud services. P.B.Patel et. al. [12] discuss the difference between traditional methods and current methods proposed by various researchers. The comparison of Cyber Crime mitigation models gives us a broad picture of which model or hybrid model can work for providing a secure and cost-effective solution [12]. B. Jajal et. al. [13] have compared and proposed various methods of mitigating illicit ports using Website port scanning tools. S.S.Iyer et.al. [14] have explored Machine Learning applications in the domain of Cybersecurity.

III. TECHNIQUES OF CYBERATTACKS

Parameters	Method	Specification	Result	Source
Authentication [2]	Here attackers can easily use HTTP debuggers to get the request-response data of the server and then can simply use brute force techniques like dictionary attacks to bypass[7]	IoT Layer:- Device Layer	OWASP Classification:- Weak	Ref :- [2]
Wireless Control [3][15]	Attackers can also control IoT models once they install some kind of malicious software to that particular IoT model	IoT Layer:- Network Layer	OWASP Classification :- Insecure	Ref:- [3] [15]
Cryptography [4] [14]	If the data is not encrypted properly and is in plain text, it just makes it way too simple for attackers to crack the code.	IoT Layer:- Network Layer	OWASP Classification:- Cryptography failure/Lack Of Cryptography in code	Ref:- [4] [14]

API [5]	If the API URLs are not handled correctly one can simply code bots to send multiple requests to the server at once	IoT Layer:- Network Layer	OWASP Classification:- Broken Authentication	Ref:- [5]

Table 1:- IoT Vulnerableness

Now using the rate limit will block the particular IP from sending multiple requests at once which can help decrease cyberattacks, 2nd is cloud services like Google, Microsoft, Amazon Webservices have their in-built tools that you use to encrypt your data, give authorization, and manage IP addresses, firewalls, etc.
Although this doesn't completely save us from attackers at least helps to decrease the attacks down. But once attackers decipher the keys, it's all gone.
This raises a question is there any system out there that can completely counter attackers and can save our data?

IV. REVIEW METHODOLOGY

Questions raised while writing this review paper:-
What type of encryptions should we use? No matter what we use, there is always a way to break through it
Is there any way to the test system for all kinds of attacks and give us detailed information on how powerful our Cybersecurity system is?
Do we have to use cloud security to protect our data?

A. Qualitative Analysis:

This topic was chosen because of the booming growth in AI/ML/IoT Technology Sector. And is still considered as one of the popular topics in industries.
The main scope of writing this paper was to analyze how perfect our current cybersecurity system is, although there are plenty of ways attackers can retrieve data.
One of the studies tells us that using encryptions will help a lot, cause it takes time to figure out the key you used to encrypt your data, there are many and many encryptions algorithms out there. One of the examples is:- HMAC + MD5, you can use many encryption combinations to secure your data and which will also help slow down the attacking process for attackers.
We also talked about what happens when you don't use cryptography in your API URL which will lead to multiple attacks on your server, a broken authentication.

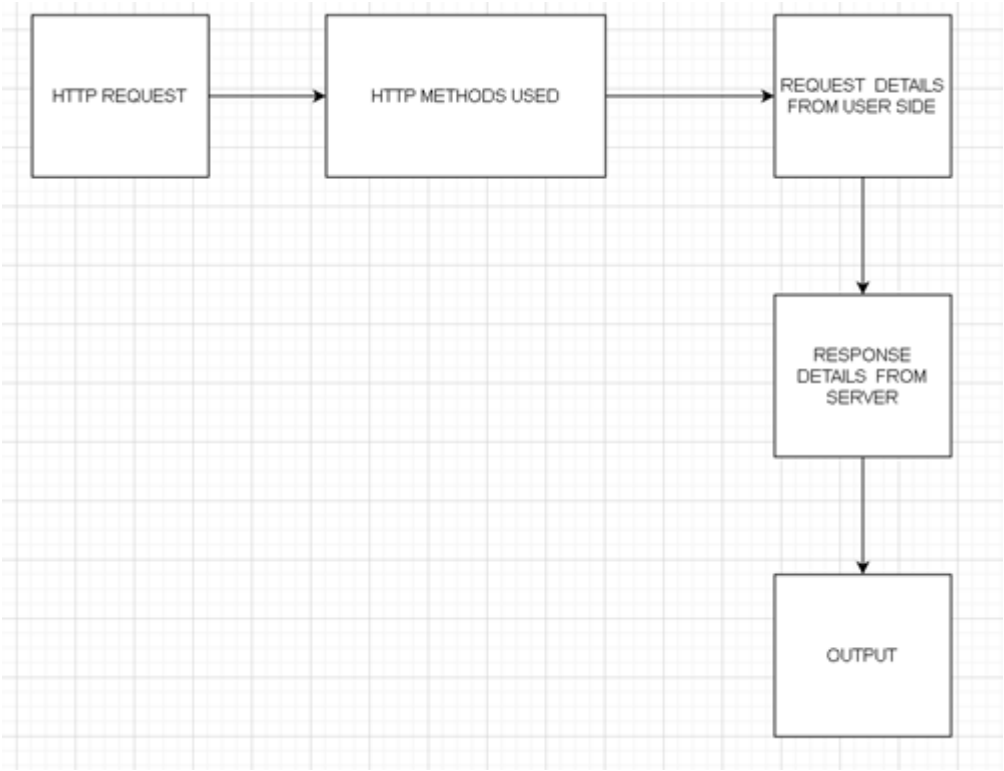


Fig.1 Network structure[10]

The above diagram explains the flow of the network structure.
HTTP REQUEST:- In this, we input API URL for sensors info
HTTP METHOD:- Here we check whether the IoT model is using the POST method or GET method to retrieve/send the data to the sensor
REQUEST DETAILS FROM THE USER SIDE:- Here attacker can read the details of data and can modify it by editing and resubmitting it which triggers the fake data at the server-side
RESPONSE DETAILS FROM SERVER:- Attacker can simply dummy test first data and can figure out what to change in request data.
This method can also be used as a DDoS attack [8].

B. Applications attackers use:

1. HTTP Debuggers:- Applications like Wireshark, Fiddler, HTTP Debugger, or any type of network sniffers to get and monitor the network data sent/received by the IoT model Schneider, Michael. et. al. [7] explain how IDEs can't find breakpoints of the particular code, if it was fixed, people would be able to debug and fix the errors/bugs, which can decrease the attacks.
2. Bots:- One can simply code their bot to send traffic to one particular URL/Site. One way to do this is by using Linux and the second is simply coding your bot [11][12]. Elahi, Meisam, et al. [9] suggest that Detecting botnets using HTTP is more difficult because botnet traffic is hidden in a large amount of normal HTTP traffic which makes it hard to monitor the network flow data.
3. Bruteforce/Dictionary attacks:- Depends on whether the IoT project has any POST data, if it has then one can simply get the data of URL (i.e. explained in the above diagram) and implement it in bots/Linux.[9]

4. Malicious software:- One can also install malicious software in an IoT model and can simply access it without the developer knowing [6] [13]. Overall there are many applications out there that one can use to exploit IoT.

V. CONCLUSION

Internet Of Things (IoT) will still stay as one of the popular topics in industries and will gain billions of users soon in the future, however with the increase in its popularity, it will also gain attackers' attention. With this review paper, we have identified what attackers can do, how they can approach, how we can tackle them, and what cybersecurity's scope is in the future.

Two of the main points were described in the table and diagram and were explained how an attacker can modify the data and send a wrong response to the server to cause wrong interactions of that particular IoT model.

VI. REFERENCES

[1]. Petrenko, Sergei A., and Krystina A. Makoveichuk. "Big data technologies for cybersecurity." CEUR workshop. 2017.

[2]. Andrade, Roberto Omar, et al. "A comprehensive study of the IoT cybersecurity in smart cities." IEEE Access 8 (2020): 228922-228941.

[3]. M. Capellupo, J. Liranzo, M. Z. A. Bhuiyan, T. Hayajneh, and G. Wang, "Security and attack vector analysis of IoT devices," insecurity, Privacy, and Anonymity in Computation, Communication, and Storage, G. Wang, M. Atiquzzaman, Z. Yan, and K.-K. R. Choo, Eds. Cham, Switzerland: Springer, 2017, pp. 593–606.

[4]. K.-H. Hsu, Y.-H. Chiang, and H.-C. Hsiao, "SafeChain: Securing trigger-action programming from attack chains," IEEE Trans. Inf. ForensicsSecurity, vol. 14, no. 10, pp. 2607–2622, Oct. 2019.

[5]. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of Internet of Things: A case study of the smart plug system," IEEEInternet Things J., vol. 4, no. 6, pp. 1899–1909, Dec. 2017

[6]. Shi, Hao, and Jelena Mirkovic. "Hiding debuggers from malware with apate." Proceedings of the Symposium on Applied Computing. 2017.

[7]. Schneider, Michael. "Pin Status: An Arduino Debugging Library for High School E-textile Courses." SIGCSE'20: Proceedings of the 51st ACM Technical Symposium on Computer Science Education. 2020.

[8]. Hong, Kiwon, et al. "SDN-assisted slow HTTP DDoS attack defense method." IEEE Communications Letters 22.4 (2017): 688-691

[9]. Elahi, Meisam, et al. "Periodicity classification of HTTP traffic to detect HTTP Botnets." 2015 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). IEEE, 2015.

[10]. Li, Jia, et al. "A method of HTTP malicious traffic detection on mobile networks." 2019 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2019.

[11]. Freeman, Adam. "Creating HTTP Clients." Pro Go. Apress, Berkeley, CA, 2022. 663-691.

[12]. P. B. Patel, H. P. Thakor, and S. Iyer, "A Comparative Study on Cyber Crime Mitigation Models," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 466-470.

[13].B. Jajal, S. Iyer and D. Chauhan, "Mitigating Illicit Entry using Website Port Scanning Tools in Indian Context," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 1223-1226.

[14].Iyer, S. S., and Rajagopal, S. (2020). Applications of Machine Learning in Cyber Security Domain. In Handbook of Research on Machine and Deep Learning Applications for Cyber Security (pp. 64-82). IGI Global.

[15].D. Chauhan, S. Iyer and B. Jajal, "Enhanced Prototype Model for Energy Efficient Algorithm of LEACH over Wireless Sensor Network," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 569-573.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Converting Normal Locks to Smart Digital Locks using IoT

Samruddhi Sunil Bhegade, Laxmi Mohan Choudhary
Master of Computer Science, Indira College of Commerce and Science, Pune, Maharashtra, India

ABSTRACT
Humans are using locks since ages, to ensure protection of their privacy and belongings. they are constantly evolving new techniques for better protection. Traditionally physical keys and a lock are the basic requirements for a door. However, managing these keys has become an issue. Digital locks are regarded as the modern successor of the traditional lock. Threat to life and property have initiated the invention of digital lock systems which has evolved with technological advancement. In recent times, digital locks are widely used as part of the IoT (Internet of Things). In spite of that many cases of digital locks being hacked or opened by invalid users to invade homes and offices are reported. To solve this problem, we need to combine all the modern security and monitoring features into one lock to achieve high security, comfort of living and features that help us easier and faster access and help to make our homes safer than before.
Keywords— Digital lock, Smart Lock, Security, Internet of Things, Authentication.

I. INTRODUCTION

This Locks have been in use since ancient times, When the Industrial Revolution started coming into light locks and keys were manufactured with increasing complexity and sophistication. The traditional lever tumbler lock was invented by Robert Barron in 1778[1] and is still used today but it has its own limitations.[2]. Technology has made a great influence on many aspects of our life. With the advancement of technology and research, more strong security mechanisms are developed. The smart lock system is an emerging framework that is gradually replacing the traditional locks due to its convenience and affordable prices. A smart lock is an electromechanical device that performs locking/unlocking operations using wireless protocols like a cryptographic key on authentication providing access only to the authorized personnel. Smart locks are starting to be used more commonly in residential areas, [3] [4] in coworking spaces and offices, banks, shops and other organizations.
In this paper, few of the versions of smart locks are elaborated with their salient features and the possible changes that can be made to make the digital lock more smart are stated. Our goal is to design a sustainable solution for secure access control and enhance the security by combining various new intelligent services with situational awareness to the digital locks to make our homes and work places more secure.

II. PROBLEM STATEMENT

At these times, many traditional and digital locks are available to limit the penetration of their personal property or privacy, but there are many defects in these locks, such as easy penetration, poor security, and the difficulty of dealing with the lock in one way and there is no other way.

III. DIFFERENT TYPES OF DIGITAL LOCKS

WiFi enabled digital lock

Face recognition Digital lock

Numeric password deadbolt digital lock

Fingerprint enabled digital lock

Bluetooth Enabled Numeric Lock

IV. LIMITATIONS OR SHORTCOMINGS OF EXISTING PRACTICES

Most locks these days have limitations in the technical characteristics and features that are required by the circumstances of this time, for example, no lock combines the characteristics of entry in one place, which is the keypad, fingerprint, face ID, and phone, and in terms of monitoring systems such as the camera and motion sensor. we've some technological limitations. For example, if the door is not firmly closed, the smart lock may not secure the deadbolt. If the battery fails, you may find yourself locked out. Or, if your wireless network is down, you may not succeed in using remote functionality.

V. OUR APPROACH

To combine the features of various digital locks like face id, finger print, keypad, sensors to develop a super secure and smart digital lock.

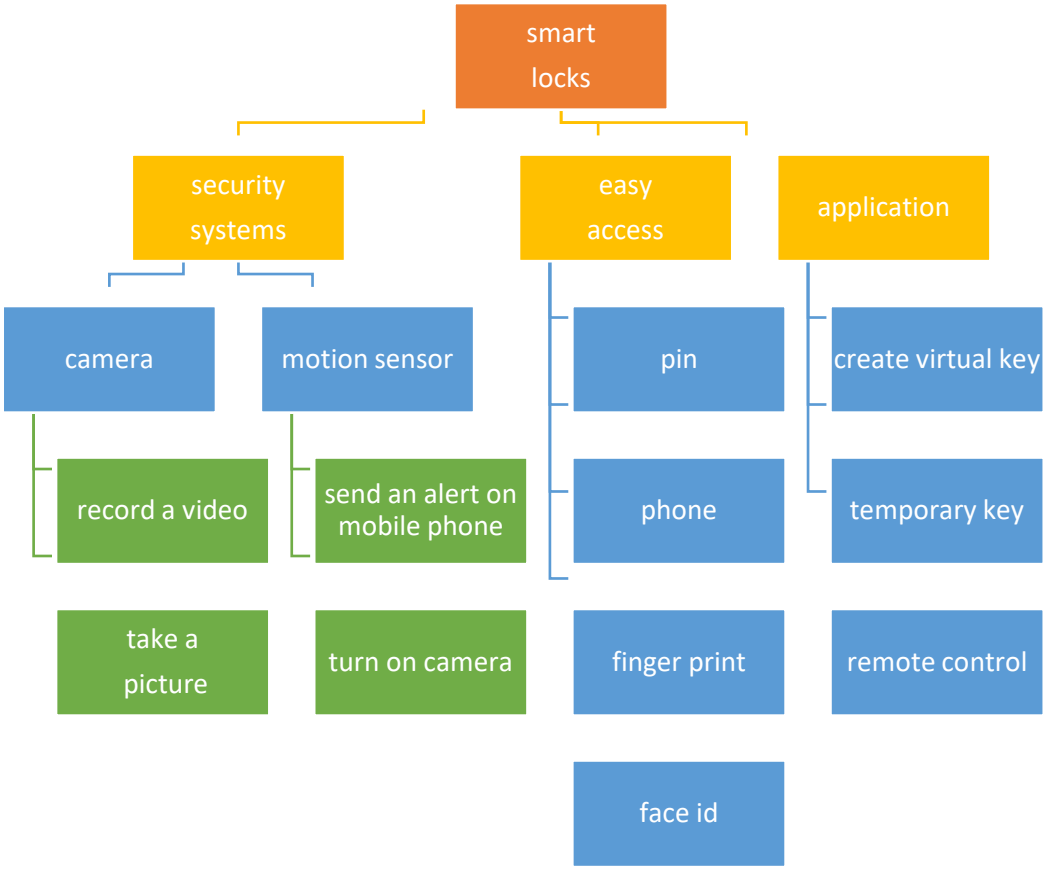


Figure 1: Objectives of a Smart Lock

VI. REQUIREMENTS

NAME	SPECIFICATION
FUNCTIONAL REQUIREMENTS	NFC tag It is a technology that works with radio waves and we take advantage of it in the requirements to facilitate for us to enter and open the lock by using this technology and it is located inside the control device.
PERFORMANCE REQUIREMENTS	We use WI-FI to get high and fast performance in transferring data from the control device to the lock so that we can control perfectly.
POWER REQUIREMENTS	The controller is used to control locking features, and it needs to be energy efficient to last longer. It uses a rechargeable battery.
ENVIRONMENTAL REQUIREMENTS	The temporary key is a good option for preserving the environment, which is to give a virtual key that is given to other users through the application instead of keys made of aluminium, so th Bluetooth Enabled Numeric Lock at we are preserving the environment.
SAFETY REQUIREMENTS	The camera and the motion sensor are safety systems that must be provided in the lock in order to protect it from many things, and it must be operable for a longer period and with high protection.

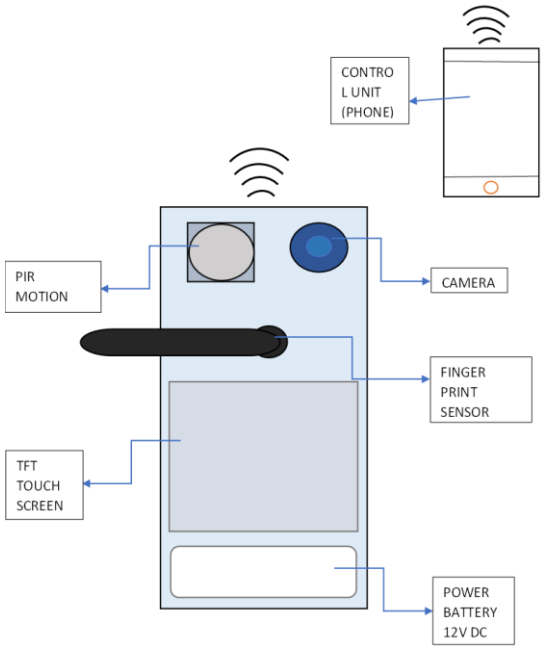
VII. CONCEPT TABLE

Considering the above requirements, we can build the following concept table to design the Smart Lock

Concept Table for Generating Security Lock System

User Interface	Control Unit	Power	Sensor	Camera
Number Pad	Phone	Battery	Infrared motion detector (PIR)	Camera vision 180^0
TFT Touch screen	Remote Control	Solar Power	Vibration Sensor	Night vision
Fingerprint Sensor	Personal Computer	AC Power	Magnetic Door sensor	FPS real time recording

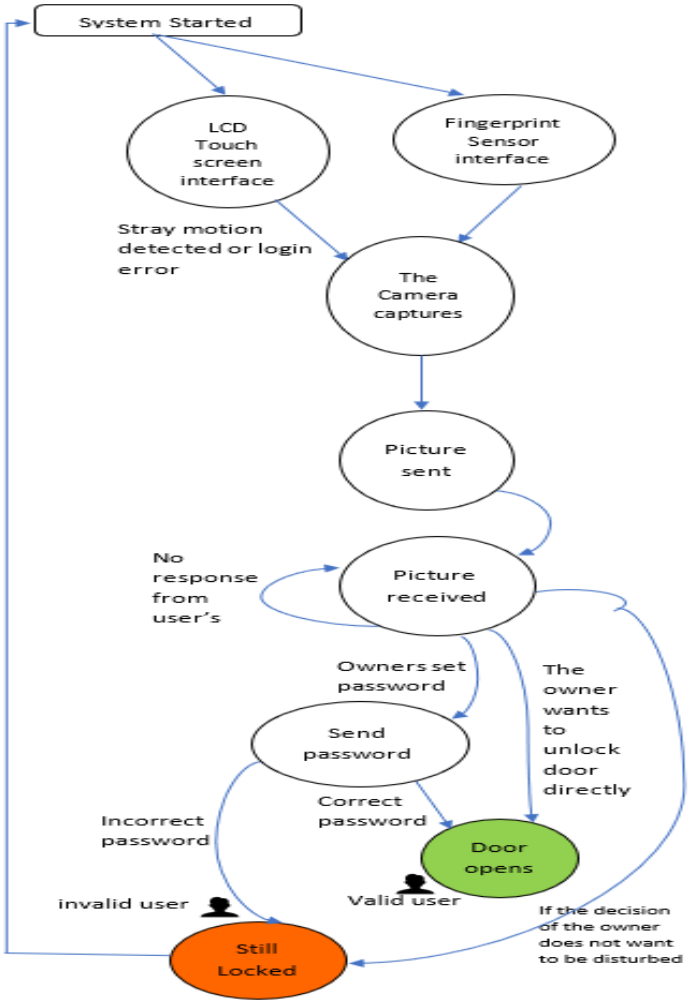
From the above Concept table, we can design the schematic representation of our Smart lock having all the above features.



Schematic Representation of Smart Lock

VIII. FINITE STATE MACHINE DESCRIPTION:

1. Start state.
a. if the door is closed, LCD touch Screen interface is activated.
b. if the door is closed, Fingerprint sensor interface is activated.
2. If stranger detected or log in error.
a. the hidden camera captures picture of visitor.
b. picture is sent from embedded system to the app of owner.
c. picture received on the app of owner.
3. The door open directly.
a. If the owner gives the command from the app, open door.
4. if there no response from owner of app.
a. stay until the owner responds.
5. the decision of the owner does not want to be disturbed.
a. does not disturb Event Door keeps locked.
6. The owner (s) set passwords.
a. Password(s) wirelessly transmitted and shown on LCD one after another (in case of multiple owners setting them).
b. if timeout of the Password the, door keeps locked.
7. visitor enters correct Password.
a. if the Password is correct, the door will open.
b. if the Password is not correct, the door still Locked and try again.



IX. CONCLUSION

In our project, we converted the normal lock into a highly secure smart lock by adding modern login features such as phone, fingerprint, keypad, and card. On the security front, we have added a camera and motion sensor so that we get higher security. The benefits were easy and fast use, high security that protects our privacy and property.

X. ACKNOWLEDGMENT

We would like to express our gratitude to our teacher and mentor Mrs. Manisha Patil for her encouragement, valuable and constructive guidance and supervision during developing this research work.
We are also grateful to our friends and colleagues for their insightful reviews and comments which led to the betterment of this work.

XI. REFERENCES

[1]. Abdullah Mohammed Saeed Alghamdi "Security Lock systems: From Problem Statement to System Design" December 2020.

[2]. Diamond Celestine Aluri," Smart Lock Systems: An Overview", February 2020, International Journal of Computer Applications, Andhra University.

[3]. Dr.N.Krishnamoorthy, Kalaimagal.R,Gowri Shankar.S, Abdhul Asif.N.S, "IOT Based Smart Door Locks", (NCIRCST 2018).

[4]. Ilkyu Ha," Security and Usability Improvement on a Digital Door Lock System based on Internet of Things" Article in International Journal of Security and its Applications · August 2015.

[5]. M. Imran and M. Rashid, "Architectural Review of Polynomial Bases Finite Field Multipliers Over GF(2m)", 2017 IEEE International Conference on Communication, Computing and Digital Systems, pp. 331-336, Islamabad, Pakistan, March 2017.

[6]. M. Rashid, M. Imran, A. R. Jafri, Turki Al-Somani, "Flexible Architectures for Cryptographic Algorithms - A Systematic Literature Review", Journal of Circuits, Systems and Computers (JCSC), vol. 28, No. 3, March 2019.

[7]. M. Rashid, M. W. Anwar, A. M. Khan, "Identification of Trends for Model Based Development of Embedded Systems", 12th IEEE International Symposium on Programming and Systems, pp. 1-8, Algiers, Algeria, April 2015.

[8]. M. Rashid, M. W. Anwar, A. M. Khan, "Towards the Tools Selection in Model Based System Engineering for Embedded Systems - A Systematic Literature Review", Journal of Systems and Software, vol. 106, pp.150-163, May 2015.

[9]. Nishad N. Gupte, Mihir R. Shelar, Department of Electronics Engineering, Datta Meghe College of Engineering, Airoli " Smart Door Locking System" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 11, November – 2013.

[10].Palak A Davda1 , Soni B Ahirrao2 , Avinash Dangwani3" IoT Based Smart Door Lock System"2020.

[11].S. O. Anaza 1 , J. D. Jiya2 and Y. S. Haruna2, "A Review of Intelligent Lock System" 2017.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Construction Industry Digitization using Internet of Things Technology

Poonam Katyare, Dr. Shubhalaxmi S. Joshi
Department of Computer Science, Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India

ABSTRACT
The Construction Industry is one of the key engines for the economic growth of the country. Construction Industry is lacking behind due to low productivity and use of recent trends in technology. There is a need to digitize the operations in construction industry. In the recent Techno world, Internet of Things Technology becomes very popular by using sensors and actuators to digitize the tasks. Digitization in the Construction Industry using IoT technology will provide Smart systems with improved efficiency and productivity of the operations in construction sector. This paper highlights use of IoT technology in the field of construction industry with various sensors available to automate the tasks involved for the execution of the construction projects on the construction job sites. This paper shows a brief overview on different sensor-based technology of the IoT and presents the impacts of the IoT on construction operations. It also discusses the importance and necessity of techno trends of the Internet, wireless sensors and actuators and data captured from sensors for timely and fast completion of the construction projects.

Keywords— Construction Industry, Internet of Things Technology, Digitization, wireless sensors, actuators.

I. INTRODUCTION

According to the Gross Domestic Product (GDP) of the country, approximately 7.16% to 8% share contributed by the construction industry which impacted on the economic growth of the country. Though, the construction industry is considered through low efficiency and productivity with low technological recent trends, less modernization/automations, and innovations etc. The Digitization, innovation and automation of Construction Industry helps to expand the productivity and efficiency of the operations performed at the construction sites. It is observed that use of recent trends in technologies and automation is very negligible in the construction industry. Indian economy is also impacted by the construction industry's growth. Growth and performance in productivity of construction industry is highly depending on the timely completion and fast execution of the construction projects. Government of India offers the construction buildings projects at high level. Significant challenges are faced by the construction industry as related to the workers, equipment and materials used in construction. Operations related to the workers and equipment need to be monitored carefully.

Significant study related to the new and advanced trends in technologies provides the enhancement of productivity in construction projects. Internet of Things is one of the recent trends in technology which enable the use of wireless sensor technology to capture data remotely. It highly contributes to improve the productivity of construction. Construction project lifecycle might be depends on assimilation of IoT and the other techno trends as Cloud Computing, Blockchain technology, Advanced Robotics, Artificial Intelligence, Augmented Reality, Embedded Systems, Machine Leaning, Advanced Networking with wireless sensor network and Big Data Analysis [2]. Live monitoring of construction job site becomes very easy by using Internet-of-Things (IoT) based advanced safety model. Along with safety information digital data is also get stored which can be used to predict the future. Analysis of operations performed by the employee and the equipment lead towards the cost monitoring, labour performance, equipment activity monitoring and provides the safety environment at the construction job sites [6]. Integrating IoT in the construction industry digitization is a new substance that leads us to the next Construction Industry 4.0 revolution. This paper reviews the necessity of IoT usage, importance of IoT and benefits of IoT in construction industry along with the applications of IoT.

II. RELATED STUDY

Significant study is found on the Construction Industry Digitization using Internet of Things technology which would enhance the efficiency and productivity of construction projects. The IoT initiates one of the emerging Industry 4.0 tools accessible in the field of the construction industry. IoT Research is an emergent stage of development which is rising rapidly. Authors have done related study of the IoT in the construction industry literature by using analytical, systematic approaches and presented some highlights which show less research study in the applications of IoT for construction job site activity monitoring, equipment health monitoring, safety at construction job site and decision making from the activity monitoring. Acceptability of such advanced technology is poor and it is observed that there is a lack of knowledge to adopt and understand the IoT technology [1]. The adoption of IoT in the Malaysian construction industry is proposed by the study which promotes use of IoT in the Construction Industry is very necessary for the growth the country. They have used IoT in for the purpose of monitoring the construction job site, for controlling the machinery, for providing the construction safety, for fleet management and for the overall project management. The accuracy of correct data from IoT devices will improve the project performance. Use of IoT devices on remote site will reduces time and efforts of employee for monitoring the tasks in Malaysia [2].

Authors used research study to showcase the IoT components and their functions in the construction industry. During the COVID-19 pandemic situation construction industry faced the various challenges like lack of availability of labours, delays in completion of projects, rescheduling of the existing projects to streamline the project work which results in economic loss of the country. Healthcare IoT as Internet of Medical Things (IoMT) plays very vital role during pandemic situation. IoMT serves the various medical applications which combine the medical devices with the software IT systems which helps in tracking the medical orders, patient monitoring and transmitting heath information to the respective medical health care departments. It also provides the patient data for analysis and diagnosis. IoT and IoMT really help in handling the influence of the COVID-19 pandemic [3]. Review study presented the maximum used IoT essentials in the construction industries are Wi-Fi, WSN, visualization, Bluetooth and RFID. Survey based data is collected from the construction professionals which help in identifying the level of adoption on the importance of IoT elements [4].

Some research study focus on the intelligent buildings and intelligent manufacturing using IoT technology. The integrated system model results in the combination of human society and physical system which helps in achieving the objective of real-time management along with monitoring the workers, machines, equipment and infrastructure on the job sites. Data from the intelligent buildings model with the wireless sensor network and communication network provides information of activity and operation of workers and equipment lead to perform the security, business decision making, cost and labour productivity in the construction industry [5]. Safety model using IoT is also proposed which used to monitor the construction job site environment and recognizes the live personnel safety problems and helps in reduction of accident rates and provides optimized construction safety. Author studied the accident rates per year in Hong Kong. Questionnaire survey was conducted and data was collected and used for analysis. [6].

Several revisions of study have been conducted using IoT and its performance has been monitored in the field of construction. It is possible to monitor the temperature and humidity of ready mix concrete remotely for making decision to the contractors on the job site. Various sensors, actuators, drone cameras are the helping hands of IoT to make construction industry with cost reduction and safety maintenance [7]. Author promotes the use of IoT with network technology, sensing technologies and cloud computing to form an effective administration and management system. This system encounters the needs of museum development and led toward the wisdom museum. Secure, convenient, efficient and safe heritage system with real time monitoring is possible using IoT technology [8].

Study related to create smart construction is observed and challenges faced in adoption of IoT in construction is listed such as onsite equipment management, transportation and packaging, time consuming task of monitoring real time operation, lack of communication and connectivity, lack of skilled employees, energy and water management issues, security, privacy, safety, maintainability, scalability and portability along with a main constantly changing environment and fragmentation among the construction industry investors, which contributes increase to difficulties such as data ownership, and investments in projects-based organizations. [9].

Business Model Innovation tool is studied and used by author to provide serialization of construction equipment in concrete industry along with working of IoT Networks, data collection prerequisites and data collection with various methods. Extended warranty, Preventive services, Live control of batching quality, Automatic documentation, Service reminder, Off-site support, Security for manager, Consultancy regarding batching recipes, Map overview of batching plants of operating batching plants and location and Batching plant security these types of services were provided by the Business model using IoT [10].

Author presented the practical integration between micro and macro IoT approaches, by given an architectural and details of performance measurement for a set of validation tests carried out in the campus of the University of Parma along with issues, difficulties and solutions of the proposed micro–macro integrated IoT systems [13].

Some study analysed the various technology with IoT smart sensors, technologies like RFID, ZigBee, Cloud Computing and Industry 4.0 which used to collect data and analysed it. This advanced sensor based IoT digitization is used in an application of monitoring of Agricultural Standardized Production [15].

III. IOT TECHNOLOGY

In era of digitization, Internet of Things technology is key driver for industry societies and other communities. IoT provides the devices which are embedded with commodity sensors, gateways, software and other

technologies computation which perform the data communication over the network of networks. IoT offers the Smart systems for Home appliances and commercial approaches along with Industrial sectors. It will provide the instant access to information about the physical world and the objects in it. It will leading to innovative services and increases in efficiency and productivity of the tasks. IoT means the things or objects to be combined into a common framework as internet [16].

IoT used in the different areas as manufacturing, agriculture, health, transport, retail and many more. It provides the services at large extend and provides a large amount of data over the internet. This data can be used to analyse the pattern of behaviour and making the business decisions using recent trends in technologies as Artificial Intelligence and Machine Learning. Big Data analysis is also used for structuring the large volume of data to retrieve information and knowledge from the raw data. It enables to communicate live data by linking all different objects and adding sensors to them enhances a level of digital intelligence to devices. [10]. When IoT is used for the business purpose that is renamed as The Industrial Internet of Things (IIoT) or the fourth industrial revolution or Industry 4.0. The objective of this is to use a blend of sensors, wireless networks, big data, AI and analytics to measure and optimise all the industrial processes.

A. IoT Key Features:

IoT provides the key features in large extends with Sensors, actuators, connectivity to cloud, identification technology, networks and communication, data storage, data processing, data analysis, softwares and algorithms , hardware interface, data and signal processing methods, power and energy storage , security and privacy, and user interface are the key features of IoT [16]. Internet of Things offers features in the form of things which are tagged and connected. Equipments or devices are attached to other devices through sensing technologies or sensors. Intelligence is another key feature which shows the sensing capabilities in IoT devices and the intelligence assembled from big data analytics. The IOT Gateway is a one of the key feature which is working as a bridge between telecommunication network or Internet and the Wireless Sensor Network (WSN) [17].

B. IoT Architecture:

IoT refers to all things which are connected to the internet and things can communicate with each other via internet. Huge data can transfer and processed across the network of networks. IoT Architecture is centre place of all sensors and actuators, getaways and the processed data which directly connected to the key features of IoT. IoT architecture consists of five layers which are Perception, Transport, Processing, Application and Business layer.

1. **Perception Layer** : This is the physical layer, which integrates physical devices as sensors or actuators for sensing and collecting data. Sensors are responsible to collect the data about the environment and from the connected devices. They sense some physical parameters or identify other smart objects in the environment. These sensors or actuators may be connected either through wired or wireless. This contains GPS, Electrochemical, Gyroscope, RFID, etc. Most of the sensors need connectivity through sensors gateways.
2. **Transport Layer:** This layer defines the transfer of data between the sensors in the Perception layer and the Processing layer through various networks. This transportation is mainly done through networks such as Software Defined Networking (SDN) or Network Functions Virtualization (NFV), 5G, wireless, local area networks, Radio Frequency Identification (RFID), Bluetooth, and NFC. The connection of sensors or actuators can be through a Local Area Network (LAN) or Personal Area Network.

3. **Processing Layer:** This layer acts as the Middleware layer which stores the data, analyses the data, and pre-processes the data coming from the Transport layer. In modern software applications, this is often located on the edge of the cloud for low potential communications. Edge in the IoT Architecture is the hardware and software gateways that analyze and pre-process the data before transmitting it to the cloud. If the data read from the sensors and gateways are not required to be changed from its prior analysis value then it does not transfer over the cloud, this saves the data used.
4. **Application Layer:** The layer is what the users' views in the form of user interface. This may be an application or dashboard which is used to provide the insights of the status of connected and non-connected devices.
5. **Business Layer:** This layer describes the whole IoT application system, including decision-making from the observation of data, implementing the profit models, applications, and businesses with the stakeholders.

IV. DIGITIZATION IN CONSTRUCTION INDUSTRY

Construction Industry is facing the challenges of low productivity and monitoring of tasks performed at the construction sites. Digitization in Construction Industry using Internet of things technology would help in improving the productivity and real time monitoring of the activities at the job site at high extend with accurate information. IoT offers keys to the construction industry problems using various things in the form of smart things and provides fast and instant solutions to the real world of construction industry.

The IoT technology is making an influence on the concrete industry slowly. As per the requirements the IoT solutions has led to progress of IoT technologies for different drives. IoT provides new processes, new business models with Buildings as a Service', new smart products, new services, New relationships as IoT enables a long-term partnership between the customer and the construction industry that provides a Building as a Service. Various technologies along with IoT as Industry 4.0, Blockchain technology, Cloud Computing, Building information modeling (BIM), advanced digital technologies need to be applied to enhance productivity and value creation for the efficient and accurate monitoring of the activities of construction job sites [11-12]. Cloud computing with the IoT is used for efficient management and handling of energy sensing data for smart building [14]. The IoT platform helps to the monitor workers and equipment performance on a real-time basis. It provides exciting opportunities for the construction industry to solve its time and resource constraints and frequent breakdowns. This would be able to identify a large amount of new service possibilities and product development possibilities, which can create new business opportunities. IoT provides safety monitoring on the construction industry job site. IoT network technology has been applied using various sensors at the in various types of workspaces such as buildings , warehouses and exhibition centres and collects the real time data to monitor and helps in reduction of accident rates at the job site along with providing safety environment at job site. Study compares the cost savings from traditional way of monitoring the job site along with sensor-based system in which it is observed that sensor-based system enables saving in time and cost for site safety [6].

Along with benefits of IoT in construction industry there are some challenges in the IoT networks as the traffic load and traffic models. Per day a large volume of objects are being connected to the internet, which cause a large amount of traffic because more data has to be stored. Privacy and security risks are the other challenges in implementing the IoT. Study provides enormous applications of IoT in construction industry digitization.

V. CONCLUSION

Construction Industry is one of the key contributors in economy of the country. It is observed that construction industry faces e some challenges in execution of construction projects at the job sites which can be solved by the use of IoT technology. This paper focuses on presenting the study of construction industry challenged in traditional approach and focus on the new technologies with IoT to overcome that challenges. This paper tried to summarize actual IoT key features which can used to improve the productivity of construction personnel and equipment along with IoT architecture. Construction industry digitization really helps in business model enhancement with fast business decision making. The establishment of the Internet of Things (IoT) in construction development is beneficial to reduce the construction time as well as the cost.

VI. REFERENCES

[1]. A. Ghosh, D. J. Edwards, and M. R. Hosseini, "Patterns and trends in Internet of Things (IoT) research: future applications in the construction industry," Eng. Constr. Archit. Manag., vol. 28, no. 2, pp. 457–481, 2021, doi: 10.1108/ECAM-04-2020-0271.

[2]. F. S. Ibrahim, M. Esa, and R. A. Rahman, "The adoption of iot in the Malaysian construction industry: Towards construction 4.0," Int. J. Sustain. Constr. Eng. Technol., vol. 12, no. 1, pp. 56–67, 2021, doi: 10.30880/ijscet.2021.12.01.006.

[3]. V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact," IEEE Access, vol. 8, no. April, pp. 90225–90265, 2020, doi: 10.1109/ACCESS.2020.2992341.

[4]. V. A. Arowoiya, A. E. Oke, C. O. Aigbavboa, and J. Aliu, "An appraisal of the adoption internet of things (IoT) elements for sustainable construction," J. Eng. Des. Technol., vol. 18, no. 5, pp. 1193–1208, 2020, doi: 10.1108/JEDT-10-2019-0270.

[5]. L. Kong and B. Ma, "Intelligent manufacturing model of construction industry based on Internet of Things technology," Int. J. Adv. Manuf. Technol., vol. 107, no. 3–4, pp. 1025–1037, 2020, doi: 10.1007/s00170-019-04369-8.

[6]. W. W. S. Chung, S. Tariq, S. R. Mohandes, and T. Zayed, "IoT-based application for construction site safety monitoring," Int. J. Constr. Manag., vol. 0, no. 0, pp. 1–17, 2020, doi: 10.1080/15623599.2020.1847405.

[7]. S. Paul, B. Naik, and D. Kumar Bagal, "Enabling Technologies of IoT and Challenges in Various Field of Construction Industry in the 5G Era: A Review," IOP Conf. Ser. Mater. Sci. Eng., vol. 970, no. 1, 2020, doi: 10.1088/1757-899X/970/1/012019.

[8]. G. Ke and Q. Jiang, "Application of Internet of Things technology in the construction of wisdom museum," Concurr. Comput. Pract. Exp., vol. 31, no. 10, pp. 1–10, 2019, doi: 10.1002/cpe.4680.

[9]. A.-Q. Gbadamosi, L. Oyedele, A.-M. Mahamadu, H. Kusimo, and O. Olawale, "The Role of Internet of Things in Delivering Smart Construction," CIB World Build. Congr., no. June, pp. 17–21, 2019.

[10]. N. V. Rasmussen and M. J. Beliatis, "IoT based digitalization and servitization of construction equipment in concrete industry," Glob. IoT Summit, GIoTS 2019 - Proc., pp. 10–13, 2019, doi: 10.1109/GIOTS.2019.8766421.

[11].S. M. Lee, D. Lee, and Y. S. Kim, "The quality management ecosystem for predictive maintenance in the Industry 4.0 era," Int. J. Qual. Innov., vol. 5, no. 1, 2019, doi: 10.1186/s40887-019-0029-5.

[12].R. Woodhead, P. Stephenson, and D. Morrey, "Digital construction: From point solutions to IoT ecosystem," Autom. Constr., vol. 93, no. October 2017, pp. 35–46, 2018, doi: 10.1016/j.autcon.2018.05.004.

[13].L. Davoli, L. Belli, A. Cilfone, and G. Ferrari, "From Micro to Macro IoT: Challenges and Solutions in the Integration of IEEE 802.15.4/802.11 and Sub-GHz Technologies," IEEE Internet Things J., vol. 5, no. 2, pp. 784–793, 2018, doi: 10.1109/JIOT.2017.2747900.

[14].J. Yu, M. Kim, H. C. Bang, S. H. Bae, and S. J. Kim, "IoT as a applications: cloud-based building management systems for the internet of things," Multimed. Tools Appl., vol. 75, no. 22, pp. 14583–14596, 2016, doi: 10.1007/s11042-015-2785-0.

[15].H. Zhou, B. Liu, and P. Dong, "The technology system framework of the internet of things and its application research in agriculture," IFIP Adv. Inf. Commun. Technol., vol. 368 AICT, no. PART 1, pp. 293–300, 2012, doi: 10.1007/978-3-642-27281-3_35.

[16].D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," Wirel. Pers. Commun., vol. 58, no. 1, pp. 49–69, 2011, doi: 10.1007/s11277-011-0288-5.

[17].Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, "IOT gateway: Bridging wireless sensor networks into Internet of Things," Proc. - IEEE/IFIP Int. Conf. Embed. Ubiquitous Comput. EUC 2010, pp. 347–352, 2010, doi: 10.1109/EUC.2010.58.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Comparative Study of Smart Farming using Technological Advancements

Sakshi Sharma[1], Karina Saiyad[1], Sailesh Iyer[2]
[1]B. Tech Student, Department Computer Science Engineering, Rai School of engineering, Rai University, Ahmedabad, Gujarat, India
[2]Professor, Department of Computer Science Engineering, Rai School of Engineering, Rai University, Ahmedabad, Gujarat, India

ABSTRACT
Farming can be basically divided into Traditional Mode and Modern Farming. Traditional Farming consists of manual methods of farming and dependence on weather and other considerations. Modern Farming uses Technology advancements to increase the output, quality of produce and also use automation in farming process. This paper explores the various methods and provides a comparative study employed in farming sector. Technological advancements including Artificial Intelligence, Internet of Things, Robotics etc. have a major influence resulting in smart farming.
Key Words — Smart Farming, Artificial Intelligence, Internet of things, Farm produce, Robotics, Farmer.

I. INTRODUCTION

Agriculture has undergo tremendous change in the last few decades. Agriculture uses land water resource as well as Natural Resource. The population is increasing at a rapid pace and agricultural produce is not able to meet the pace. Decreasing farm area due to rapid industrialization, Migration of villagers to cities and changing weather conditions have multiplied the problems faced by farming community.
There are two types of crops Kharif crops and Rabi crop.

Kharif crop:
Kharif crops are cultivated in monsoon season from June to September. Kharif crops is also known as monsoon crop example cotton, ragi etc

Rabi crops:
Rabi crops cultivated in the winter season from October to March. they are grow in the winter season and at the spring season example wheat, mustard etc. e.g. wheat the farmer aput the seed in the field due to the month of October and November that process is called sowing. After three or four month the seeds will grow properly and green field and paddy field turn into yellow at the end of month.

When crops are mature then it means it is ready to cutting. Harvesting define the cutting and gathering of mature food crop is called harvesting. After harvesting the next process is threshing processing means the seat green are separated from crops.

Agriculture tools are used in agriculture sector to reduce labour cost. Harvesting is take place at the time when the grain has moisture in the range of 18 to 20% if the high moisture rise grain are harvest then it is ricks of loss from module nutrition insects. It is done by using sickle.

Sickle is it tools with sharpest metal which is attached to wooden handle. Harvesting is also done by the Machines or Technology.

Polluted water is the big concern to the living organisms and aquatic animal and climate change and it is also this disturb whole economic system.

II. SURVEY OF EXISTING METHODS

Fig. 1 depicts the Crop Classification.

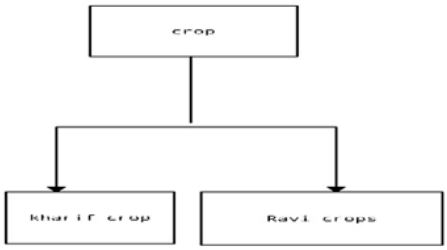


Fig.1 Crop Classification

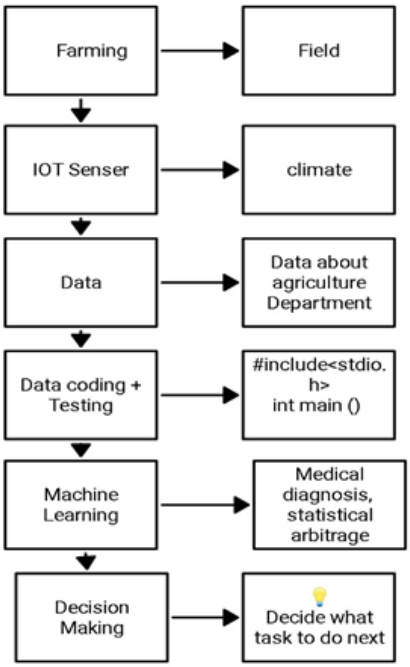


Fig 2: Block Diagram of Existing Farming Ecosystem

Fig. 2 depicts Existing Farming Ecosystem and how transofrmation can play an important role.4

Figure 3 explores Smart Farming Mechanism proposed by many researchers.

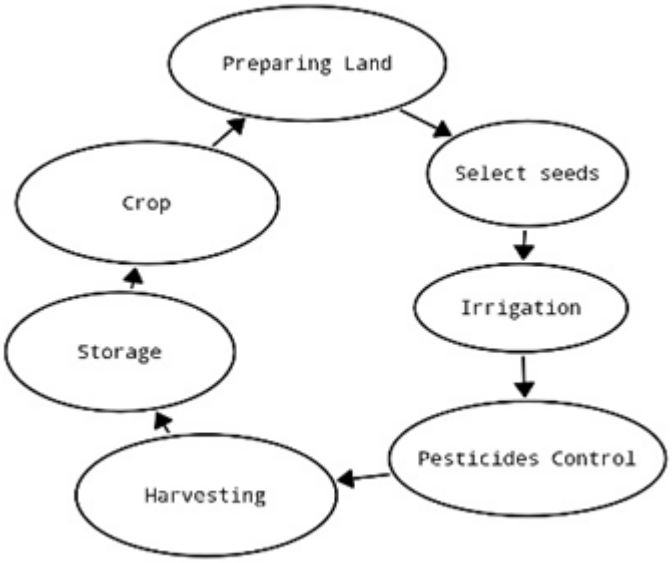


Fig 3 : Smart Farming Mechanism

K.M. Devi et.al. [1] presented the steps to be undertaken to strengthen the Computer and Information technology education in rural India. R. Chaudhary et. al. [2] explores the use of IoT in area of agriculture. The case study provided insights into how IoT can play a vital role in Agriculture Sector.

H.P. Thakor et. al. [3] analyzed and proposed a robust Smart Farming solution which can be utilized to increase the produce.

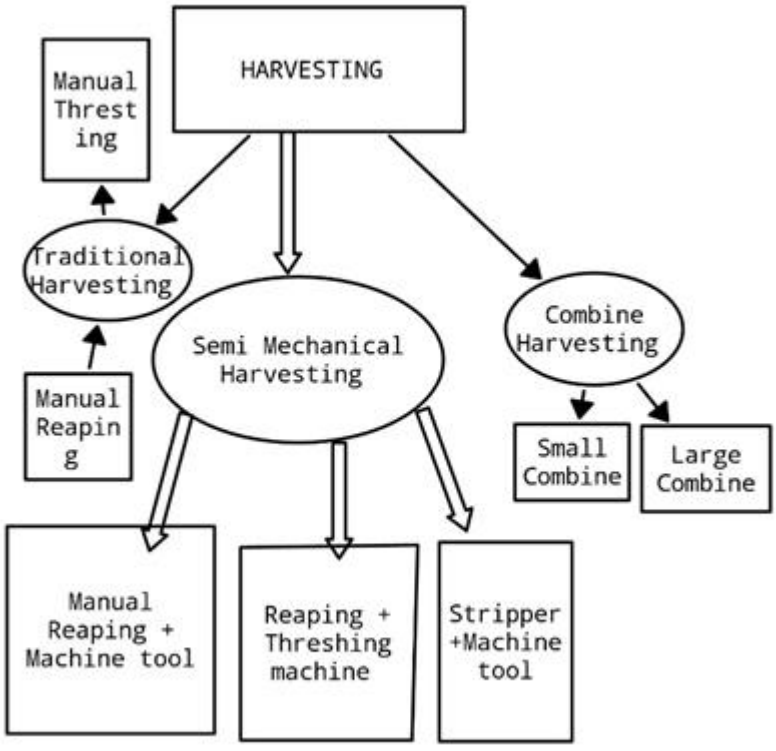


Fig. 4. Harvesting Mechanism

Fig. 4 show harvesting stage and how harvesting can be classified into pre harvesting, harvesting and post harvesting. Yaganteeswarudu et. al. [4[analyzed and develop a mobile application which can be used to detect and prevent suicide cases among Farmers. The existing conditions were not conducive for the farmer to lead a respectable and satisfied life.

C.M. Dwarkani et. al. [5] have proposed a Smart Farming Solution using various sensors like Soil Testing, Leaf and other plant disease sensing sensors. The data and implementation method provides better results than the previous ones. M.S. Mekala et. al. [6] have surveyed various research papers in the field of Smart Farming using IoT and cloud computing. The major implementation challenge for these survey papers was insufficient data and lack of tool uniformity to check results.

C. Yoon et.al [7] have implemented practices of Smart Farming with technological advancements like IoT. The results are found to be at par with Farming global industry standards.

S. Heble et. al. [8] have compared and suggested a cost-effective solution using Internet of things for smart farming. The comparison criteria is at par with Industry standards. S. jaiganesh et.al. [9] have used IoT to incease the productivity of farming community.

M. Lee et. al. [10] have proposed and discussed at large IoT based Smart farming options. This paper provides a comparative analysis of various methods deployed. J. Sheney et. al .[11] study the various IoT and allied technology in Agriculture. S.S. Iyer et. al. [12] have explored and discussed various security mechanism in the era of Smart farming. Ethical secure data management and practices with proper cyber setup should be installed [13] .

III. COMPARATIVE RESULTS

Criteria

Method	Efficiency	Power weight	Cost effective	Products quality
[1]K.M. Devi,M.Krishna, And V.Murlidharan	No	Yes	Yes	Average
[2]H.P.Thaor and S.Iyer	Yes	Average	No	Good
[3]C.Yoon,M.Huh, S.Kang,J.park,and C.lee	Yes	Yes	Average	Good
[4]S.Heble,A.kumar, K.V.V.D.Prasad,S.samirana, P.Rajalakshmi,and U.B.Desai	No	Average	Yes	Yes

IV. CONCLUSION

Farmer had been largely at the mercy of nature, commission agents, loan sharks and big corporate entities. This paper compared Traditional and Modern or Smart Farming mechanisms using advanced Technology. This paper also discusses an farming ecosystem as suggested in various methods. Various Protocols and knowledge orientation towards technology in villages need to be developed and deployed. Future Work involves designing and deploying an effective Smart farming mechanism which is viable and can reduce manual labour to a certain extent leading to complete automation of the farming operations.

V. REFERENCES

[1]. K. M. Devi, M. Krishna, and V. Muralidharan, “Empowering IT education in rural India,” in Proc. of the 12th IEEE International Conference on Information Technology Based Higher Education and Training (ITHET), October, 2013, pp. 1-4.

[2]. R. Chaudhary, J. R. Pandey, P. Pandey, and P. Chaudhary, “Case study of Internet of Things in area of Agriculture, ‘AGCO's Fuse Technology's’, ‘Connected Farm Services’,” in Proc. of the IEEE International Conference on Green Computing and Internet of Things (ICGCIoT), Octiber, 2015, pp. 148-153.

[3]. H. P. Thakor and S. Iyer, "Development and Analysis of Smart Digi-farming Robust Model for Production Optimization in Agriculture," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 461-465.

[4]. A. Yaganteeswarudu and Y. V. Vardhan, “Software application to prevent suicides of farmers with ASP. NET MVC,” in Proc. of the 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence, January, 2017, pp. 543-546.

[5]. C. M. Dwarkani, G. R. Ram, S. Jagannathan, and R. Priyatharshini, “Smart farming system using sensors for agricultural task automation,” in Proc. of the IEEE Technological Innovation in ICT for Agriculture and Rural Development (TIAR), Chennai, Inida, 2015, pp. 49-53.

[6]. M. S. Mekala and P. Viswanathan, “A Survey: Smart agriculture IoT with cloud computing,” in Proc. of the International conference on Microelectronic Devices, Circuits, and Systems (ICMDCS), Vellore, India, 2017, pp. 1-7.

[7]. C. Yoon, M. Huh, S. Kang, J. Park, and C. Lee, “Implement smart farm with IoT technology,” in Proc. of the 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-is Gangwon-do, Korea (South), 2018, pp. 749-752

[8]. S. Heble, A. Kumar, K. V. V. D. Prasad, S. Samirana, P. Rajalakshmi, and U. B. Desai, “A low power IoT network for smart agriculture,” in Proc. of the IEEE 4th World Forum on the Internet of Things (WF-IoT), Singapore, 2018, pp. 609-614.

[9]. S. Jaiganesh, K. Gunaseelan, and V. Ellappan, “IOT agriculture to improve food and farming technology,” in Proc. of the Conference on Emerging Devices and Smart Systems (ICEDSS), Tiruchengode, 2017, pp. 260-266.

[10].M. Lee, J. Hwang, and H. Yoe, “Agricultural Production System Based on IoT,” in Proc. of the IEEE 16th International Conference on Computational Science and Engineering, Sydney, 2013, pp. 833-837.

[11].J. Shenoy and Y. Pingle, “IOT in agriculture,” in Proc. of the 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 1456-1458

[12].S.S. Iyer, K.I. Kamaljit, Practical evaluation and comparative study of text steganography algorithms. Int. J. Innov. Res. Comput. Commun. Eng. 5(3), 74–77 (2016). ISSN (Online) 2278-1021 ISSN (Print) 2319-5940

[13].S.S. Iyer, K.I. Kamaljit, Practical evaluation and comparative study of big data analytical tools, in Int. J. Innov. Res. Comput. Commun. Eng. 5(2), 57–64 (2017). ISSN (Online): 2320-9801 ISSN (Print): 2320-9798

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

IoT Based Quarantined Isolation Ward System Design for Covid-19 Patients

Valerie D'souza, Vidhi Biltheria, Dr. Rajeshree Khande
Department of Computer Science, MIT WPU, Pune, Maharashtra, India

ABSTRACT

The IoT (Internet of things) has huge scope in modern day society, it has not only helped in increasing a better functionality but has also reduced manual labor. It is cost effective and produces effective, precise, and quality results. It has improved work safety conditions and time management. Advancement in machine learning and Artificial intelligence (AI) and its implementation in the healthcare sector through wearable sensory devices can help to remotely monitor patients. In this research paper an IoT system is designed to help monitor the Covid-19 patients who are in a hospital isolation ward. With the help of IoT it is possible to build a system where IoT based sensor devices, along with AI can be linked to a database of patients. It can be used to monitor heart rate, temperature, oxygen level and blood saturation along with diet pattern of patients in an isolation ward, and alert medical staff if a sudden change is observed. This way necessary actions can be taken accordingly and it reduces the risk of medical staff contracting the virus as exposure would be limited.

Keywords—: IoT, Covid19, Healthcare, AI, Machine Learning

I. INTRODUCTION

Healthcare systems around the world have seen a drastic change in infrastructure due to the ongoing Covid-19 pandemic. Increase for isolated intensive care has gained importance due to the nature of the Coronavirus. This pandemic was caused by the SARS CoV-2 Coronavirus. Coronaviruses are a group of RNA viruses making them highly prone to mutation [1]. In humans SARS CoV-2 causes respiratory tract infections which could end up being lethal. Covid-19 symptoms range from undetectable to deadly. It is more likely to severely effect elderly patients and those with certain underlying medical conditions.[2]. In some cases, the outcome of the effect of the virus on people differs. The virus enters the human body through the airway and infects cells along it by attaching itself to the angiotensin-converting enzyme 2 (ACE2) receptor which is physiologically important in protecting the lungs from injury. After entering the cells through ACE2 the virus multiplies. This triggers an inflammatory response from the immune system causing the lungs to scar and stiffen or causes fluid to fill in them, thus blocking the passage of oxygen to the bloodstream via lungs.[15] According to the most recent report by WHO during the week of 24 to 30 January 2022, the number of new Covid-19 cases remained similar to that reported during the previous week, while the number of new deaths increased by 9%. Across the six WHO regions, over 22 million

new cases and over 59 000 new deaths were reported. As of 30 January 2022, over 370 million confirmed cases and over 5.6 million deaths have been reported globally. [3].

Since SARS CoV-2 is airborne it spreads When-

a) An infected person coughs, sneezes or talks, the droplets or tiny particles called aerosols carrying the virus spreads out into the air through their nose or mouth and anyone within a 6 feet radius can risk getting infected by breathing the virus in.
b) As the virus is seen to survive 3 hours without a host, airborne transmission by someone passing by and breathing in the air is highly possible.
c) Surface transmission is when the virus can be transmitted through a surface medium on which it was probably settled upon to another person.
d) Another least likely scenario is fecal-oral infection which happens when the infected person uses the bathroom and doesn't wash their hands, they could infect things and people that they touch.[4]

It has raised concern for betterment of healthcare in a quarantined environment concerning pandemics and possibilities of future outbreaks. This pandemic has resulted in job losses in all sectors of the industry. Visiting a hospital or local clinic for a diagnosis or for any other medical condition increased the risk of contracting the virus through possible pre-exposure of the attending medical staff and other patients. The Internet of Things (IoT) is a concept that aims to broaden the capabilities of the internet network. The functions and benefits of internet networks, such as data sharing, remote control, and so on, can connect objects in the real world, allowing them to communicate with one another. Remote control features are provided by IoT technology. Bluetooth, Wi-Fi, or the internet can be used for the control network. IoT has helped redefine healthcare, it has made the remote contact between a patient and doctor possible. IoT technologies have helped create systems which are cost effective as well as time saving. With the help of IoT it is possible to create a system that helps improve healthcare services for these pandemic and possible future ones. IoT devices can be used to monitor a patient's heart rate, body temperature, SpO_2 etc. The newly termed IoMT (Internet of Medical things) is predicted to have an estimate value of $176 billion by 2026[6]. The most popular form of IoMT is remote patient monitoring. Other uses are tracking location and availability of medical equipment, tracking staff and bed availability along with inventory and even reducing emergency room wait-times. Mt Sinai hospital in New York city, partnered with GE healthcare to create an IoT-driven software, known as AutoBed, that tracks occupancy among 1,200 units and factors in 15 different metrics to assess the needs of individual patients. This effectively slashed wait times for 50% of their emergency room patients who are in need of inpatient care.[7] Covid19 patients are highly advised to stay in quarantine at home, however in severe cases when patients need more medical attention and need to visit a hospital, risks of cross infection arise by the above-mentioned scenarios. This could infect other hospital patients, suffering from other underlying conditions. Hospitals do have isolation wards, however there is still the risk of the hospital staff contracting the virus through constant exposure by attending to patients. With the help of an IoT system we could limit the number of attending staff required with the help of AI and create conditions where the patients' vitals can be monitored accurately from a remote distance.

II. RELATED WORK AND MOTIVATION.

The current pandemic crisis has changed the livelihoods of people across the world and has brought issues like global poverty into focus. It has vastly disrupted economies and is known as the Covid-19 recession. On the other

hand, it has also led to innovations in different sectors. Many companies have taken into consideration the need for digitization of their platforms. The need for IoT devices and IoT systems have seen a huge spike. Currently, hospitals have designed their isolation wards in the best way possible, to avoid cross-infection. The isolation ward is a designated building which is at a distance from the main building and only specific attending staff are assigned, with ventilation being the key component to an isolation ward to prevent spreading of infectious airborne spores. An IoT based isolation ward on the other hand can help lessen the risk of the attending staff and provide more affective healthcare.

2.1. Wearable monitoring devices

The first wireless smart watch was released in 1994 and was developed in partnership with Microsoft. The watch is linked to a reading light emitting from a computer through an optical sensor that is embedded in the watch, to download information, display and work on.[17] There has been an increase in the use of smart wearable devices that track different body functions, like blood pressure, temperature, SpO_2, step count per day, and many more.[8] These smart wearables can help to better monitor a covid patient in an isolation ward. To reduce human contact, these devices can track the necessary vitals of the patients and send it to the database and can be relayed further. The GOQii Smart Vital is one of the devices designed to measure your vitals. [8]

The GOQii watch image from GOQii Blog

2.2. AI powered chatbots

Artificial Intelligence or Augmented Intelligence helps perform tasks with the available data by using algorithms. With the help of AI, the number of rigorous tasks that humans need to do is reduced. A common misconception based on Modern fiction about AI is that it would take away jobs and replace humans, however, a more realistic definition of AI is that it makes human jobs easier by doing all the tasks faster and more effectively. AI primarily performs tasks according to the way they are programmed. According to a study by PDC 16 trillion dollars of GDP will be added between now and 2030 and it would vastly change economies across the world. AI algorithms exist so that we can interact with AI such as Alexa, SIRI etc. AI powered conversational bots also known as Chatterbots/Chatbots are software application used to conduct online conversations with customers/patients.

They are designed to convincingly stimulate the way a human would behave as a conversation partner [9]. Some early examples of chatbots are A.L.I.C.E(Artificial Linguistic Internet Computer Entity) which is a chatbot that uses natural language processing and engages in conversation with humans using heuristic pattern matching rules to match a human's input.[10] Nowadays multiple applications use chatbots to better their customer service. Applications like Practo use chatbots to assess the initial symptoms of a user and then provide the services for online consultation with doctors along with pharmaceutical and testing services.

2.3. Machine Learning

Machine learning is a branch of AI in which a system uses algorithms to analyze large amounts of data and make predictions and come up with patterns. A popular example of machine learning are facial recognition systems, in which supervised learning is implemented by using algorithms to train the machine to analyze and categorize data by providing it with multiple samples. Google photos uses this to help recognize people, places, and things in your gallery of photos and creates albums for them, you can then name the albums, and search for photos based on what you require instead of scrolling through the entire photo gallery. A well-documented example of machine learning application in healthcare is the early prediction of Alzheimer's disease in which speech pattern like intervals between words, speech-pattern, pronunciation, frequency and amplitude of sound are analyzed.[13]. Machine learning could be used to predict heart failure by taking an input of a person's age, sex, BMI, average BPM, which could help doctors come up with precautionary solutions.

2.4. Semi- autonomous robots

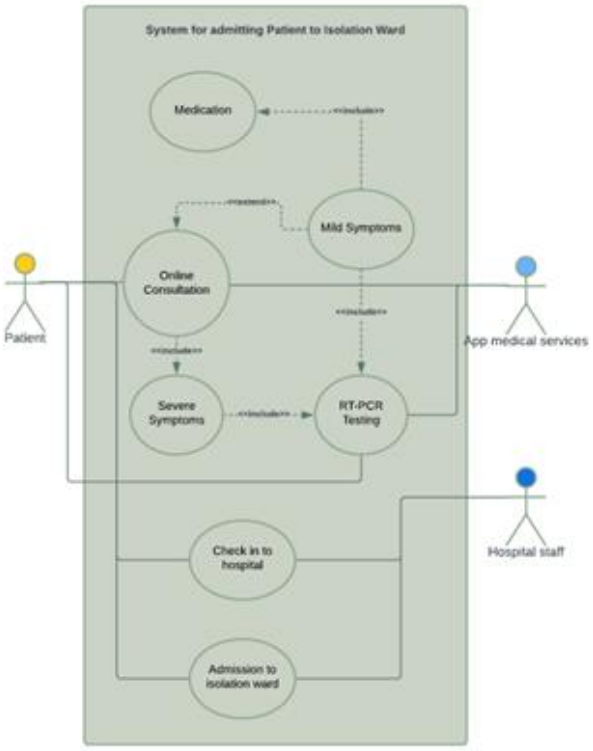
Robots, particularly service robots have aided humans in performing laborious, risky, or repetitive tasks. They can be autonomous or semi-autonomous. Semi-autonomous robots facilitate humans by expanding human capabilities and can be remotely controlled by them. Service robots can be manually operated from remote distances to perform tasks like lifting heavy loads from ship cargo, performing disinfection in clustered environments as well as aid in search and rescue missions. Service robots can be seen as an extension of humans and are used by employees to perform tasks that they themselves cannot physically do. Orihime-D is a semi-autonomous avatar robot with a height of 120 cm and a built-in camera, microphone and speaker. It can be remotely controlled via internet. It can be used to convey various and greetings the original idea of this robot was developed by Kentaro Yoshifuji in 2010 as technology which allowed one to connect with family and friends whilst being away from them. It can perform tasks like carrying objects while being remotely controlled. Orihime-D has been seen to be in use in Dawn-Avatar robot cafe. This was so people with ALS (Amyotrophic Lateral sclerosis) could still have an opportunity at life by remotely controlling the Robots through a tablet application from the hospital.[11] Semi-autonomous robots increase job opportunities for those who are unable to physically go to workplaces.

Orihime-D image from roboticgizmos.com

III. IOT SYSTEM FOR ISOLATION WARD

3.1 Use case

With the help of chatbots it is possible to determine the primary symptoms of a disease based on the patient's input. The patient can then be recommended to a doctor for consultation. Based on the doctor's advice, the patient is given medication and is asked to do the RT-PCR (Real time polymerase chain reaction) test which is used to determine if one has contracted Covid-19. If they test positive for infection, they are advised to home quarantine. If the symptoms get too severe, they are recommended to admit themselves in a hospital, where they are allocated to the Isolation Ward. The below diagram shows the process for this system.



Use case diagram for admission of symptomatic patients to hospital

3.2 Diagnosis

The incubation period of corona virus is 14 days from exposure and common symptoms for corona virus are fever, cough, loss of smell and taste, tiredness and sore throat. Anyone experiencing these symptoms can remotely consult with a doctor without having to physically go to a clinic but by using a mobile application. A patient can search for doctors based on their symptoms and location and consult with doctors online, who could administer the treatment and suggest the required tests. Some applications offer testing services where the services of home collection of the patient's samples are provided. The RT-PCR (Real time polymerase chain reaction) requires nasopharyngeal swabs which can help determine if a patient has contracted the corona virus. The severity of the symptoms can be classified as-

A) Mild to moderate (limited to mild pneumonia)
B) Severe (dyspnea, hypoxia, or more than 50% lung involvement on imaging)
C) Critical (respiratory failure, shock, or multiorgan system dysfunction) [14]

If the patients' symptoms are mild, they are advised to be quarantined at a room at home and take the necessary treatment. However, in cases where the patient is experiencing severe symptoms, they are in need of greater medical attention. Hospitals need to keep and treat such patients in an isolation ward for fear of them or other patients contracting this airborne virus.

3.3 Admission to hospital

When a patient diagnosed with Covid-19 is admitted to hospital, they are taken directly to the hospital's designated isolation ward for treatment. Isolation wards are designed so that the rooms are ventilated and the airflow of the wards are controlled so that the airborne infectious particles don't spread. In India, to ensure disinfection the isolation wards do not have non-essential furniture and access to the ward is limited to dedicated staircase or elevator. They are equipped with double door entry rooms, changing station and nursing station.[16] However, even after taking these precautions, there are still chances of infection to the attending medical staff as they need to constantly monitor the patient's vitals.

Using wearable IoT devices, patient's vitals can be monitored constantly, from a distance. Machine learning technology helps analyze data and make predictions by using the data of the patient like age, sex, blood type, any other underlying conditions etc. along with the incoming data provided by the monitoring devices. These datasets can be compiled and collated in a database of patients, where machine learning can be used to analyze this data and make predictions for the recovery or worsening of a patient's state.

Dietary lapses and diet patterns can be predicted based on factors like body temperature, SpO_2 and Blood pressure, and taking the patient's age and medical history into consideration along with the medicines administered to them. Patients are primarily administered IV drip however based on their mobility and vitals they can slowly start ingesting food themselves. Instead of nurses having to go into the rooms, semi-automated robots with fitted cameras, microphone and speaker can be used to provide food to patients. These robots are remotely operated by nurses through a device like a tablet and can also tend to the patients. Through the fitted camera a nurse can view the patient and operate the robot in a manner that gives an impression of physical presence of the in the room.

Each room can be provided with their own semi-automated robot and designated staff. This way the robot can help deliver basic necessities like food, a change of clothes, bedsheets etc. However, in cases where a patient needs to be administered an injection or needs more intensive care, a nurse can enter a room, after following the

precautionary measures. This system would prove more efficient as it would enable constant monitoring of the patient along with instant service. Moreover, the contact between the medical staff and patient would be limited to administering injections.

IV. DISCUSSION

This IoT framework has not been put to pragmatic use due the current Covid-19 pandemic, thus the aftereffects of this exploration are obscure. Be that as it may, the aftereffects of this examination could assist with fostering a framework for this pandemic as well as would prompt progression in medical services in anticipation of a potential future emergency. This framework has impediments as clinical treatment with these gadgets can't be ensured to have total exactness, mistakes can occur whenever. As far as every patient's clinical history, AI administrations wouldn't be as particular and customized as those given by a human attendant. Innovation for Semi-independent robots to perform more steady activities like administering injections and so on haven't grown to this point. Later on, innovation might foster where all emergency clinic affirmation and clinical consideration could utilize an IoT framework or IoT based gadgets to make treatment more compelling. IoT ventilators have effectively begun to become an integral factor. Hospitals would see a gigantic difference in framework with the total implementation of IoT frameworks and gadgets and would be prepared all of the time for crisis circumstances like the ongoing one.

V. FUTURE WORK

We have entered a new phase of our lives with the current pandemic situation and with the rise of Covid-19. This virus has caused damage to economies across the world and given rise to unemployment. The market, jobs, industries, the general way of life has changed to a much more cautious approach. With the damage, also comes the advancement in the medical approach to the virus. Through medical research by experts, vaccines were developed and administered, and booster doses were administered to certain age groups who had taken the initial required dosage. The research is ongoing and there is yet to be more development for the current crisis and different solutions for all situations.

Many more handsfree technologies may be developed for use in medical fields, and IoT as well along with machine learning is likely to become an integral part of this development. These advanced technologies may provide simpler and more convenient ways to cope with the ongoing virus recovery. More robots and other IoT based devices will come into play with features for touchless contact for different tasks with a view to stay safe. For the day-to-day tasks of the general population, new technology, software, and machinery have been developed which will make working easier at home to reduce physical contact with the outside world. Depending on the seriousness of the future variants, the medical development and machine advancement will evolve to cope with it. Machine learning can be developed to make advanced medical machinery, for example, devices that could detect abnormalities from a scan itself.

Safety measures will play a major role in the imminent years, as technology develops, means of safety and quarantine will also advance. For transport, self-driving cars will come into play to make it more efficient and faster.

Hospitals can have their own personalized apps that can be used for various purposes like enquiries, online consultation, or to book appointments. The app can also be used to display the patient's information and recovery process to their family, or to anyone who is their guardian. Family or selected individuals can have access to the patient's information and could access it through the app. Payments and pharmaceutical delivery can also be based online, so that there is minimal physical contact between humans.

VI. CONCLUSION

A hypothetical IoT system for admitting and monitoring patients infected with the SARS CoV-2 Coronavirus is proposed in this paper. A hospital can use this system to monitor patients remotely and effectively. This system not only provides near-perfect disease containment in an isolation ward, but it also does so without affecting the medical staff caring for the infected patients. With the ongoing virus, its mutations, and the potential for new viruses, IoT-based systems have become more important. In this system AI, and Machine Learning have been implemented to assist the attending medical staff in performing routine tasks. Each of these plays an important role in the system. Smart technology does not fully control this system; rather, it aids the human workforce in completing their tasks. The functionality of this system, as well as its results, are unknown because this paper is based on a hypothesis and has not been put to practical use.

VII. REFERENCES

[1]. Ted-Ed Lesson by Elizabeth Cox directed by Anton Bogaty https://youtu.be/D9tTi-CDjDU
[2]. Coronavirus Wikipedia https://en.wikipedia.org/wiki/COVID-19_pandemic
[3]. World Health Organization (WHO) https://www.who.int/publications/m/item/weekly-epidemiological-update-on-covid-19---1-february-2022
[4]. WebMD website https://www.webmd.com/lung/coronavirus-transmission-overview#1
[5]. Ordr website https://ordr.net/article/IoT-healthcare-examples/
[6]. Exciting IoT applications in Healthcare by Kayla Matthews https://www.iotforall.com/exciting-iot-use-cases-in-healthcare
[7]. A Brief History of Wearable Technology by Nick Thilen https://www.modjoul.com/blog/a-brief-history-of-wearable-technology#:~:text=The%20first%20wireless%20smart%20watch,as%20appointments%20and%20other%20reminders.
[8]. GOQii image from GOQii blog September 4, 2020 https://goqii.com/blog/tag/blood-pressure-monitor/
[9]. Chatbot Wikipedia https://en.wikipedia.org/wiki/Chatbot
[10]. A.L.I.C.E Wikipedia https://en.wikipedia.org/wiki/Artificial_Linguistic_Internet_Computer_Entity
[11]. Using OriHime robot for diverse workstyles and closer relationships by Tomoyo Matsuda https://zenbird.media/using-orihime-robot-for-diverse-workstyles-and-closer-relationships/
[12]. Orihime image https://www.roboticgizmos.com/orihime-d-robot-waiters/
[13]. Machine learning applied to medical by Ronald Hernández https://www.encora.com/insights/machine-learning-applied-to-medical-diagnosis#:~:text=Another%20well-documented%20healthcare%20example,of%20patients%20with%20this%20disease.

[14]. Centers for disease control and prevention https://www.cdc.gov/coronavirus/2019-ncov/hcp/clinical-guidance-management-patients.html
[15]. Role Of Angiotensin-converting enzyme (ACE2) in Covid-19 by Wentao Ni, Xiuwen Yang, Deqing Yang, Jing Bao, Ran Li, Yongjiu Xiao, Chang Hou, Haibin Wang, Jie Liu, Donghong Yang, Yu Xu, Zhaolong Cao & Zhancheng Gao https://ccforum.biomedcentral.com/articles/10.1186/s13054-020-03120-0
[16]. The National Centre for Disease Control is an institute under the Indian Directorate General of Health Services, Ministry of Health and Family Welfare. https://ncdc.gov.in/WriteReadData/l892s/42417646181584529159.pdf
[17]. Wearable Sensors for Detecting and Measuring Kinetic Characteristics by Zihao Huang, Junan Li and Jiakun Lian https://iopscience.iop.org/article/10.1088/1742-6596/2174/1/012007

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

A Comprehensive Study of Blockchain Technology in Healthcare

Shivam Kumar Pandey, Suman Maity
Faculty of Information Technology, ICFAI University, Ranchi, Jharkhand, India

ABSTRACT
Blockchain innovation has filled in fame throughout the last ten years, drawing in interest from a wide scope of ventures like money, government, energy, and wellbeing. This is an article which gives a comprehensive explanation of how is blockchain being used in the clinical benefits business. In all actuality, continuous exploration in this field is advancing rapidly. Subsequently, we've distinguished different best in class use cases for innovation in blockchain, for example, electronic clinical information sharing, distant persistent observing, and the medication store network, to make reference to not many. We likewise checked out the impediments of the approaches we took a gander at, and we discussed some open examination questions and potential exploration bearings.

KEYWORDS: BLOCKCHAIN • HEALTHCARE • REVIEW

I. INTRODUCTION

Blockchain has quickly become one of the most encouraging advances in the new ten years, drawing in the consideration of different scholarly examinations and industry. In a white paper published in 2008, Satoshi Nakamoto presented this notion. It's a decentralised, appropriated, and distributed system unchanging record that is utilized to safely record exchanges across various PCs in a shared organization without the utilization of outsider assets.

Blockchain 1.0, the principal variant of blockchain, depends on Bitcoin, the first blockchain execution in view of cryptographic money applications. The possibility of splendid arrangement has progressed later on, known as Block chain 2.0, and is portrayed as a code snippet that is described, carried out, completed, and it was noted in the scattered record. Blockchain 3.0, the third era of blockchain innovation, is generally utilized in non-monetary applications like government, energy, and medical services. Actually, some medical care associations have acknowledged this innovation and put it to use in an assortment of situations. The most captivating blockchain properties that are gainful to medical services

[1] Other blockchain 1.0 innovations, as Dash, Litecoin, and others, have showed up.

Applications incorporate decentralization, protection, and security, since blockchain innovation can give secure admittance to clinical information for patients and different partners (insurance agencies, medical clinics, specialists, and so on)

We give the most applicable blockchain-related investigations in the medical services area in this review. Electronic clinical records, distant patient observing, drug inventory network, and health care coverage claims are only a couple of the utilization cases that have been examined. This examination likewise views at the relevance of these arrangements as well as their innovative limitations. Likewise, a few examination bearings and examples learned are distinguished.

"The remainder of this paper is as follows. Section 2 deals into the fundamentals of blockchain technology. Section 3 discusses several medicinal applications of this promising technology in healthcare. We'll sum up the important findings at the end of this section. Section 4 discusses research problems and opportunities. Finally, Section 5 brings the paper to a close and makes recommendations for further research".

II. KEY CONCEPT ON BLOCKCHAIN

We'll go over the basics of blockchain innovation in this part to assist you with getting a handle on the remainder of the article.

Outline and Architecture of Blockchain

In its most focal plan, blockchain is a typical affiliation that startling spikes pursued for top of the web and was first proposed in 2008 as a piece of a Bitcoin idea. The blockchain is a straightforwardly accessible report included a movement of squares that contains a complete record of all trades that have happened on the association. A header and a body make up most of a square. The past square's hash is put away in the header of each square. Therefore, the squares make a connected rundown or chain, with each square construction expanding on the first one.

The block header looks for timestamps that indicate when the square was sent, nonces, unpredictable numbers that the excavator periodically changes to get a specific "hash value to solve a maths puzzle, and also transactions". It also remembers the Merkle tree, which shows the work required to do this. Within a very basic level square.

A Blockchain exchange is a little unit of work that is recorded openly hinders. A vast portion of the framework's clients double-check each trade. When transactions are recorded on the blockchain, they are guaranteed to be sealed. As far as blockchain changelessness, every member imitates, has, and keeps a solitary duplicate of the record.

The business rationale is written using shrewd agreements, which are self-executing code on the blockchain system that consider straight-through processing, regardless of the blockchain type.

When shrewd agreements are incorporated in the blockchain, they become forever sealed because no one can modify what has been changed, self-confirming because of automated capacities, and self-implementing since the principles are followed at all phases.

Decentralization by making records accessible to all individuals, constancy by making the blockchain framework almost difficult to change and limit, admittance to all timestamped trade records by furnishing each friend with a duplicate of the blockchain, and lack of definition by allowing each client to interact and permitting every client to interface with the blockchain utilizing a made location that conceals the client's actual personality are only a couple of the critical components of Blockchain. [1]

Taxonomy of Blockchain Systems

Public, private, consortium, and hybrid blockchains are the four types of blockchain systems now in use.

Public blockchains "(like Bitcoin and Ethereum) allow for a completely decentralised network in which every member may examine the blockchain content and participate in the consensus process". [1]

Private blockchains "are used to track data transactions between different departments or persons and are dedicated to single enterprise solutions. To join the network, each participant must first give their approval, after which they will be deemed a known member". [1]

Consortium blockchain "is a authorized network that is exclusively accessible to a certain set of people. It is utilised as a distributed database that is auditable and reliably synced and keeps track of participant data exchanges". [1]

Hybrid blockchains "includes the advantages of both public and private blockchains. As a result, a public blockchain is used to make the ledger completely visible, while a private blockchain operates in the background to manage access to the ledger's modifications". [1]

III. BLOCKCHAIN USE CASES IN HEALTHCARE

"One of the industries where blockchain is regarded to have a lot of potential is health care. Recognizing the relevance and usefulness of this technology", "the Office of the National Medical Information Technology Coordinator (ONC)" launched a white paper idea contest on the potential use of blockchain in medical care in 2016. As a result of this difficulty, a few blockchain-based healthcare applications have been presented.

We'll look at the most important research in this part, which are organised by use cases including electronic clinical records, far off tolerant observing, drug store network, and medical coverage claims.

Medical Records on the Internet

The executives, who could benefit from the ability to coordinate various frameworks and work on the precision of Electronic Health Records, should be the focus of medical care reform (EHRs). While the terms electronic clinical records (EMRs) and electronic health records (EHRs) are sometimes used interchangeably, there is a distinction to be made. The expression "electronic clinical records" (EMR) was authored first, and it alludes to an advanced variant of a clinician's paper archives. The clinical and treatment chronicles of patients in a single practice are put away in an EMR. EHRs, then again, are worried about a patient's general wellbeing, going past the fundamental clinical information gathered in the specialist's office to incorporate "a more extensive perspective on the patient's therapy". [2]

As per the arranging study, blockchain innovation helps with the administration of electronic wellbeing records. Ekblaw et al. (Ekblaw, 2016) describe MedRec as an "EHR-related implementation that presents a decentralised strategy to handling authorization, approvals, and data sharing" across clinical benefits partners. MedRec utilizes the Ethereum stage to furnish patients with information and data concerning who approaches their clinical records. [1]

"FHIRChain (Fast Health Interoperability Records + Blockchain) [3] is a second application that unites EHR. It's an Ethereum-based blockchain-based clinical data sharing tool that shines a light on clinical benefits record association. For patients, FHIRChain provides ONC-acceptable responses".

In essence, Xia et al. offer Medshare, an Ethereum application for structures that deal with a lack of shared effort for data splitting between cloud firms due to the risks of disclosing confidential data content. For trading clinical information in cloud storehouses, Medshare gives information provenance, reviewing, and control between enormous information substances.

MedBlock and Block-HIE are two more blockchain-based EMR configurations. MedBlock comes with a record search function. “The proposed framework, which is managed by a medical professional or office, keeps track of the addresses of squares containing a patient's records. Every enduring stock has a link to the blockchain record that it corresponds to”. BlocHIE [4] is a blockchain-based medical services stage suggested by Jiang et al. BlocHIE combines off-chain storage, where data is stored in exterior clinic records, with on tie validation, which ensures that up-to-date records are used. The blockchain framework stores hash values for external records. To improve fairness and throughput, the designer proposes two replacement press calculations based on fairness, FAIR FIRST and TP & FAIR. Ancile [5], a medical care blockchain-based structure, impacts Ethereum-savvy agreements to provide data security, executive access, and EMR interoperability.

Roehrs et al. [6] describe omniPHR, a distributed architecture for maintaining a solitary, interoperable perspective on Personal Health Records (PHR). The proposed arrangement is built on a flexible, interoperable, and extensible PHR information framework. Furthermore, omniPHR assessment could guarantee PHR information block division and dispersal in a steering overlay organization. [1]

Remote Patient Monitoring

“PDAs, body district sensors, and IoT (Internet of Things) devices are used to accumulate clinical data” to remotely screen a patient's condition. Blockchain considers the capacity, sharing, and recovery of biomedical information gathered from a distance.

Ichikawa et al. [7] describe a system that uses mobile devices to send data to a Hyper-Ledger Fabric-based blockchain-based application.

By giving continuous patient observing applications, Griggs et al. show how

Ethereum savvy agreements can permit mechanized mediations in a protected setting. Different procedures propose that the Internet of Things (IoTenormous) has immense guarantee in an assortment of fields, including e-wellbeing, where it is right now being broadly taken advantage of and utilized. As indicated by Ray et al. [8], IoBHealth is an information stream engineering that mixes IoT and blockchain and might be utilized to access, store, and oversee e-wellbeing information [1]

Pharmaceutical Supply Chain

One more utilization of blockchain that has been recognized is in the drug business. Patients might endure genuine fallouts assuming they get fake or insufficient medications. Blockchain innovation has been distinguished as a possible answer for this issue.

A startupBocek et al. present Modum.io AG, utilizes blockchain to make data permanent. This company makes temperature data of drug items during transportation available to the public in order to ensure that they are in compliance with quality control temperature regulations. In light of blockchain innovation, he also tended to falsify prescriptions, advocating a secured, irreversible, and traceable medicine production network to avoid forging.

Jamil et al. [9] addressed medication consistency troubles when it came to sedate regulations. The creators have underlined the difficulties of recognizing fake drugs and introduced a blockchain-based way to deal with distinguish them. While a couple of studies portray a functioning execution of the proposed framework, a few captivating audits on drug production network difficulties [10] [11] merit perusing. [1]

Health Insurance Claims

Medical care claims are one of the therapeutic benefit areas where blockchain's eternal nature, simplicity, and auditability of data kept on it can be beneficial.

While medical services protection guarantee handling is a fundamental region where blockchain has potential, there are different regions where blockchain has potential. Model executions of such frameworks, then again, are very restricted. MIStore is a blockchain-based clinical protection arrangement that gives scrambled and permanently put away clinical protection information to the clinical protection market. [1]

Table 1. Significant contributions classified by use cases

Use cases	Paper	Structure	Storage of Data	Contribution	Year
Electronic medical records	(Ekblaw, 2016)	Ethereum	Off-chain	Provides a patient-centered system that makes medical history transparent and accessible.	2016
	(Xia, 2017)	Ethereum	Off-chain	Create a stage in cloud storehouses for shared healthcare data.	2017
	(Roehrs, 2017)	Specific	Off-chain	A circulated PHR model that proposes dormancy arrangements.	2017
	(25. Zhang, 2018)	Ethereum	Hybrid	Proposes an ONC-compliant blockchain-based EMR solution.	2018
	(Fan, 2018)	Proprietary	Off-chain	A blockchain based EMR management solution is provided	2018
	(Jiang, 2018)	Proprietary	Off-chain	A healthcare system that integrates off-chain storage and on-chain verification	2018
	(Dagher, 2018)	Ethereum	Hybrid	Proposes a system of electronic health records that protects personal health data.	2018
Remote patient monitoring	(Ichikawa, 2017)	Hyperledger	Off-chain	A blockchain-based mobile health system for insomnia cognitive behavioural treatment	2017
	(Griggs, 2018)	Ethereum	Hybrid	Proposes the use of smart contracts based on the blockchain to perform real-time data analysis.	2018
	(Ray, 2021)	–	–	Propose a system that combines blockchain technology with IoT sensor data obtained from patients.	2020
Pharmaceutical supply	(Bocek & Stiller, 2017)	Ethereum	Off-chain	Maintains drug accessibility throughout transportation by keeping public temperature records.	2017

chain	(Haq, 2018)	–	–	Explains how to use blockchain to improve medicine supply traceability and visibility.	2018
	(Bryatov & Borodinov, 2019)	Hyperledger Fabric	On-chain	Create a blockchain-based control mechanism for drug distribution.	2019
	(Raj, 2019)	Hyperledger Fabric	On-chain	Create a pharmaceutical supply chain that is safe, unchangeable, and traceable.	2019
Health insurance claims	(Zhou, 2018)	On-chain		Proposes a medical insurance storage system based on blockchain technology.	2018

Source: - [1]

In Table 1, we offer an outline of the papers examined. The majority of these applications are built on prominent blockchain frameworks like Ethereum and Hyperledger Fabric, as we've discovered. [1]

IV. RESEARCH CHALLENGES AND OPPORTUNITIES

We can distinguish many constraints of medical services Blockchain-put together applications based with respect to the proposed models and created applications.

First off, semantic interoperability isn't tended to in EMR frameworks. Thus, clinical and wellbeing information experts should do manual assessment and planning of predefined ontologies. Second, at this level, clinical wrongdoing is wild.

Besides, worries about versatility and interoperability are at the very front of momentum and future examination around here. The trouble in interoperability uncovers an absence of rules for planning blockchain-based medical care applications. Accordingly, the various applications that have been made might not be able to speak with each other. Moreover, versatility is a significant issue with blockchain-based medical care frameworks [21], particularly while managing a lot of clinical information. Because of the huge volume of medical services information, keeping it on-chain, for example on blockchain, isn't plausible on the grounds that it could bring about huge execution decrease. There is likewise a dormancy issue in a blockchain-based framework because of exchange handling speed and off-chain information load. At long last, due to the blockchain's permanence and self-execution of code, brilliant agreements might be defenceless against programmers. Hacks like the decentralized independent association (DAO) assault brought about the deficiency of millions of dollars in shrewd agreement resources somewhere in the range of 2016 and 2018. [1]

V. DISCUSSION

Clinical studies benefit from blockchain technology in terms of credibility and results.

These recordings can be stored as intelligent contracts on the Blockchain in the form of a digital fingerprint. Network infrastructure security on all levels, identity verification and authentication of all players, and consistent patterns of authorization to access electronic health information are only a few of the advantages of Blockchain Technologies in Healthcare. Blockchain technology is used to track medication commitments and monitor the pharmaceutical supply chain. This technology may be used to preserve information on a single patient, making it easier to analyse and validate the results of a surgery. Medical records, clinical trials, and patient monitoring all benefit from the use of blockchain, which improves security, transparency, and information display.It keeps financial statements in hospitals up to date and reduces the time and expense of data migration.

It solves a number of issues in a data-centric setting.

For each blocks of patient health records, blockchain technology will create a hash. Patients will be encouraged to provide their needed data with third parties while maintaining their anonymity thanks to the blockchain technology. A clinical study necessitates a significant number of data sets. The researchers focus on these data sets and conduct routine experiments in order to produce analyses, estimations, and efficiency ratios in a variety of situations. The information is analysed, and further judgments are taken based on the results. Many scientists, on the other hand, can falsify the data and evidence acquired to change the outcome.

Furthermore, many pharmaceutical companies wish to document the discoveries that will benefit their company. As a result, researchers are employing Blockchain technology to make clinical trials more equitable and transparent. It will aid in the recording of safe, uneven, and uncomplicated clinical studies. The information acquired can help enhance patient care and enable post-market analysis to maximise efficiency gains.

These guidelines are based on key features of Blockchain technology, such as open management, clear auditing trails, data openness, resilience, and enhanced privacy and security. This enables healthcare professionals to adhere to current healthcare requirements, including the safety of pharmaceutical supplies.

VI. CONCLUSION

The current review offered a layout of Blockchain's application in medical services. Truth be told, blockchain has been utilized in a scope of utilizations fully intent on expanding the computerization of clinical benefits, attributable to its quick development.

Most of blockchain-related investigations in medical services, as per our information, are centered around sharing electronic wellbeing records. Different areas of interest for blockchain analysts incorporate natural exploration, drug supply frameworks, and protection. Furthermore, we saw that article managing execution subtleties are interesting.

Despite the fact that blockchain innovation has a great deal of potential, more examination is expected to additionally grasp, create, and survey this innovation in a safe and productive way. To fortify partners' trust in involving this innovation and lift its acknowledgment in medical services, progressing endeavours are being made as far as possible in versatility, security, and protection.

VII. REFERENCES

[1]. R. B. Fekih and M. Lahami, "Application of Blockchain Technology in Healthcare: A Comprehensive Study," ICOST 2020: The Impact of Digital Technologies on Public Health in Developed and Developing Countries, pp. 268-276, 2020.

[2]. "Electronic health and medical records".

[3]. P. W. Zhang, "FHIRChain :applying blockchain to securely and scalably share clinical data," Computational and Structural Biotechnology Journal, vol. 16, pp. 267-278, 2018.

[4]. S. C. Jiang, "BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange," 2018 IEEE International Conference on Smart Computing (SMARTCOMP), 2018.

[5]. G. M. Dagher, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," vol. 39, pp. 283-297, 2018.

[6]. A. d. Roehrs, "OmniPHR: a distributed archi - tecture model to integrate personal health records.," J Biomed Inform, vol. 71, pp. 70-81, 2017.

[7]. D. K. Ichikawa, "Tamper-Resistant Mobile Health Using Blockchain Technology," JMIR Mhealth Uhealth, vol. 5, p. 7, 2017.

[8]. P. D. Ray, "Blockchain for IoT-based healthcare," IEEE Systems Journal, vol. 15, pp. 85-94, 2021.

[9]. F. H. Jamil, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," Electronics, 2019.

[10]. E. e. Fernando, "Success factor of implementation blockchain technology in," 2019 6th International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE), 2019.

[11]. T. N. Mackey, "A review of existing and emerging digital technologies to combat the global trade in fake medicines," Expert Opin. Drug Saf, pp. 587-602, 2017.

[12]. A. A. Ekblaw, "A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data," 2016 2nd International Conference on Open and Big Data (OBD), vol. 13, p. 13, 2016.

[13]. Q. S. Xia, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," IEEE, vol. 5, pp. 14757 - 14767, 2017.

[14]. K. W. Fan, "MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain," Journal of Medical Systems, vol. 42, no. 8, p. 136, 2018.

[15]. K. O. -. Griggs, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring," Journal of Medical Systems, vol. 42, no. 7, p. 130, 2018.

[16]. T. Bocek and B. Stiller, "Blockchains everywhere - a usecase of blockchains in the pharma supply-chain," 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 772-777, 2017.

[17]. I. E. Haq, "Blockchain technology in pharmaceutical industry to prevent," International Journal of Computer Applications, vol. 975, p. 8887, 2018.

[18]. S. Bryatov and A. Borodinov, "Blockchain technology in the pharmaceutical supply chain: researching a business model based on hyperledger fabric," Information Technology and Nanotechnology, 2019.

[19]. R. R.Raj, "Anticounterfeiting in Pharmaceutical Supply Chain by establishing Proof of Ownership," TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), pp. 1572-1577, 2019.

[20]. L. W. Zhou, "a blockchain-based medical insurance storage," vol. 42, no. 8, p. 149, 2018.

[21]. A. D. Mazlan, "Scalability Challenges in Healthcare Blockchain System—A Systematic Review," IEEE Access, vol. 8, pp. 23663 - 23673, 2020.
[22]. T. S. Ahram, "Blockchain technology innovations," IEEE Technology & Engineering Management Conference, p. 137–141, 2017.
[23]. R. B. Fekih and M. Lahami, "Application of Blockchain," pp. 1-9, 2020.
[24]. "Ethereum: a secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1-32, 2014.
[25]. S. Nakamoto, "A Peer-to-peer Electronic Cash System," 2008.
[26]. M. L. Iansiti, "The truth about blockchain," Harv. Bus. Rev, pp. 118-127, 2017.
[27]. V. L. Gatteschi, " Blockchain and smart contracts," Future Internet, 2018.
[28]. D. . Bender and K. Sartipi, "HL7 FHIR: An agile and RESTful approach to healthcare information exchange," Proceedings of the IEEE Symposium on Computer-Based Medical Systems, pp. 326-331, 2013.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

IoT Technique - Added Advantage for Border Security

Saurabh Chaudhari, Suvarna Ranade, Krutveej Shinde
M.Sc. (Statistics), MITWPU, Pune, Maharashtra, India

ABSTRACT

India has a massive and complicated border of 15,106.7 km, which is shared with Bangladesh, China, Pakistan, Nepal, Myanmar and Bhutan, and also a small portion with Afghanistan containing harsh terrains including deserts, fertile lands, swampy marshes, snow-covered peaks including world's highest battleground Siachen glacier and tropical evergreen forests. The difficult terrain, peculiar conditions related to each one of them, climatic conditions, relationship with certain neighbours, etc, all these factors make safe guarding our borders challenging and vulnerable to insurgency, intruders' activity, smuggling, anti-national activities and many more. So, in this paper we propose a device which identifies terrorist using Mobile app, soft chip, IOT device on Border that can capture some important information of intruders.

Keywords — Mobile Application, ArduCAM, Soft Chip, Raspberry-Pi, Pi-Camera, IR sensor.

I. INTRODUCTION

Today in asymmetric warfare, identification and control over the enemy is not easy as they can be disguised as civilians or access military bases with stolen badges. IoT sensors scan irises, fingerprints & other biometric data to identify individuals who are recognised as a threat. An IoT device system is a revolution of modern technology. It has been able to provide significant support to mankind by accomplishing the task that is impossible for human beings. These devices can be used to accomplish tasks like rescue, security, surveillance in unstructured and natural environments. Wearable sensors are the basic elements of military smart devices. The sensing module contains an information resilience, collects information on the battlefield under strict resource constraints and realizes data transmission and analysis by cooperating with other modules that are integrated with the equipment.

II. WHAT IS IOT?

IOT simply has made ordinary devices digitally intelligent that were otherwise inarticulate. Devices & systems are now connected through the internet which interact with each other & the users.

IOT is a vast network of devices connected via sensors including things like Smart Watches, Smart Phones, Soft Chip to air conditioning units. It allows users to achieve automation, analysis, integration, and users can have better reach over areas & more control over them.

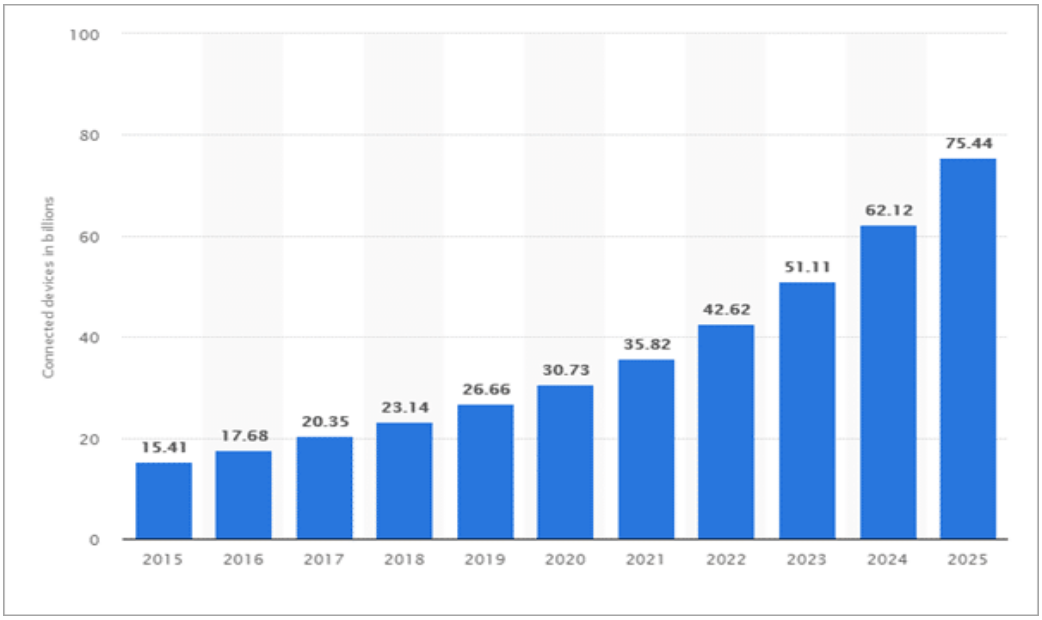
Surveying the battlefield in advance can help the military in taking relevant decisions at the right time. This can also be achieved by combining unmanned aerial vehicles with IoT sensors that sense & provide information in real-time to the command centres.

III. DEMANDS OF IOT DEVICES

It is a matter of fact today that several IOT products have surpassed a huge number of humans on this planet. Approximately there are around 7.62 billion humans on our planet, but to your surprise, by the year 2022 with an increasing graph of IoT devices, there may be around 20 billion IoT smart devices up and running with an increase in the demand of 5g network.

Nowadays, the production and usage of the Internet of Things devices are increasing very rapidly. IoT products and devices basically include laptops, smartphones, smart gadgets, smartwatches, smart and digitized vehicles, and almost all of these are used majorly today.

Please refer the below graph for to know the increasing demand for these devices in the near future:



If an average is made then after some years each and every individual in America would be having more than 10 IoT devices of their own.

IV. THE PAST, PRESENT, AND FUTURE OF THE IOT IN THE MILITARY

Information has always been an important aspect in the military. Soldiers have lived and died for it. Technology brings the ability to improve communication, routing, and processing of information, thus providing them with more and more sorted data. And an IoT is one such kind of technology.

It started with the US military during the Cold War that made use of a wireless sensor network in IoT technologies to detect Soviet submarines called the “Sound Surveillance System” (SOSUS).

The military is slowly but steadily integrating more and more IoT technologies such as machine-to-machine communications, also commonly known as RFID. IoT technology provides cost efficiency and war fighting effectiveness to the military by providing quick and easy information.

V. IDEAS

1. Mobile Applications

- One of the most important IoT-based mobile applications is the use of IoT mobile applications in the Military. Technology has always helped to strengthen the military in the past years. Now, mobile applications are assisting soldiers in the overall analysis of strategies for terrorist & war situations.
- IoT creates a smart environment using smart devices. Pairing with mobile applications enables users to control these devices remotely, this technology is one of the most remarkable technologies of this era. IoT - based mobile applications have a wide range of benefits.
- The IoT devices with mobile applications can be used for monitoring security purposes with reduced risks and costs to the human workforce. With a single application on a device, IoT devices can be efficiently managed and monitored. Mobile applications play a significant role in enriching the growth of IoT.

2. Soft Chip

- The U.S. Land Warrior Integrated Soldier System (LWISS), which includes a protective system, an information-processing system, and a combat system, has been one of the marvelous achievements in military smart devices. The system includes a variety of sensors and communication devices that assist soldiers to exchange intelligence in the point-to-point model.
- The U.S. Tactical Assault Light Operator Suit (TALOS), which has been in development for many years, is equipped with exoskeletons, smart helmets, protective Armor, and multiple biosensors to maximize the battlefield capabilities of soldiers.

3. IoT device on Border

- Every movement on borders cannot be surveilliated by soldiers easily which may lead to illegal border activities and attack of invaders unknowingly.
- At the moment when an unknown person is recognized in the scope of the IR sensor immediately it sends the flag to the raspberry pi and the pi camera starts capturing the images.
- IR sensors are capable of detecting the living and non-living things, it can differentiate between humans and animals and also can detect weapons. After capturing images, it will compare with the database stored in the server. It will send a flag to the command centre and if the image does not match with any normal aspect and is confirmed as an intruder, the robot carrying the gun will be directed to shoot that person immediately at the moment on the orders of the commander.
- At that point the protection operation will be quick in identifying the people who have entered unknowingly and necessary action can be taken accordingly.

VI. THE SYSTEM IMPLEMENTED USING FOLLOWING HARDWARE COMPONENTS

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper.

In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

A. Raspberry Pi

Raspberry Pi is a credit-card-sized computer manufactured and designed in the United Kingdom by the raspberry pi itself.

B. Pi – Camera

In order to meet the increasing need of Raspberry Pi compatible camera modules. The ArduCAM team now released a revision C add-on camera module for Raspberry Pi which is fully compatible with the official one. It optimizes the optical performance than the previous Pi cameras, and give user a much clear and sharp image.

C. IR Sensor

This device emits and/or detects infrared radiation to sense a particular phase in the environment. Generally, thermal radiation is emitted by all the objects in the infrared spectrum. The infrared sensor detects this type of radiation which is not visible to the human eye.

VII. HOW DOES IOT WORK AND HOW DOES IT HELP ON THE BORDER?

Transformation of a normal device into an IoT smart device basically depends on two things.

1. The device which has the capability to connect with the internet in any way.
2. The device which is integrated with technology like sensors, functional software, some inbuilt technology which support network connections and also actuators.

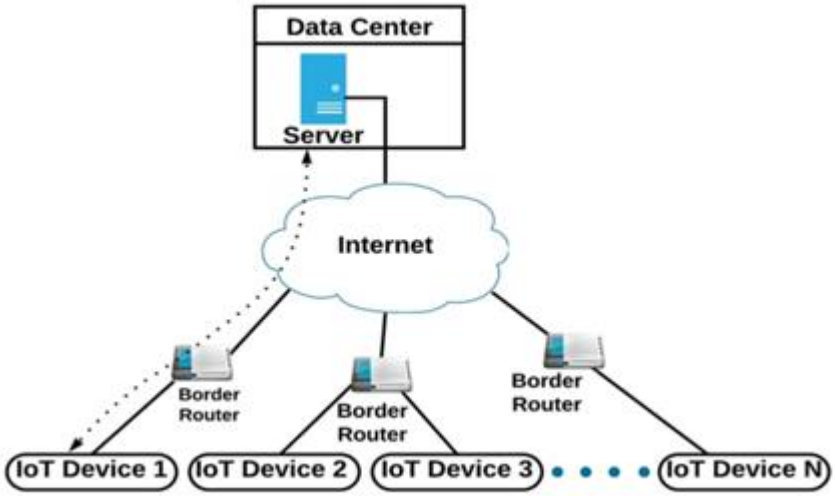
When both these functionalities are combined together an IoT device is formed. Earlier only simple watches were used to see the time and date, but now the smart IoT watches allow a user to see heart rate, pulse rate, calorie count, temperature etc. of soldiers

The demand for IoT devices is expanding rapidly day by day and becoming more popular as well with the drastic increase in the number of users who use them daily.

VIII. WORKING STRUCTURE OF IOT DEVICE

The figures at the bottom are IoT devices that are installed on the border. They collect the information and send it to the server eventually with help of the Internet. The server accesses the information and analyses it to send it to the commander so as to take required action further.

IX. ADVANTAGES AND DISADVANTAGES OF IOT DEVICES



Apart from this information, there are some advantages and disadvantages of the Internet of Things devices which may have a great impact on the current and future generation of mankind.

Advantages

There are several advantages of these smart devices and some of them are given below.

- IoT encourages the interaction between devices called as a machine-to-machine interaction. The physical devices are capable of staying connected; hence, total transparency is available with higher quality and minor inefficiencies.
- It provides good automation and control.

- Integrated with more technical information, it is better to operate.
- IoT possesses strong monitoring features.
- It saves a lot of time.
- IoT helps to save more money by reducing manual tasks and time.
- Automating daily life tasks makes good monitoring of devices.
- Increased efficiency and time-saving.
- Good features make a better quality of life.

Disadvantages

Though there are several advantages, there are certain disadvantages too.
Enlisted below are the various demerits:

- Internet of Things devices do not have any international compatibility standard.
- As there is the involvement of different devices and technologies, the number of connected devices increases, and more information is shared between them. It increases the chances that a hacker could steal confidential information, which directly questions the security and privacy issues.
- They may become highly complex resulting in failure.
- Internet of Things devices may get affected by privacy and security breaches.
- Reduced safety for users.

X. CONCLUSION

Internet of Things is the notion where the virtual world of information technology is connected to the real world of things. The technologies of the Internet of things such as RFID and Sensor make our life become better and more comfortable.
Wearable advances are currently infesting numerous applications in a few fields. The aim of this paper is to abridge the genuine savvy attire in the military field where conditions could be basic for wellbeing and security, and diagram the advancement pattern for inventive administrations to security forces and warriors.

XI. ACKNOWLEDGEMENT

We would like to express our sincere gratitude to the team of organizers of MITWPU for giving us this platform to learn and excel in project work. Special thanks to the Defense Research and Development Organization for providing the data on their website for easily accessible research... Also, thanks to our parents for making necessary things available at home during this lockdown which helped the research project go smoothly, and lastly thanks to our mentors for their support and motivation.

XII.REFERENCES

[1]. Rhagini, Karvendhan, Santhvel V, Sindhu Priya V, Sivasakthi “IoT based Soldier Monitoring System with Automatic Temperature Adjust Suit”. International Journal of Advanced Trends in Computer Science and Engineering, pp(2278-3091).

[2]. Tushar Samal, Saurav Bhondve, Suraj Masal, Sagar Gite, Prof.Sushma B. Akhade “Soldier Health Monitoring and Tracking System Using Iot”. International Journal of Advance Scientific Research and Engineering Trends, pp (2456-0774).

[3]. M. Pradeeppa, Dr. E. Kirubakaran "International Journal of Wireless Communications and Networking Technologies". International Journal of Wireless Communications and Networking Technologies, pp(2319-6629).

[4]. Websites: Most Popular IoT Devices in 2022 (Only Noteworthy IoT Products) (softwaretestinghelp.com)

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Seed Certification Using Blockchain Technology

Nakia Lightwala, Mehul Sherdiwala, Anuradha Kanade
School of Computer Science, MIT-World Peace University, Pune, Maharashtra, India

ABSTRACT
One of the major targets to achieve worldwide is food security, proper nutrition and sustainable agricultural practices. The large number of stakeholders involved – the farmers, distributors, retailers, etc present the maintenance and understanding of the agricultural supply chain as one the most complex structures. A subsystem is the Seed Supply chain which is an equally complex structure in the ecosystem involving various collaborators. Due to vast coherent internal connections across the supply chain, it becomes extremely difficult to maintain the traceability and integrity of the stored data. Most farmers across the world are exploited in terms of accountability and their respective ongoings. The present paper determines a solution to maintain the traceability of various transactions that take place keeping in mind several important criteria such as the origin of the seed, stages of production, conformance to quality standards such as genetic purity, germination rate, etc while keeping utmost security and lower costs. With various applications of blockchain technology renown, the greatest choice to maintain records of sustainable practices is in the agricultural sector.
Keywords—Blockchain, sustainable agriculture, traceability

I. INTRODUCTION

In 2015, the United Nations, in collaboration with the UNESCO, proposed 17 major goals to achieve before 2030 which were adopted by United Nations member countries. The UN has embodied inter-governmental teams to turn these goals into actual policies. With overall 169 targets and 5337 actions taken in consideration of these goals as of February 2021, the UN focuses on worldwide issues from gender inequality to localising small cities and regions. One of the major goals among these is the quality of food that is made available to people across the world. The root of this issue starts with the quality of seeds provided to the crop producing farmers. One of the widespread solutions for this problem statement is Seed Certification. It is followed to preserve the genetical hierarchy of crops and the purity in their variety. Certified seed is just the first step towards better quality of crops. It is the most practical and reliable method after years of research and field work of verifying genetic identity and purity for the improved varieties of commercially available crops across the agricultural sector.

Implementation of blockchain technology is enabled to allow a better maintenance of records and keeping them secure with fewer costs. The blockchain is basically a distributed database technology which allows to

maintain authenticity and integrity of the data at zero transactional cost. It is said to be a disruptive technology and is expected to take communication and business to another level like the web.

The working of blockchain is similar to that of a ledger, wherein data is stored as/in a block which is then connected to another block, thereby forming a chain of records. Each record is stored as a verified block which is then added – creating a chain of transactions stored across the net, creating not just a unique record, but a unique record with a unique history. Moreover, the blockchain technology provides the facility to view the users accessing these transactional records. The greatest benefit of the working of blockchain technology is that it exists as a shared — and continually reconciled — database. Thus, the records in a blockchain are not stored at one single location and are kept truly verifiable by authenticated users.

The above-mentioned functionality of blockchain allows us to store data from scratch into a properly constructed database with an additional feature of security maintenance and traceability. It thereby allows these blockchain features to be implemented in order to cross check and identify the base of the seed – from its origin, genetic history, seed aggregators, distributors, retailers to farmers with maintenance of authenticity of stored data. This work proposes a thesis on blockchain-based solution that removes the need for a secure centralized structure, intermediaries, and exchanges of information, optimizes performance, and complies with a strong level of safety and integrity.

II. HURDLES FACED BY FARMERS IN THE AGRICULTURAL SECTOR

Within a world changing drastically and new innovations taking place across the globe, the agriculture sector faces an unprecedented challenge every day. While each bit of these is constantly been worked upon by scientists and developers to find an optimum solution for, the existential crisis remains the same. These problems are not just faced by farmers but are also faced by each stakeholder involved in the procedure from germination stage to cultivation stage till it reaches to the end user.

Major issues being addressed by the world, it is a major task to look out for a solution for each minor problem faced by them. Most of the problems in the sector are in regards to irrigation systems, quality of seeds, bad weather, crop diseases, manure and fertilizers, the lack of mechanical equipment and inadequate storage facilities. The farmers also face problems in terms of financial loans and subsidies towards which the government works for a solution by launching beneficial schemes and easy repay mechanism for farmers. The increasing ratio of farmer suicides is another issue of concern which is the end result of problems of land holdings, scarcity of capital, demographic change, involvement of middlemen, etc. In the proposed paper, we take into account the problem of seeds provided to farmers which affects the overall health of a nation, and the world on a whole.

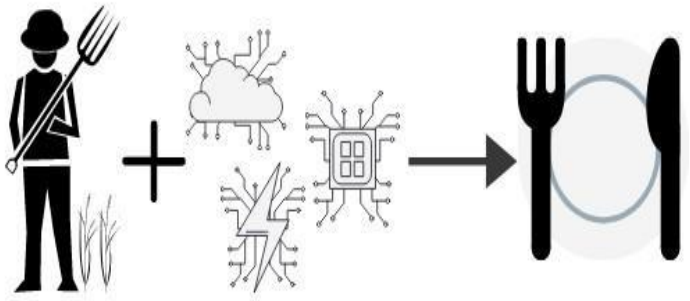


Fig. 1. Use of blockchain in agriculture.

III. SEED CERTIFICATION

Seed is basically the agricultural input that grows into embryonic plant, into an edible food item. With increasing population, the requirement of agricultural produce has been increasing on a wider level and parallelly the implementation of various farming techniques to increase production through chemicals and hybrid seeds production is also increasing. Poor quality seeds hamper the production in terms of cultivated produce. Hence, in order to preserve genetic purity and varietal identity of each produced seed, the process of seed certification came into being.

The seed is divided into four classes in the certification program – Breeder Seed, Foundation Seed, Registered Seed and Certified Seed to classify the required land features, field stock and improvisation of yield. The seed chain is basically processing seed from the breeder program who is well informed about the seed structure into a properly "blue labelled" certified seed. Seed laws and regulations are implemented across the world to examine the properties of the seed offered to sale. Features of the seed such as its weight, kind, variety, origin, purity, inert matter – everything in the line is taken into consideration. The Seed Certification Department carries out the certification work in various seeds notified under Indian Seeds Act, 1966 and in accordance with the provisions of the Seed Rules 1968 to maintain the quality of the seeds produced in the state. In order to maintain and make information available to the public, through certification, high quality seeds and propagating materials of notified kind and varieties are grown and distributed as to ensure genetic identity and genetic purity. The government has set protocols and rules for seed development meaning it has certified foundations and laboratories which cultivates varieties of seeds under a controlled environment, and checks the quality and purity of the cultivated seeds keeping in view the physical and physiological parameters, before it is sent to the seed aggregators. This allows consumers to be aware of the entire supply chain and related information.

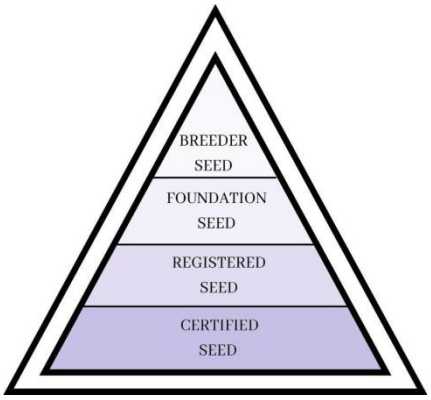


Fig. 2. Stages of seed for certification.

IV. BLOCKCHAIN AND ITS APPLICATIONS

A. Overview and Definitions

The blockchain is one of the most rapidly growing distributed ledger technologies. One of the core principles of blockchain technology is the "fingerprint" concept that is termed as the unique identifier of every block. In the usage of blockchain, each data record is stored as a block. The block consists of three important components that form a chain like structure – Data stored in the block, a hash value that represents the previous block and finally, a value that represents its own hash. According to Mayank Raikwar et al., a very general definition of blockchain is: "Blockchain is a distributed ledger maintaining a continuously growing list of data records that are confirmed by all of the participating nodes". One of the most innovative solutions to the constant agricultural issues is through the application of blockchain technology. The blockchain technology allows all the involved nodes to keep a check on the transactions of all the participating nodes which reduces the chances of discrepancies to a much larger level than in the current scenario.

Fig. 3. Concept of blockchain.

The concept of blockchain prevails on two types – Private Blockchain and Public Blockchain. Public Blockchains are generally used for one of the most popularly growing implementations of blockchain concepts – Cryptocurrency – Bitcoin, Ethereum, Dash – all these use the concept of public blockchains where anybody can read and add contracts and data and also choose between maintenance of one hundred percent transparency or absolute anonymity. Private blockchains, on the other hand, keep data, information, contracts – everything private. However, hybrid approaches for implementation of blockchains have come into existence wherein authenticated users are provided permissions for configurational flexibility. There are instances where

list of participants is predefined and kept generated and actions on the blockchain is restricted based on the user role.

B. Farm to Fork using Blockchain Tools and Technology

Blockchain technology allows us to produce a proper trail of all the transactions and connect them with utmost security and at minimal cost. Blockchain provides a solid mechanism to secure transactions and also allows anonymity to users that fit into the criteria proposed by the developer in the first place. Smarter approach to traceability can be acquired to store and connect data blocks and records in an optimum manner to follow food production from the beginning i.e. origin of the seed to the distributors and retailers, added substances – pesticides to fertilisers, undertaken procedures across the farmer network before it reaches to the consumer's plate via blockchain. This approach can be taken all across the globe, which will not only reduce costs but also help the United Nations achieve the mission of food security.

Permissioned Blockchain approach can also be taken on board to provide permissions to specific stakeholders that play significant role in the construction, application and implementation of the food supply chain. The same concepts can also be utilised by the end users via facilities such as QR code to be acknowledged about the supply chain and maintain the records and enhance their food and nutritional security, since they can ensure the traced details from the seed origin to the produced food on their plate.

C. Applications of Blockchain Technology

The greatest widespread application of Blockchain Technology that has spread its wings across the globe is the emerging Cryptocurrency. The scope of blockchain technology is way beyond bitcoins and Ethereum. This technology holds up the capability to enhance and outgrow every sector across the globe with its efficiently aligned features of security and transparency. An added advantage of this technology is the reduced cost for conducting such transactions that can help not only developing countries to grow but also help developed nations to enrich their economy without delimiting their scope.

Monitoring supply chains is one of the very basic yet very important real world application of the blockchain technology. In addition to the existing supply chains, blockchain technology holds the power to maintain proper track record and traceability for the subsystems formed within the ecosystem.

D. Traceability

With the advancement of technology and the world growing and on the lane turning towards technology, one of the great accomplishment of goals with concepts of Blockchain and Internet of Things is automating the closely related matter in a supply chain, in a sector, on the whole. With the application of blockchain in an optimised manner, it is possible to keep track and trace each and every occurrence of events that takes place without comprising on security and integrity of data but also maintaining authenticity of the data stored at each stage by any one or all of the stakeholders. These features of the forementioned technologies allow every participant to maintain the paradigm and retain the flow of the data through various data gathering and maintaining procedures. Hence, this traceability allows every stakeholder to keep track and verify all the details.

E. Agriculture Traceability

As for the old-school approach followed in the agricultural sector, in order to maintain track records, it was crucially important, even if inconvenient, to maintain record of every operation that takes place across not just a specific farm area but on the whole, every bit of the sector which is involved in the supply chain – from seed details, distributors who engage in the transportation of produced goods, farm equipment that is being used on

the farm – on a daily basis, weekly, and so on. As mentioned and elaborated in the seed certification section – the features and properties of the seed that need to be kept into consideration to trace each piece of information, updates and every detail in relation to the seed from its origin to its cultivation can be made available to all the participants of the supply chain, thereby improving the maintenance of integrity of the data and making it much more secure.

V. CONCLUSION

Various societal problems, problems of food fraud, food security, tracing of products can be solved since blockchain is a part of prominent and vastly growing distributed ledger technologies. Existing systems use certification access mechanism which fail to provide visibility on a larger level to its peer networks; traceability, however, helps address several issues allowing to store, facilitate and execute programs. Research conducted in the context of this paper is to thereby show and prove how blockchain is benefiting every sector as a whole and how it can be specifically implemented to grow and digitalise the agricultural sector. It increases user security thereby reducing risk, decreases the involved costs on a larger level. The consolidation of blockchain technology in agricultural sector will help to increase productivity, add value and solve enormous challenges that exist in the sector.

VI. REFERENCES

[1]. Konstantinos Demestichas, Nikolaos Peppes, Theodoros Alexakis and Evgenia Adamopoulou, “Blockchain in Agriculture Traceability Systems: A Review,” applied science, pp. 1-22, June 2020.

[2]. Agritech.tnau.ac.in, “CHAPTER X SEED CERTIFICATION”. [Online]. Available: http://www.agritech.tnau.ac.in/seed_certification/pdf/seed_cert_09.pdf. [Accessed: 10-Feb-2022].

[3]. Puja Mondal, “10 Major Agricultural Problems of India and their Possible Solutions”. [Online]. Available: https://www.yourarticlelibrary.com/agriculture/10-major-agricultural-problems-of-india-and-their-possible-solutions/20988. [Accessed: 10-Feb-2022].

[4]. William Warshauer, “How digital is solving 3 problems in agriculture”, Jan. 2016. [Online]. Available: https://www.weforum.org/agenda/2016/01/how-digital-is-solving-3-problems-in-agriculture/. [Accessed: 11-Feb-2022].

[5]. The Central Seed Certification Board Department of Agriculture & Co-operation Ministry of Agriculture Government of India, “INDIAN MINIMUM SEED CERTIFICATION STANDARDS”, 2013. [Online]. Available: http://odishaseedsportal.nic.in/SeedPortalData/Resource%20Material/INDIAN_MINIMUM_SEED_CERTIFICATION_STANDARDS.pdf [Accessed: 11-Feb-2022].

[6]. The Central Seed Certification Board Department of Agriculture & Co-operation Ministry of Agriculture Government of India, “State Seed Certification Management System”. [Online]. Available: https://seednet.gov.in/seedcert/Seed%20Certification%20User%20Manual.pdf. [Accessed: 11-Feb-2022].

[7]. K. Parimala, K. Subramanian. S. Mahalinga Kannan and K. Vijayalakshmi, “A Manual on Seed Production and Certification”, Dec. 2013. [Online]. Available:

https://agritech.tnau.ac.in/seed_certification/pdf/A%20Manual%20on%20Seed%20Production%20and%20Certification.pdf. [Accessed: 12-Feb-2022].

[8]. Mcia.msstate.edu, "Why Go Certified?". [Online]. Available: https://www.mcia.msstate.edu/certified/. [Accessed: 12-Feb-2022].

[9]. Nathan Fiala, "The supply chain for seed: Where does it all go wrong?", Dec. 2016. [Online]. Available: https://www.theigc.org/project/the-supply-chain-for-seed-where-does-it-all-go-wrong/. [Accessed: 12-Feb-2022].

[10]. J S Chauhan, S Rajender Prasad, Satinder Pal and P R Choudhury, "Seed Systems and Supply Chain of Rice in India," Research Gate, vol. 10, pp. 9-16, Jan. 2017.

[11]. Samuel Burer , Philip C. Jones, Timothy J. Lowe, "Opportunities for Quality Seed Production and Diffusion through Integration of the Informal Systems in Sub-Saharan Africa," Science Direct, pp. 354-377, Dec. 2006.

[12]. Munyiri SW, "Coordinating the supply chain in the agricultural seed industry," Research Gate, pp. 1-20, Oct. 2020.

[13]. SOMASHEKHAR I C, Dr. J.K. RAJU, Dr. HEMA PATIL, "Agriculture Supply Chain Management: A Scenario in India," The International Journal Research Publication, pp. 1-20, 2014.

[14]. Open Link, "Blockchain food traceability can revolutionize the industry". [Online]. Available: https://openlink.com/en/insights/articles/blockchain-food-traceability-can-revolutionize-the-industry/. [Accessed: 14-Feb-2022].

[15]. Juan F.Galvez, J.C.Mejuto, J.Simal-Gandara, "Future challenges on the use of blockchain for food traceability analysis," Science Direct, pp. 1-41, Aug. 2018.

[16]. Reshma Kamath, "Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM," The JBBA, vol. 1, pp. 41-53, June 2018.

[17]. M.Creydt, M.Fischer, "Blockchain and more - Algorithm driven food traceability," Sceince Direct, pp. 1-15, May 2019.

[18]. Huanhuan Feng, Xiang Wang, Yanqing Duan, Jian Zhang, Xiaoshuan Zhang, "Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges," Sceince Direct, pp. 1-37, Mar. 2020.

[19]. Jun Lin, Zhiqi Shen, Anting Zhang, Yueting Chai, "Blockchain and IoT based Food Traceability for Smart Agriculture," ACM, pp. 1-6, July 2018.

[20]. Yung Po Tsang, King Lun Choy , Chun Ho Wu , George To Sum Ho, Hoi Yan Lam, "Blockchain-driven IoT for Food Traceability with an Integrated Consensus Mechanism," IEEE, pp. 1-18, 2017.

[21]. Miguel Pincheira Caro, Muhammad Salek Ali, Massimo Vecchio and Raffaele Giaffreda, "Blockchain-based Traceability in Agri-Food Supply Chain Management: A Practical Implementation," IEEE, pp. 1-4, 2018.

[22]. QIJUN LIN, HUAIZHEN WANG,XIAOFU PEI AND JUNYU WANG, "Food Safety Traceability System based on Blockchain and EPCIS," IEEE, vol. 4, pp. 1-10, 2016.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Comparative Analysis of Ethereum and Solana

Brinda Chanchad[1], Anuradha Kanade[2], Sahil Vaidya[1], Himanshu Patil[1]
[1]Student (MCA), School of Computer Science, MIT-World Peace University Pune, Maharashtra, India
[2]Faculty, School of Computer Science, MIT-World Peace University Pune, Maharashtra, India

ABSTRACT
Cryptographic types of cash are still first thing in their journey; Ethereum has been among the first cryptos to emerge as a "blue chip," In any case, being a first-mover in a space doesn't mean you keep your crown, and choices have emerged to challenge Ethereum. Solana is one of these difficulties; a choice as opposed to Ethereum, it's been around since its improvement in 2017, but it didn't get very well known until this earlier year. Solana is right now the fourth-most popular cryptographic cash on Coinbase and conveys a $54 billion market cap, but it's as yet a limited quantity of Ethereum's size. Solana organizes well with Ethereum in two fundamental areas for development, speed and low trade costs. Ethereum's plan limits trades each second to 15-30 on its association, making the bottleneck that results in these high gas costs. Then again, Solana can deal with undeniably more, upwards of 50,000 every second, and its expenses are simply $0.00025. Solana has dramatically increased in cost somewhat recently.

Keywords—Ethereum, Solana, Cryptocurrency, Proof-of-history, Proof-of-work

I. INTRODUCTION

A digital money is a computerized or virtual cash that is obtained by cryptography, which makes it almost difficult to fake or two-fold spend. Numerous digital forms of money are decentralized organizations in view of blockchain innovation, a disseminated record upheld by a different organization of PCs. A characterizing component of digital forms of money is that they are by and large not given by any focal power, delivering them hypothetically insusceptible to government impedance or control. The digital money was created in 2008 by an obscure individual or gathering utilizing the name Satoshi Nakamoto. Digital cash started to be used in 2009. whenever its execution was delivered as open-source programming. The benefits of digital currencies incorporate less expensive and quicker cash moves and decentralized frameworks that don't fall at a weak link. It is used for Low-cost money transfers, Earn interest on Bitcoin and other cryptocurrencies with 'Yield Farming' etc.

II. LITERATURE REVIEW

The utilization of virtual cash has become boundless in various frameworks lately. Virtual cash isn't completely controlled and managed henceforth the majority of the nations have not conceded this money in their monetary exercises. This paper researches digital money present legitimateness as well as future government moves away on these monetary standards. The paper additionally dissects speculation taking a chance in both Bitcoin and Gold nations that have reacted as far as guidelines and regulations towards cryptographic forms of money to foster an unmistakable image of its effect on different regulations in India to direct it [4]. The possibility of a common economy becomes one of the organizations as a venture type. Particularly with the high-level improvement of computerized savvy gadgets and the web, a few types of the common economy have progressed as per the requirement for sharing of discrete pay. In this exploration, they have proposed a substance assurance and exchange strategy utilizing Blockchain Ethereum Technology. The encryption calculation is fused in the proposed framework to make straightforward exchanges and it is likewise executed on content itself to keep from brilliant imitation and hacking. The test results connote that the proposed strategy can possibly upgrade exchange straightforwardness by limiting the security dangers in computerized content exchanges [2]. Cryptographic money, an encoded, shared organization for working with computerized trade, is an innovation created eight years prior. While cryptographic forms of money are not liable to supplant conventional government issued money, they could change the way Internet-associated worldwide business sectors communicate with one another, cleaning up boundaries encompassing standardizing public monetary standards and trade rates. Innovation does make progress at a quick rate, and the achievement of a given innovation is exclusively directed by the market whereupon it looks to move along [1]. Ethereum is a blockchain stage that supports savvy contracts. Brilliant agreements are bits of code that perform broadly useful calculations. Throughout the long term, the predictable improvement of blockchain innovation and cryptographic forms of money, for example, Ethereum has been impacted by the digital currency economy. In this paper, we present a broad overview of brilliant agreements. Along these lines, we present a cytology of shrewd agreement arrangements, ordered by included exploration papers, and examine the current brilliant agreement-based examinations. In light of the discoveries from the study, we recognize a bunch of difficulties and open issues. Likewise, we recognize the resulting patterns for Ethereum and Solana [7]. Blockchain is a developing and arising record innovation, which is a moderately new methodology. The one for which blockchain innovation was concocted, bitcoin as a digital currency has enamoured a ton of consideration. As Ethereum, and blockchain executions center around brilliant agreements, they address the essence of improvement [6]. Shrewd agreements are carried out on a blockchain framework assuming that specific conditions are met, without the need of a third power. Shrewd agreements definitely stand out enough to be noticed. The type of Ethereum and the activity rationale of shrewd are breaking down and improving to deal with security issues of savvy contracts. Henceforth, the idea of Ethereum is introduced in blockchain application, with the sub construction of Ethereum [8]. The design of Ethereum and the activity rationale of shrewd agreement are examined and improved to deal with security issues of brilliant agreement. In this way, the idea and hypothesis of Ethereum are introduced in blockchain application, with the information construction of Ethereum. Then, at that point, the activity system of brilliant agreement is given pseudo code at the specialized level for savvy contracts, which is the center of Ethereum. In the genuine tests of shrewd agreement, the sale is executed by Solidity language. Finally, the deformities of the bartering application are

fixed and improved to help the use of shrewd agreement in Ethereum blockchain [10]. This implementation additionally makes use of a conveyed test RPC-based Ethereum blockchain and client master as an instruction specialist. Blockchain innovation can assist with decreasing misrepresentation in the dispersion and the executives of digital currency [12]. Bitcoin has arisen as the best digital currency since its appearance back in 2009. Other than its security heartiness, two principal properties have presumably been vital to progress: namelessness and decentralization [13]. Research on cryptographic forms of money is as yet missing regardless at its outset stage. In giving a significant aide and view to the scholastic field and clients, this paper talks about the valuable open doors in cryptographic money, for example, the security of its innovation, low exchange cost and high venture return. The future endeavors of digital money and its application are efficiently surveyed in this paper [5].

III. WHAT IS ETHEREUM AND SOLANA

A. Ethereum:

Ethereum is a decentralized blockchain platform that establishes a peer-to-peer connection which executes smart contracts. Smart contracts are responsible for transactions between participants without any central authority. Ethereum was founded in 2013 by Vitalik Buterin along with Gavin Wood, Charles Hoskinson, Anthony Di Iorio and Joseph Lubin.

B. Solana:

Solana is a blockchain network that provides a marketplace for decentralized apps. Solana has stateless architecture. Solana is the first block chain to use proof of history concepts. Solana is one of the most famous cryptographic forms of money among in excess of 10,000 that presently exist. Solana is created by Anatoly Yakovenko, Solana operates on a decentralized computer network using a ledger called blockchain.

IV. TRENDING TOP CRYPTOCURRENCY

The top six cryptocurrencies are Bitcoin, Ethereum, Solana Cardano, Dogecoin, Polkadot. Among these Solana and Ethereum are considered for the comparison in this paper.

V. SMART CONTRACTS

Smart contracts make Ethereum, Solana, Cardanol and surprisingly the Binance Smart Chain, not the same as Bitcoin. Described in their computations are little pieces of code that execute when certain circumstances are fulfilled. By and large, they are 'in case, when' clarifications that execute normally.

Envision a tenant contract, which says your lease should increase by 10% at regular intervals.

In the conventional financial framework, you could set up a standing instalment guidance where the lease sum is paid to your property manager consistently, however you should continue to transform it like clockwork, isn't that so? On a savvy arrangement, the structure will understand the rent has extended and could theoretically construct the total whenever reapplications' splendid arrangements can be portrayed on a

blockchain stage once, and they can't be changed by anyone. The elaborate gatherings can set up as many 'on the off chance that, when' conditions as they need inside a brilliant agreement.

VI. APPLICATIONS OF SOLANA

Solana can control a few applications that offer an assortment of highlights:

- Smart contracts: Smart contract is the code on specified blockchain technology which gets triggered whenever the certain condition is true
- Decentralized finance: With Solana, you can create a completely decentralised finance system which is free from any kind of middle party.
- Non-fungible tokens (NFTs): NFTs is any kind of digital property which exists on blockchain technologies like Solana, Ethereum
- Currency: cryptocurrency wallet, you can use Solana to transfer it in the form of services and goods.
- Proof of history approach: notwithstanding a proof of stake way to deal with approved exchanges, Solana timestamps them, disposing of the capacity to re-request exchanges to a validator's benefit. This helps make Solana an "oversight safe" affiliation.
- Digital apps: Besides all its use cases solan can be used for many more different kinds of applications like gaming apps.

Once more, consider Solana a symbol that can drive different applications rather than simply as a money that moves financial worth starting with one individual then onto the next.

VII. ARCHITECTURE

A. Proof of work:

Proof-of-Work is very energy intensive. The amount of computing power that's mining for cryptocurrencies like Ethereum, known as gas, is immense. This results in more energy consumption all over the planet. It's additionally affected the worldwide GPU market as excavators purchase costly PC equipment to mine all the more proficiently.

Energy consumption is one downside of Proof-of-Work. Also, pow follows a "longest chain" rule in which the longest chain in a blockchain is acknowledged by clients as being legitimate. This means that pow cryptos are more susceptible to 51% attacks, which occurs when an entity achieves 51% of total hash rate and builds the longest chain with fraudulent blocks and double-spends their crypto.

B. Proof of history:

Proof-of-History is an understanding instrument that Solana, one of the greatest computerized monetary forms by market cap, uses nearby PoS to help with settling the issue of general blockchain time and augmentation network speed. Solana's advantage is that it's extraordinarily capable. It can manage trades a ton faster than computerized monetary standards like Bitcoin and Ethereum in light of using PoH and various headways. Essentially, with PoH, centers have their own inside clock that affirms events and the movement of time. The verification utilizes an unquestionable postpone work (VDF) to hash approaching occasions and furthermore

notes when occasions happened. At the point when different hubs take a gander at the succession of hashes, they can promptly tell the request in which occasions happened without approving time with different hubs.

VIII. HOW SOLANA AND ETHEREUM DIFFER

Proof of history architecture is much cheaper than proof of work architecture. PoH requires less power than that of PoW. Time taken by PoW is more as compared to PoH. Solana uses PoH and Ethereum uses PoW which eventually makes Solana a cheaper, more efficient and faster alternative to Ethereum.

1.0(the one we are utilizing as of now) depends on a Proof-of-Work (PoW) framework, comparable to the instrument that is used by Bitcoin's blockchain. The association, then, at that point, is gotten by many thousands (in the event that not a large number of) diggers who take part during the time spent agreement by "denoting" their enrolling power/hardware. While this ensures that the association, by and large, stays decentralized and the block to entry to taking an interest inside the association is high, it similarly prompts diminished execution on the association as it can't deal with various trades each second.

The second point that makes Ethereum not quite the same as Solana is its "stateful" nature.

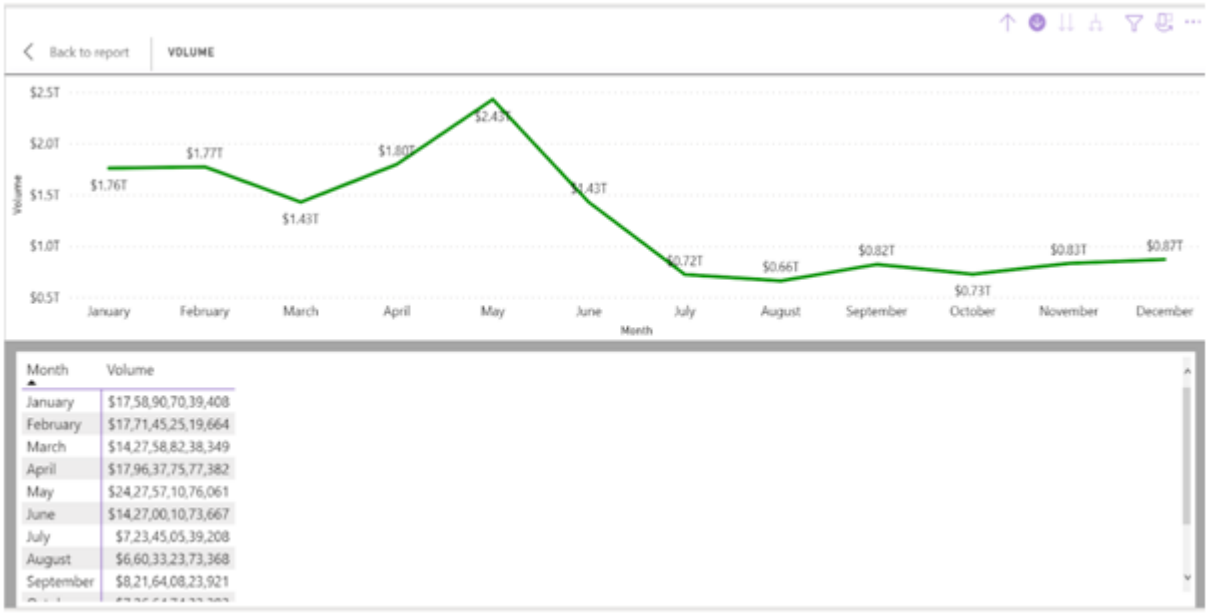
It implies that every one of the exchanges on the organization are recorded into one state and on the off chance that any new exchange happens, the whole organization (or every one of the diggers) should refresh their duplicate of the company to clone that new transaction. In simple words, if Alice could send Bob $10 through Ethereum, then, at that point, the whole organization of excavators (which for supposition that are 10,000) all over the planet would need to invigorate their records to reflect that. This Sequence isn't unassuming, and therefore Ethereum 1.0 is considered slower than other 'stateless' blockchains like Solana.

The earnest spot where Solana contrasts from Ethereum is the principal understanding part. It is known as Proof-of-History (PoH) and, on a very basic level, it requires a progression of computational advances that choose the time section between two events cryptographically. This is furthermore wrapped up by adding timestamps to all trades and following each one's association. This kind of solicitation sequencing is significantly not the same as that in Bitcoin and Ethereum, where their trades are not submitted in a fortunate solicitation.

The other key difference with Ethereum is that Solana has a 'stateless' designing and, as right now analyzed over, this diminishes the overall memory usage. Since the entire state of the association shouldn't mess around with invigorating for each trade, they can be easily finished sequentially. This is one of the factors that make Solana exceptionally adaptable.

Solana is amazingly adaptable, coming about its exchange expenses 60 thousand times lower than that of Ethereum.

IX. GRAPHICAL INSIGHTS OF SOLANA VS ETHEREUM



Month	Volume
January	$17,58,90,70,39,408
February	$17,71,45,25,19,664
March	$14,27,58,82,38,349
April	$17,96,37,75,77,382
May	$24,27,57,10,76,061
June	$14,27,00,10,73,667
July	$7,23,45,05,39,208
August	$6,60,33,23,73,368
September	$8,21,64,08,23,921

Fig. 1. Volume by Month - Ethereum/ Solana

1) In the first line chart we have shown the volume for the Ethereum vs Solana coin by Month, Quarter & Year. It has a drill down option from which we can see the volume of the coin respectively. Now, as the slicer is clicked for Ethereum, it shows the Volume for Ethereum by Month.

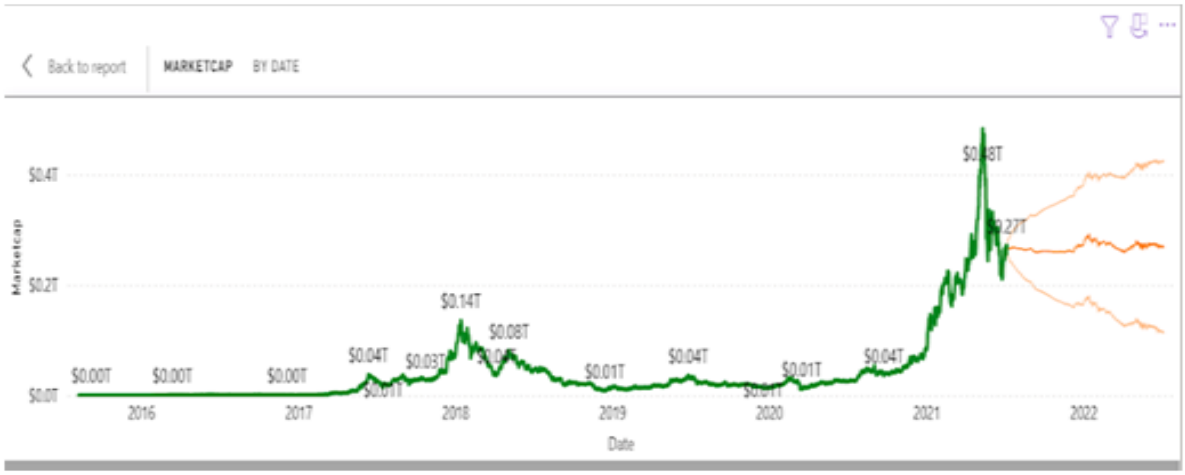
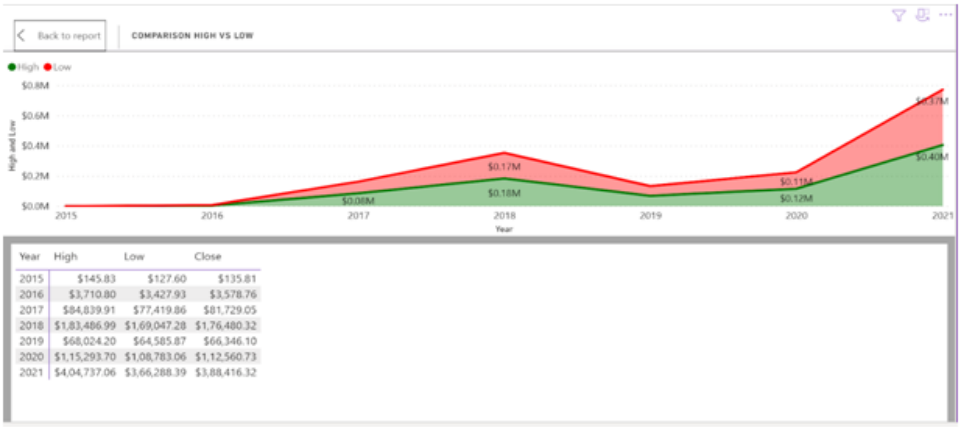


Fig. 2. MarketCap by Year - Ethereum/Solana

2) In the second line chart we have shown the MarketCap by Year and added a forecasting line which Predicts/Show how much it will grow over the next 12 months. It will show the lowest market cap and the highest it would go. So, the trend line would set expectations of those who wish to buy it.

Fig. 3. KPI's of Ethereum and Solana



Year	High	Low	Close
2015	$145.83	$127.60	$135.81
2016	$3,710.80	$3,427.93	$3,578.76
2017	$84,839.91	$77,419.86	$81,729.05
2018	$1,83,486.99	$1,69,047.28	$1,76,480.32
2019	$68,024.20	$64,585.87	$66,346.10
2020	$1,15,293.70	$1,08,783.06	$1,12,560.73
2021	$4,04,737.06	$3,66,288.39	$3,88,416.32

Fig. 4. Comparison Highest it went vs Lowest it

Fig. 4. Highest vs Lowest values

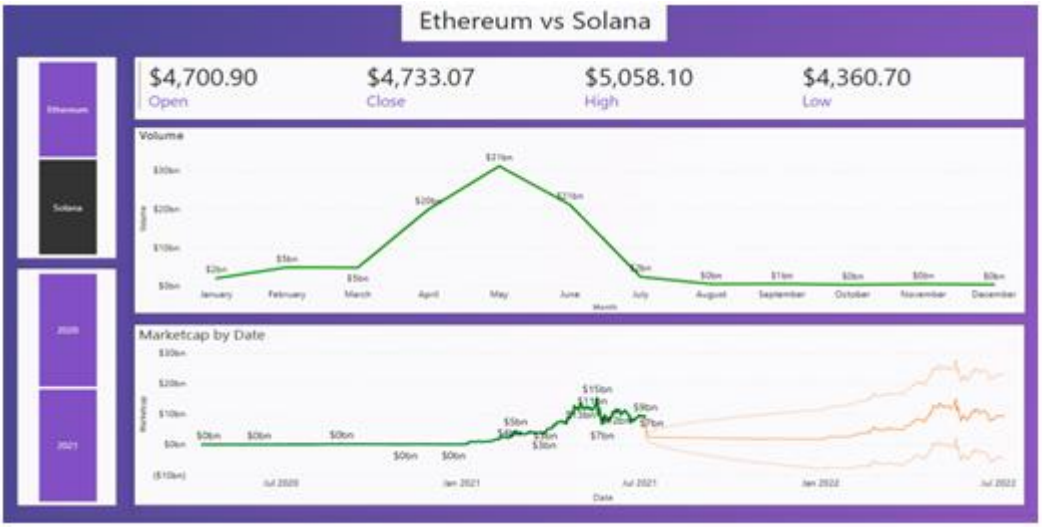
The stacked area chart shows the comparison for Ethereum & Solana for High vs Low over the years. The green color shows Highest value of Ethereum/Solana as selected in the slicer over that specific year and the red color shows the Lowest value.

Month Name	January Open	January Close	February Open	February Close	March Open	March Close	April Open	April Close	May Open	May Close	June Open	June Close	July Open	July Close
Ethereum	$79,795.29	$80,692.76	$83,089.80	$83,006.24	$83,902.77	$83,895.08	$95,222.64	$96,468.22	$1,35,801.22	$1,35,933.50	$1,11,309.80	$1,10,859.46	$50,770.47	$50,7

Fig. 5. Open vs Close

This is the Impact Bubble Chart which shows Open and Close of the respective Bitcoin by Month as selected in the slicer for the specific bitcoin. As we click on play the impact bubble goes according to it and if we hover over it, it shows the highest open and close value for that month.

The Marketcap of the Solana and Ethereum in another month is shown in the following figure. The curves of the graph show the variation in both currencies on the different month.



X. CONCLUSION

In the realm of Blockchain, Solana has the tag of most versatile and first genuinely web-scale Blockchain, as it's one of the few protocols achieving over 1,000 TPS. On the current testnet, Solana group professes to help north of 50,000 TPS, with more than 200 hubs. Presently as per this, it makes Solana one of the most performant Blockchain networks contrasted with different frameworks that work over the Proof-of-Work component.

XI. REFERENCES

[1]. DeVries, Peter. (2016). An Analysis of Cryptocurrency, Bitcoin, and the Future. International Journal of Business Management and Commerce. Vol. 1. Pages 1-9.

[2]. U. Khan, Z. Y. An and A. Imran, "A Blockchain Ethereum Technology-Enabled Digital Content: Development of Trading and Sharing Economy Data," in IEEE Access, vol. 8, pp.217045217056,2020.

[3]. Oliva, Gustavo & Hassan, Ahmed E. & Jiang, Zhen. (2020). An Exploratory Study of Smart Contracts in the Ethereum Blockchain Platform. Empirical Software Engineering. 25. 10.1007/s10664-019-09796-5.

[4]. Mubarak, Mohammed. (2021). "A Study on Cryptocurrency in India".

[5]. Fauzi, Muhammad & Paiman, Norazha. (2020). Bitcoin and Cryptocurrency: Challenges, Opportunities and Future Works. Journal of Asian Finance Economics and Business. 7. 695-704. 10.13106/jafeb.2020.vol7.no8.695.

[6]. Vujičić, Dejan & Jagodic, Dijana & Ranđić, Siniša. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. 1-6. 10.1109/INFOTEH.2018.8345547.

[7]. Sarita Kumari , “A Research Paper on Cryptography Encryption and Compression Techniques”,Volume 6 Issue 4 April 2017, Page No. 20915-20919(2017, April).

[8]. Khan, S.N., Loukil, F., Ghedira-Guegan, C. et al. Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Netw. Appl. 14, 2901–2925 (2021).

[9]. Alharby, Maher & Aldweesh, Amjad & van Moorsel, Aad. (2019). Blockchain-based Smart Contracts: A Systematic Mapping Study of Academic Research (2018).

[10]. Huang, Yuxin & Wang, Ben & Wang, Yinggui. (2021). Research and Application of Smart Contract Based on Ethereum Blockchain. Journal of Physics: Conference Series. 1748. 042016. 10.1088/1742-6596/1748/4/042016.

[11]. Mishra, Raaj & Kalla, Anshuman & Singh, Nimer & Liyanage, Madhusanka. (2020). Implementation and Analysis of Blockchain Based DApp for Secure Sharing of Students' Credentials. 10.1109/CCNC46108.2020.9045196.

[12]. Ch. Rupa, Divya Midhunchakkaravarthy, Mohammad Kamrul Hasan, Hesham Alhumyani, Rashid A. Saeed. Industry 5.0: Ethereum blockchain technology based DApp smart contract[J]. Mathematical Biosciences and Engineering, 2021, 18(5): 7010-7027.

[13]. Herrera-Joancomartí, Jordi. (2014). Research and Challenges on Bitcoin Anonymity. 8872. 10.1007/978-3-319-17016-9_1.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

IoT Device: 'NUTRIO' An Allergy Detecting Device

Vaishnavi Yavagal[1], Shruti Shirke[1], Anujna Patwardhan[2], Ganesh Jadhav[3]

[1]Department of Product Design, School of Design, Dr. Vishwanath Karad MIT World Peace University Pune, Maharashtra, India

[2]Department of UX Design, School of Design, Dr. Vishwanath Karad MIT World Peace University Pune, Maharashtra, India

[3]Assistant Professor, Department Product Design, School of Design, Dr. Vishwanath Karad MIT World Peace University Pune, Maharashtra, India

ABSTRACT

Background: The complexity of food items makes the process of allergy detection a tedious process. Existing Products mainly focused upon detecting 1-2 allergens in the food and not an overall detection of all the major allergens & nutrients in the food. Limiting the detection to one allergen limits the user as well. Existing products require adding the sample of food into the device and then clean the device after every use. This makes it a problem for the user to test every food item while they are outside.

Objective: As per various food categories, there are many devices and methods which detect a particular allergy. However, our study focuses on identifying multiple food categories and allergens at a micro level, within a single device. It will make use of biosensor as a method of detection of micronutrients in complex food items.

Methods: Interviews with a few doctors and medical professionals along with a survey among the target group of people were conducted.

Results: We conducted a survey of potential people suffering from various allergies along with doctors and laboratory personnel. Based on the questionnaire we identified that many existing devices fail to deliver in terms of affordability, maintenance, portability, ease of use and giving quick results, all in a single device.

Conclusion: The proposed design intervention was shown to several medical professionals and they have shown their wide acceptance towards this design.

Keywords— Food allergy, Food intolerance, Gender, Histamine, Biosensor, Portable device.

I. INTRODUCTION

Food Allergy is a reaction of the immune system when the foodeaten is not suitable to the body's digestive system. (13) Diarrhea, abdominal pain, rashes, itchiness, dizziness, fatigue, etc are some of the common symptoms of food allergy.Studies show that up to 3 percent of Indians have food allergies.Most of the food allergies are caused

due to peanuts and eggs inIndia. (4)It is considered to be type 1 hypersensitivity. It is a condition when certain allergens in food trigger the immune system causing discomfort. Food Allergens are difficult toidentify due to the complexity in food preparation. Food Allergy in India is observed to be quite prevalent as there are more than10 million cases per year. Food allergy is suffered more by females than by males as the anaphylaxis and histamine hormones are responsible after puberty. (13)Most common foodallergies include tree-nuts, shellfish, eggs, wheat, soy, peanuts,gluten, lactose. Lifestyle factors and unhealthy eating habits aremain reasons for provoking food allergies. Medication and clinical tests are temporary solutions since there is no permanentcure. There is also a high risk of allergens getting accidently exposed from adulterated products , unknown substances or even cross contamination. Many people have multiple food allergies because of cross reactivity, which occurs when antibodies against one allergen recognise a structurally related epitope of another similar allergen.(3) Given the cross-reactivityof allergens, it is almost certain that a device that can detect multiple allergens in a single sample will be developed, savingtime and money. (3) As the quality life of children and adults gets affected so this can be reduced by using allergy detecting devices. (21)There are various methods through which Food allergies are detected for e.g. Oral food challenge, skin prick test,blood tests etc. Such devices are mainly used by the doctors orin the pathology labs. But these devices or methods are not easilyavailable to the man who is prone to allergies at any time of theday. During our field survey, it was found that with respect to these allergens, which brought about many design interventionsand products into the market focusing mainly on one or two allergens.

1.1. Types of Food Allergy Tests:

Fig. 2.1.1 Skin prick test (22)

Fig.2.1.2 Oral food challenge test

Fig. 2.1.3 Blood test (24)

1.2. BIOSENSORS :

The biosensors are analytical devices that include a sensor system and a transducer, as well as other biological detecting elements. (26) When compared to any other currently availablediagnostic instrument, these sensors are superior in terms of selectivity and sensitivity. These Biosensors' principal uses arein environmental pollution management, agriculture, and the food industry. Durability ,price , susceptibility and reproducibility are the primary features of biosensor.(10)

A biosensor is the abbreviated form of the term biological sensor. An enzyme, nucleic acid, or antibody could be used as abiological element in this sensor. The bio-element communicates with the analyte under investigation, and the biological response can be converted into an electrical signal viathe transducer. (27) Biosensors are classed as resonant mirrors,immunological systems, chemical canaries, optrodes, bio-computers, glucometers, and biochips, depending on theirapplication.

1.3. Types of Biosensors

- Electrochemical Biosensors
- Amperometric Biosensors
- Blood-glucose biosensor
- Potentiometric Biosensors
- Conductometric Biosensors
- Optical Biosensors
- Fibre optic lactate biosensor
- Optical Biosensors for Blood Glucose
- Luminescent biosensors to detect urinary infection(10)

II. LSPR-BASED COLORIMETRIC BIOSENSING

A promising solution for improving food quality and safety is the LSPR-based colorimetric biosensing platform. This sensing technique lends itself easily to further development onfield-deployable platforms such as cellphones for onsite and end-user applications, (18) thanks to improvements in nanotechnology. Using this biosensor for a product makes a lot of sense as it's used for food monitoring. LSPR-based detection is more easily downsized, allowing for higher detection throughput and lower operational expenses.

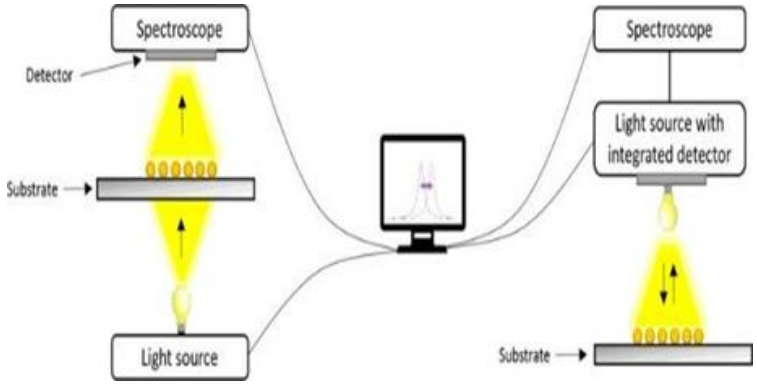


Fig. 2.4.1(25)

III. METHODOLOGY

3.1 Selection of Subjects for the Survey:

Inclusion criteria for the survey consisted of people who have or want to stay aware about food allergies. The survey wasconducted for an age group between 20-60 years. This survey was conducted over a period of 1 month and was taken throughan online mode, by sharing a google form link.

3.2 Questionnaire for Sample space:

The categories for the age group were, 20-30, 30-40 and 40+ years respectively. The gender of the user study was askedto specify. For the determination of the food allergy among thesubjects, they were asked about their current allergies with pre specified categories including egg, milk, fish/shellfish, soy, peanut, gluten and tree-nuts. If a family member has a food allergy, they were asked to share their experiences in detail.

The survey form consisted of a multiple choice question regarding the reaction that occurs due to this allergy, which includes vomiting, swelling, runny nose, dizziness, diarrhoea, itchy mouth and other if any. They were asked that when they are away from home, do they have a method to determine if food is allergen free. How often does one take a rapid detection test for detection of food allergy, specifying to choose if daily, weekly, monthly, a few times a year or never. What problems do you face when you go outside to eat? Overall how knowledgeable do you find the food service providers to know about food allergens or ingredients? Most importantly they were asked if a device or test that rapidly detects allergens in the food, would it be useful. If yes then what features would you be looking for in the device?, Selecting from portable, affordable, maintenance, ease of use or other.

3.3 Interview Questions for Doctors or Medical practitioners:

These below are the interview questions asked to family doctors.

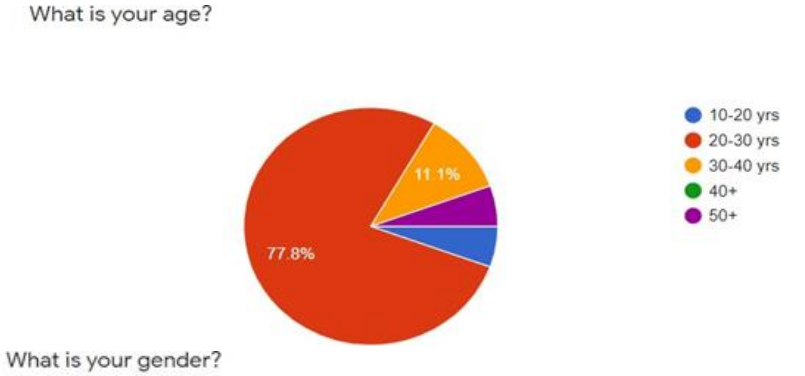
- Do you treat food allergy patients ? If yes , what is the ratio of those patients ?
- What type of food allergy do the patients usually have ?
- What kind of medication do you give to these patients ?
- How do you identify which kind of food allergen it is ?
- Are people usually aware about the cause of food allergy ?
- What kinds of tests are available to identify the allergens?
- At what point do you think it is necessary to take a test?
- Do you think these tests are handy and useful?

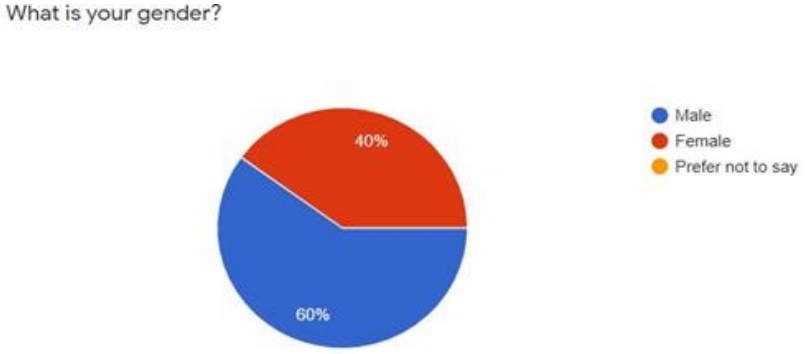
- I would also like to ask if you think a test that rapidly detects allergens in cooked foods be useful?

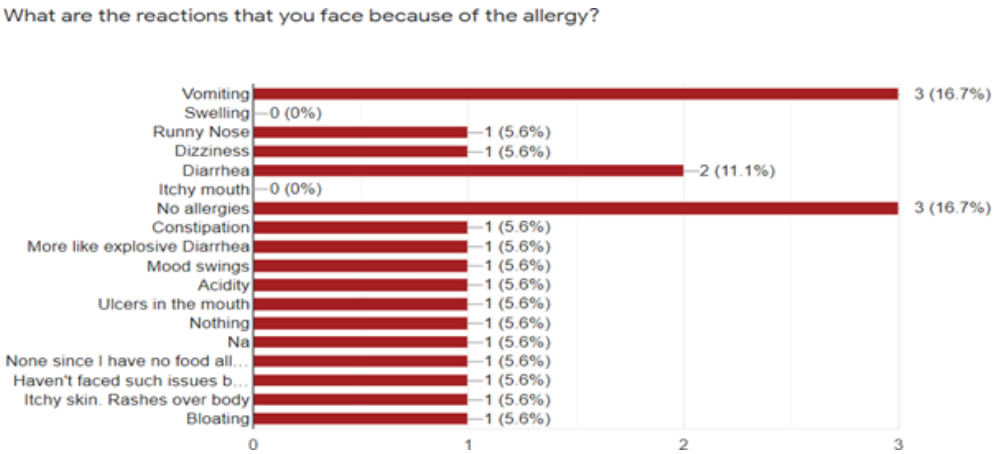
IV. RESULTS

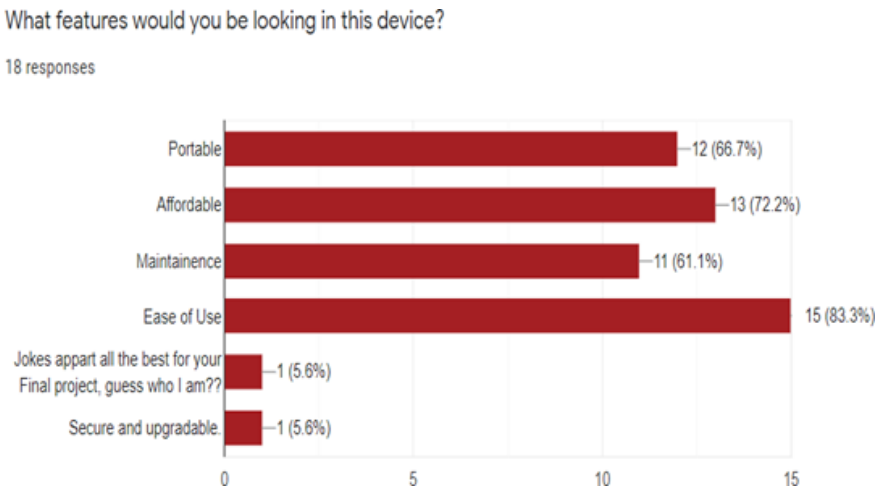
4.1 Primary Analysis (Survey Results)

From the survey, the requirements of the target users were briefly studied. It was found that many people are not aware about food allergies. Although the people who have these food allergies, face a lot of problems when their routine depends upon outside food. Even though the ingredients of the food items can be found out through the menu or by asking the waiters, the complexity of food preparation makes it difficult to find out the precise allergens in the food. Another finding indicated that many people are unaware or do not have the access to any portable devices that they can carry with them for everyday use. The need for a device that gives fast and precise results is seen to be increasing. Something that can be travel friendly and that helps avoid frequent visits to the hospital due to severe allergic reactions, is the preferred response by the target study.







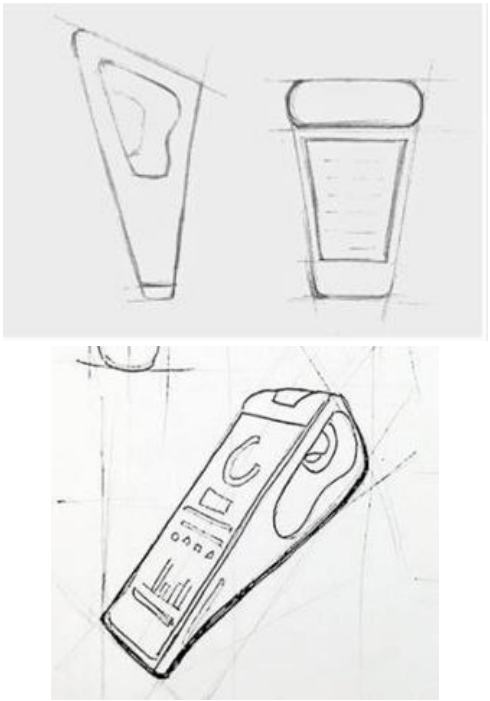


4.2 Interview Questions Results:

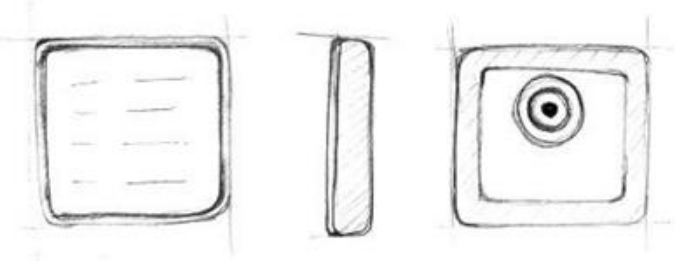
He answered saying that he roughly treats around 1 in 25 allergy cases at his clinic . Lactose, Nuts, Eggs, Sea Food, Foods having artificial colours, Fenugreek , Capsicum, cheese , paneer are some of the causes of the food allergy he mentioned. He treats them with homeopathy medicines and to observe the condition of the patient he tells them to keep a food diary . In this food diary he tells the patients to note down all the ingredients of the meals they had in a day and see what reaction the body is having after every meal , so accordingly this will help to detect which food item is causing the reaction to the immune system . But as he mentioned this is a long process and sometimes even after keeping a diary it becomes hard to find the allergen so if the medicine fails to provide relief within a span of 4 weeks he recommends the patients to take the food allergy test done on blood sample . He also said that these tests are comparatively costly .

4.3 Pugh Matrix:

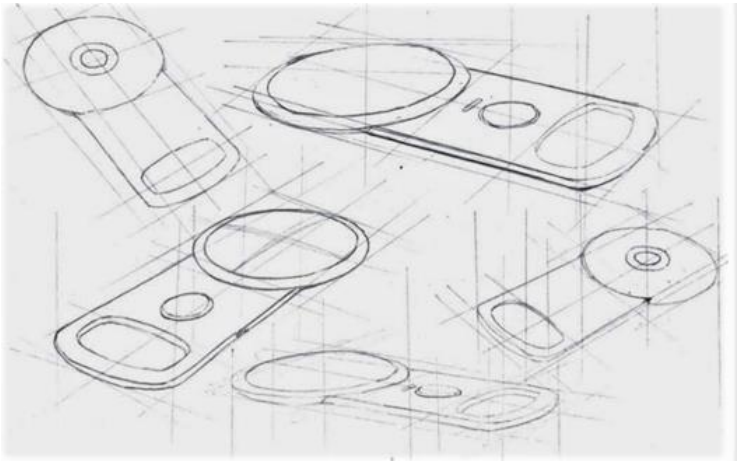
Concept 1



Concept 2



Concept 3



4.3.1. Our Main Attributes:

1. Ease of Use:

More clients will be attracted to your product, service, application, or programme if it is simple to use. You are more likely to attract a far wider spectrum of clients if your product is simple to use and further information and assistance is readily available. The product is handy and the interface is also user friendly.

2. Affordable:

The cost of the product is comparatively low and the product is designed with the view to keep the product affordable.

3. Maintenance:

Maintenance is less as the product is handy and can be even used as a keychain. The product is small and can be carried around in pocket as well.

Criteria	Concept 1	Concept 2	Concept 3
Ease of use	-1	0	+1
Affordable	0	+1	+1
Battery Life	+1	0	0
Maintenance	0	+1	+1
Net Score	0	+2	+3

4.3.2. Product Details -

While a lot of people suffer from food allergies all over the world; very few are aware & actually take precautions while eating. Most of them face problems when they go out to eat and are unable to track the allergens present in the food. The goal is to help people detect the allergens from the food that is kept in front of them within a few minutes.

4.3.3. Existing Solutions: -

Existing Devices are mainly focused upon detecting 1-2 allergens in the food and not an overall detection of all the major allergens & nutrients in the food. Limiting the detection to one allergen limits the user as well. Existing products require adding the sample of food into the device and then clean the device after every use. This makes it a problem for the user to test every food item while they are outside.

4.3.4. Our Solution: -

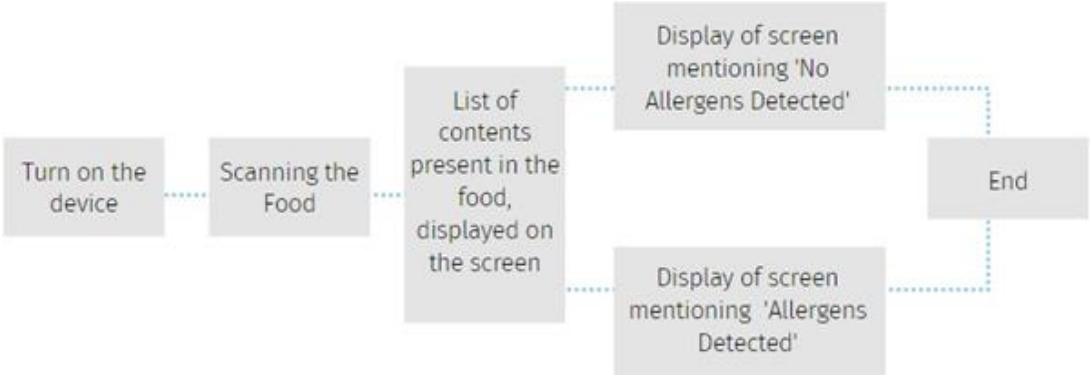
Our device uses a biosensor to detect the allergens in the food. One just needs to place the dish in front of the device and within a few moments, the device will provide you with a list of nutrients in the food and give you an alert if there are any allergens present. This makes the device user friendly as it requires very low maintenance, it gives quick results and mainly it can be used to detect variable allergens. Being a portable device makes it easy to carry it anywhere, which can fit in one's pocket. This device will reduce the stress of people who have to eat outside food and are unclear of the ingredients present in their food.

4.3.5. Working: -

When you start the device by clicking the power button , the device will be ready to quickly scan the food through its optical sensors and the ingredients and the molecular make–up of the foodstuff will appear on the screen.

You can save the ingredient you are allergic to with the help of the app that you can install on your respective phones and the device will warn you if it's safe to eat the dish you just scanned!

4.3.6. Use Case Diagram:



4.3.7. SWOT Analysis:

4.3.8. User Selling Point: -

The device uses an optical biosensor which detects all the ingredients from the food & classifies them into allergens and nutrients, just by scanning the food on the table. It's portable, sleek, reusable, affordable and fits in your pockets! Detection of variable allergens makes it a unique product.

4.3.9. Materials: -

- Main Body - Aluminium Body with a thin anodizedoutside layer for extra protection

- Scanner - Sapphire glass (It's a synthetic material covering the lens, which is very hard & protects themain scanner)

- Display - LCD screen for the display

Cost of materials:

MATERIALS	COST
Bending Toughened Glass	₹650/- Sq. ft
Pinhole Lens	₹229/ Piece
LCD Touch Screen	₹8,000/-
Cold Rolled Rectangular Embossed Aluminium Sheet	₹200/- Kg
Arduino Mega Board	₹1/- Piece
Plastic Buttons	₹150/- Packet(s)
Mini LED Light Bar	₹3,500/- Unit

Approximate Cost: 12,730

V. CONCLUSION AND FUTURE PLAN

Hence to conclude, our product can be very useful and handy to all the people facing food allergies. This product will help them to analyze food allergens before having a meal. In the survey many of them quoted that they are unaware about theirown food allergies and it's sometimes difficult to find the allergen. They can rely on this device to find the allergen and the device can also be carried around anytime they want.

Our 5-year plan is to reach a wide base of customers, make collaborations with brands, introducing new features as per current trends. Our focus will always be to keep the product and its UI simple. We aim to study our competitors, testing &altering prototypes if needed and having a well-planned product launch which will keep us engaged for the next 5 years.

A. Impact :

As people will use this technology, they'll become more awareabout the allergies that their food contains. This will lower thecasualty rate in the hospitals and people will be more aware and take precautionary measures beforehand. Hence this product will help people in staying healthy.

B. Commercialization :

Making videos on how to use the product, it's display, customer reviews. Giving out free demos at clinics and hospitals & asking doctors to recommend the product. Puttingcompulsory ads that run on YouTube and chrome and also advertising on hoardings with launch offers and discounts. Wewill also make the product available on Amazon and Flipkart for more reach to online customers.

VI. ACKNOWLEDGMENT

PROF. GANESH JADHAV AND PROF. SAI OJHA ARE TO BE THANKED FOR THEIR HELP AND PERSISTENT GUIDANCE IN THE RESEARCH OF THIS ARTICLE. THE AUTHORS WERE IN CHARGE OF PERFORMING RESEARCH ON THE TOPIC, CONDUCTING USER
SURVEYS, ANALYSING THE DATA, AND FINALISING THE DESIGN.
THE FINAL RESEARCH PAPER WAS APPROVED BY ALL OF THE AUTHORS

VII. REFERENCES

[1]. https://sci-hub.hkvisa.net/10.1038/nrdp.2017.98
[2]. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5940350/
[3]. https://link.springer.com/article/10.1007/s00216-018-0989- 7#Sec18
[4]. https://www.sciencedirect.com/science/article/pii/S221418041730 1137
[5]. https://sci-hub.hkvisa.net/10.1016/j.jaci.2009.08.028
[6]. https://www.nature.com/articles/s41598-021-00241-6
[7]. https://www.sciencedirect.com/science/article/abs/pii/S030881462 0325103
[8]. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5948517/
[9]. https://medicalfuturist.com/top-8-technologies-combating-food- allergy/
[10].https://www.elprocus.com/what-is-a-biosensor-types-of- biosensors-and-applications/
[11].https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4862100/#:~:text= Various%20types%20of%20biosensors%20being,and%20thermal%20and%20piezoelectric%20biosensors.
[12].https://www.tandfonline.com/doi/full/10.1080/15476910490919140
[13].https://www.mayoclinic.org/diseases-conditions/food- allergy/symptoms-causes/syc-20355095#:~:text=Food%20allergy%20is%20an%20immune,pro blems%2C%20hives%20or%20swollen%20airways.
[14].https://www.degruyter.com/document/doi/10.1515/almed-2020- 0051/html
[15].https://www.ift.org/news-and-publications/food-technology-magazine/issues/2020/january/columns/special-considerations- for-allergen-testing
[16].https://sci-hub.hkvisa.net/10.1016/j.jaci.2005.05.048
[17].https://www.elprocus.com/what-is-a-biosensor-types-of- biosensors-and-applications/
[18].https://www.biologydiscussion.com/enzymes/biosensors/biosenso rs-features-principle-and-types-with-diagram/10240
[19].https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4986466/#:~:text= An%20optical%20biosensor%20is%20a,a%20measured%20subs tance%20(analyte).
[20].https://www.sciencedirect.com/science/article/pii/S132389301500 146X
[21].https://medlineplus.gov/lab-tests/food-allergy-testing/
[22].https://fineartamerica.com/featured/7-allergy-testing-microgen- imagesscience-photo-library.html?product=poster
[23].https://trouver-un-metier.fr/wp- content/uploads/2019/11/puericultrice-enfant.jpg
[24].https://www.sheridanhospital.org/community/volunteer- opportunities/
[25].https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4986466/bin/bse0 600091fig5.jpg
[26].https://www.news-medical.net/health/What-are-Biosensors.aspx#:~:text=The%20term%20%E2%80%9Cbiosens or%E2%80%9D%20is%20short,electrical%20signal%20by%20th e%20transducer.
[27].https://www.mdpi.com/1424-8220/21/4/1109/htm

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Sentimental Analysis of Customer Reviews: By using Data Analysis

Vikas Shukla, Prof. Sachin Bhoite
School of Computer Science, MIT-World Peace University, Pune, India

ABSTRACT

Online shopping and e-commerce are an area that has experienced considerable growth over the last 5-6 Years. Sentiment analysis - this area of research attempts to determine the feelings, opinions, emotions, among other things, of people on something or someone. To work on this, we use new techniques NLP (Natural Language Processing) and machine learning algorithms. Reviews on product by customer make a big impact on sellers profit margin However, negative reviews can reduce the profits for companies as people become transparent in expressing their' opinions and post them online without considering the consequences the companies would face. To help the business owner we are going to do this project, in which we will be taking E-commerce website FLIPKART for our dataset and the product as headphones. Reading one by one reviews takes a lot of time, so what we will do is summarize the whole reviews into 3 points. For this we will be using Sentiment intensity analyzer algorithm. It is more efficient than any other algo like visualization or data mining.

Keywords— Data Science, Sentiment analyze, opinion mining, reviews, e-commerce, natural language processing, semantic analyze

I. INTRODUCTION

Now a days everyone buys items online on different e-commerce websites like flipkart, amazon, snapdeal and many more. In growing country like INDIA e commerce, play a big role and their business depends upon the reviews given by the customer. The sentiment is a feeling that expresses judgement, attitude or thought. Sentiment analysis, also known as opinion mining, studies people's sentiments towards certain entities.

In today's world reviews dropped by users on a certain product/item makes a big impact on the owner's business. It is practically not possible for seller to keep track and analyse all these feedbacks.

So basically, the main objective of this project is to analyse the sentiment of customers by reviews given by them on the review section.

We will use different libraries which are already defined in Python like PANDAS, SKLEARN, NLTK etc. The model we are going to use is in NLTK – sentiment intensity analyser. Usually, business owners read the reviews and takes a lot of time ten minutes to read 7-8 reviews which is not suitable but using this model we can read up to 15 thousand reviews in seconds and make a summary out of it. The motive of this study is to use Python and

to predict the sentiment of reviews and how this could deliver valuable information to the manager, how can you make the product better or what are the problems customer facing.

II. RELATED WORK

Various research and students have published related work in national and international research papers, thesis to understand the objective, types of algorithms they have used and various techniques for pre-processing, Feature.

Hanan Alasmari have used Tableau, Python & Knowledge discovery and data mining (KDD) is a common methodology, which refers to the overall process of detecting useful insights from a collection of data they said "It is true that it is possible to understand customers opinions towards products through the massive scale of unstructured text online that are also informal" [1]

Shweta Rana and Archana Singh used SVM, and Naïve Bytes techniques and they said "The future scope of the work is that we can explore our data to a wider genre of different products on social networking sites or e-commerce as day by day the user is moving online and they prefer buying stuff online so we can identify the accuracy rates of the products like books, games etc." [2]

Zied Kechaou, Mohamed Ben Ammar and Adel.M Alimi "Improving e-learning with sentiment analysis of users' opinions" Applying a sentiment analysis to examine the nature and the structure of web forums and e-learning blogs turns out to be an important endeavour; however, the current accuracy is promising for effective analysis of forum conversation sentiments. Such analysis can help provide a better understanding of users' opinions regarding the e-learning system for the sake of its improvement. [3]

"Sentiment Analysis and Opinion Mining: A Survey" G.Vinodhini, RM.Chandrasekaran. "The main challenging aspects exist in use of other languages, dealing with negation expressions; produce a summary of opinions based on product features/attributes, complexity of sentence/ document, handling of implicit product features , etc.". [4]

"Thumbs up? Sentiment Classification using Machine Learning Techniques" Bo Pang and Lillian Lee they said "The classification accuracies resulting from using only unigrams as features are shown in line (1) of Figure 3. As a whole, the machine learning algorithms clearly surpass the random-choice baseline of 50%." [5]

III. DATA SET DESCRIPTION

For this analysis, we will be using Flipkart Review dataset present on Kaggle. The dataset contains the reviews given by the users on a particular product named "BoAt Rockerz 235v2 with ASAP Charging".

IV. RESEARCH METHODS

Our methodology comprises of three sections –Data collection, Data pre-processing and VADER Sentimental Analyzer.

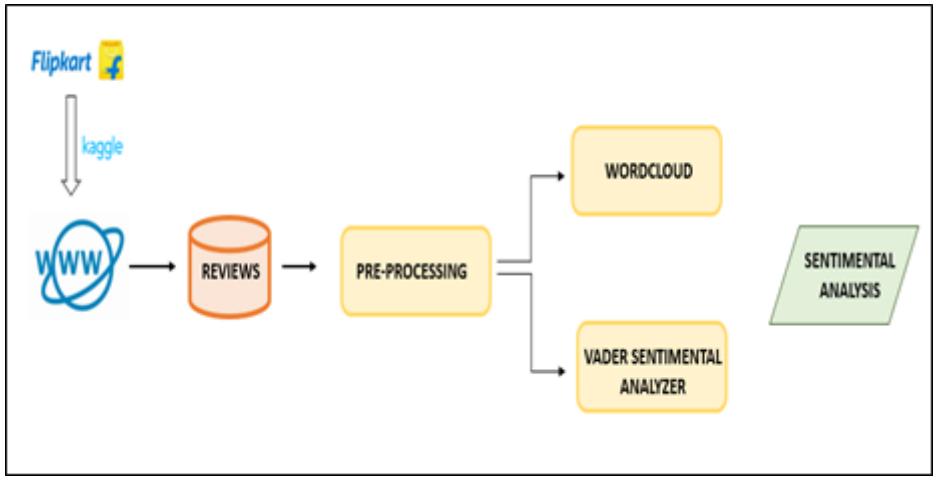


Fig. 1. Architecture of methodology to process reviews

A. Data Collection

In this section, we discuss the architecture framework and programming libraries we used in our experiment to pull and process the unstructured reviews from the Flipkart product page. To extract reviews from the products page we have used third party website Kaggle database which is a web application that exports stores different data to a comma-separated file (CSV).

Libraries used and a brief about them:

1. **NumPy**-NumPy is a library for the Python programming language, adding support for large, multi-dimensional arrays and matrices, along with a large collection of high-level mathematical functions to operate on these arrays. [7]
2. **Pandas**-Pandas is a software library written for the Python programming language for data manipulation and analysis. It offers data structures and operations for manipulating numerical tables and time series [7]
3. **Matplotlib**-Matplotlib is a plotting library for the Python programming language and its numerical mathematics extension NumPy. It provides an object-oriented API for embedding plots into applications using general-purpose GUI toolkits like Tkinter, wxPython, Qt, or GTK. [7]
4. **Seaborn**-Seaborn is a Python data visualization library based on matplotlib. It provides a high-level interface for drawing attractive and informative statistical graphics. [7]
5. **NLTK**-The Natural Language Toolkit, or more commonly NLTK, is a suite of libraries and programs for symbolic and statistical natural language processing for English written in the Python programming language. [7]
6. **WordCloud**-Word Cloud is a data visualization technique used for representing text data in which the size of each word indicates its frequency or importance. Significant textual data points can be highlighted using a word cloud. Word clouds are widely used for analysing data from social network websites. [7]

```
import pandas as pd
import seaborn as sns
import matplotlib.pyplot as plt
from nltk.sentiment.vader import SentimentIntensityAnalyzer
from wordcloud import WordCloud, STOPWORDS, ImageColorGenerator

Reviewdata = pd.read_csv("flipk.csv")
Reviewdata.head(10)
```

	product_id	product_title	rating	summ
0	ACCFZGAQJGYCYDCM	BoAt Rockerz 235v2 with ASAP charging Version ...	5	Terrific purch
1	ACCFZGAQJGYCYDCM	BoAt Rockerz 235v2 with ASAP charging Version ...	5	Terrific purch
2	ACCFZGAQJGYCYDCM	BoAt Rockerz 235v2 with ASAP charging Version ...	5	Sup
3	ACCFZGAQJGYCYDCM	BoAt Rockerz 235v2 with ASAP charging Version ...	5	Sup

Fig. 2. The Dataset overviews

B. Pre-Processing

- There are 1293 Attributes with null values, were dropped from location columns and were replaced with their upper attributes.

```
print(Reviewdata.isnull().sum())
```

```
product_id          0
product_title       0
rating              0
summary             0
review              0
location         1293
date                0
upvotes             0
downvotes           0
dtype: int64
```

Fig. 3. Null Values

- Cleaned the data which is not useful for us. Dropped the following columns: product_id, product_title, location, upvotes, downvotes.
- Removed all the symbols like ' "", . ! @' and converted all the text into lowercase.

```
Reviewdata['cleaned_summary']=pd.DataFrame(Reviewdata.summary.apply(cleaned1))
Reviewdata['cleaned_review'] = pd.DataFrame(Reviewdata.review.apply(cleaned1))
Reviewdata.head(10)
```

	rating	summary	review	cleaned_summary
0	5	Terrific purchase	1-more flexible2-bass is very high3-sound clar...	terrific purchase
1	5	Terrific purchase	Super sound and good looking I like that prize	terrific purchase
2	5	Super!	Very much satisfied with the device at this pr...	super
3	5	Super!	Nice headphone, bass was very good and sound i...	super
4	5	Terrific purchase	Sound quality super battery backup super quali...	terrific purchase
5	5	Wonderful	Wowwww it's amezing bluetooth nice look, nice ...	wonderful
6	4	Pretty good	Awesome colour! Amazing experience .. but only...	pretty good
7	5	Terrific purchase	For the first time, I am posting a review, jus...	terrific purchase

Fig. 4. Removing Symbols and converting to lowercase

C. Feature Selection

Let's start by deleting the unnecessary or redundant columns. For data analysis, we do not need the :

id , title , location , upvotes , downvotes :

Some of these columns may looks like they are important but all of them are not usable in the project . The columns being used are:

Ratings, summary , review and date .

```
Reviewdata['cleaned_summary']=pd.DataFrame(Reviewdata.summary.apply(cleaned1))
Reviewdata['cleaned_review'] = pd.DataFrame(Reviewdata.review.apply(cleaned1))
Reviewdata.head(10)
```

Fig. 5.

D. VADER(Algorithm)

We applied Valence Aware Dictionary and sentiment Reasoner or VADER library in python programming language to calculate the semantic score of each comment. The positive sentiment, negative sentiment and neutral were extracted from each sentence using NLTK in Python 3.5.1. This was completed by utilizing Naïve Bayes Analyzer module "it finds the probability of an event given the probability of another event that has already occurred.

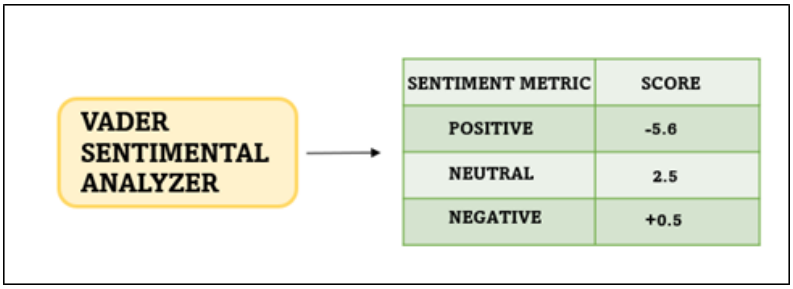


Fig. 6. Sentimental module uses VADER to calculate sentimental score .

V. EXPOLATORY DATA ANALYSIS

We predominantly used Python Libraries. Specifically, we used the Pandas Python Library, which is a data manipulation script . We used Pyplot for data visualization.

The Rating column of the data contains the ratings given by every reviewer. So let's have a look at how most of the people rate the products they buy from Flipkart:

A. Rating By Percentage

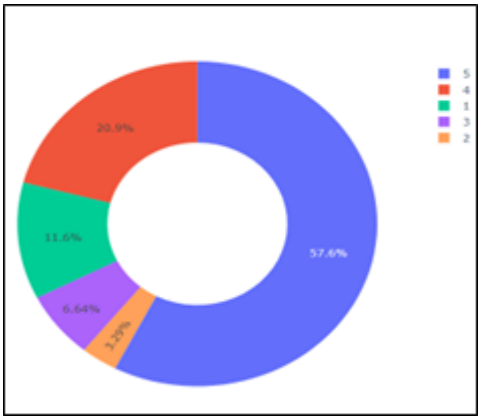


Fig. 7. Ratings in percentage

So 57.6% of the reviewers have given 5 out of 5 ratings to the products they buy from Flipkart.
Now let's have a look at the kind of reviews people leave. For this, I will use a word cloud to visualize the most used words in the review's column.

B. Word Cloud from Reviews

Fig. 8. WordCloud of the reviews written by user.

The bigger the size of word is visible the most it is used in the reviews.

C. Count of Ratings

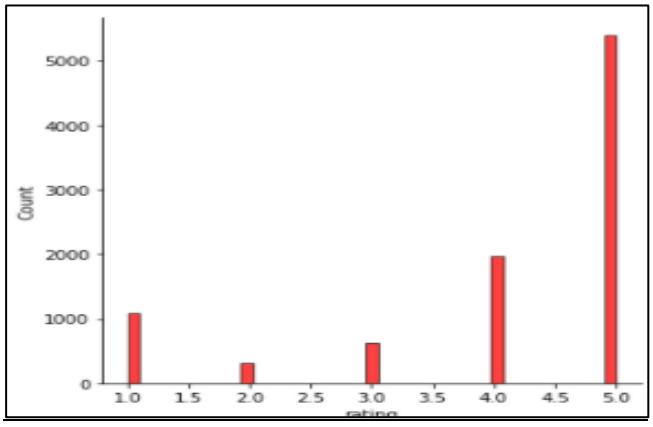


Fig. 9. Count of the rating.

As we can see in the above graph 5 star rating is given by more than 5000 customers and 1 star rating is given by 1000 plus customers.

D. Adding Column in CSV

Now I will analyse the sentiments of Flipkart reviews by adding three columns in this dataset as Positive, Negative, and Neutral by calculating the sentiment scores of the reviews:

```
[nltk_data] Downloading package vader_lexicon to /root/nltk_data...
```

	review	Positive	Negative	Neutral
0	1-more flexible2-bass is very high3-sound clar...	0.167	0.017	0.815
1	Super sound and good looking I like that prize	0.759	0.000	0.241
2	Very much satisfied with the device at this pr...	0.278	0.000	0.722
3	Nice headphone, bass was very good and sound i...	0.286	0.082	0.632
4	Sound quality super battery backup super quali...	0.600	0.000	0.400

Fig. 10.Positive , Negative and Neutral scores adding .

E. Word Cloud by One-star Reviews

Fig. 11. 1star rating reviews

Here we can see that words like ‘QUALITY’,’SOUND QUALITY’, ‘VOICE’ , ‘WORST’ and many more by this company can work on their products and analyse what’s the major problem customer is facing.

F. Word Cloud by five-star rating

Fig. 12. 5star rating reviews

VI. KEY FINDINGS

Now let's see how most of the reviewers think about the products and services of Flipkart:

```
x = sum(Reviewdata["Positive"])
y = sum(Reviewdata["Negative"])
z = sum(Reviewdata["Neutral"])

def sentiment_score(a, b, c):
    if (a>b) and (a>c):
        print("Positive 😊 ")
    elif (b>a) and (b>c):
        print("Negative 😠 ")
    else:
        print("Neutral 🙂 ")
sentiment_score(x, y, z)
```

```
Neutral 🙂
```

Fig. 13.The overall .

So most of the reviews are neutral. Let's have a look at the total of Positive, Negative, and Neutral sentiment scores to find a result about Flipkart reviews:

VII. RESULTS AND DISCUSSION

In this research we have considered a particular e-commerce website and a product. This will help business personals to open a new restaurant there. Such analysis is essential part of business. Having a prior idea about the product and how customer are feeling with that. So, most people give Neutral reviews, and a small proportion of people give Negative reviews. So, we can say that people are satisfied with Flipkart products and services. You can refer the word cloud –[Fig.11&12] to check what keywords are mostly used by customer and what are the defaults in the product. So, in future you can develop a more enhanced product

Various methods have been used to measure the performance. From the performance achieved by these methods it is difficult to judge the best choice of classification method, since each method uses a variety of resources for training and different collections of documents for testing, various feature selection methods and different text granularity.

For our research we have used Boat headphone as product and the scores from the reviews are like this :

```
print("Positive: ", x)
print("Negative: ", y)
print("Neutral: ", z)
```

```
Positive:  3439.9740000000415
Negative:  532.5680000000009
Neutral:  5401.457999999954
```

Fig. 14.Positive , Negative and Neutral scores.

VIII. CONCLUSION

Sentiment detection has a wide variety of applications in information systems, including classifying reviews, summarizing review and other real time applications. There are likely to be many other applications that is not discussed. Based on customer reviews. We concluded that the product is neutral. And for many customers it is positive also. By this a company can make their product more efficient. For future studies, this study could be extended to focus on integration of the sentiments found from the reviews with the tokens in each cluster. It is also recommended to use the sentiment analysis with the regression line as a dependent variable to investigate their causal relationship. The outcomes of this study could support Flipkart business managers to develop the usefulness of the product and enhance the way of marketing this product.

In future, more work needed in this field for further improving the performance measures . Sentiment analysis can be applied for new applications. Although the techniques and algorithms used for sentiment analysis are advancing fast, however, a lot of problems in this field of study remain unsolved.

IX. REFERENCES

[1]. "Sentimental Visualization: Semantic Analysis of Online Product Reviews Using Python and Tableau" Hanan Alasmari, IEEE ON BIG DATA VO., XX, NO., X, DECEMBER 2020.

[2]. "Comparative Analysis of Sentiment Orientation Using SVM and Naïve Bayes Techniques" Shweta Rana and Archana Singh, 2016 2nd International Conference on Next Generation Computing Technologies (NGCT-2016)

[3]. Zied Kechaou, Mohamed Ben Ammar and Adel.M Alimi " Improving e-learning with sentiment analysis of users' opinions "2011 IEEE Global Engineering Education Conference (EDUCON)

[4]. "Sentiment Analysis and Opinion Mining: A Survey" G.Vinodhini, RM.Chandrasekaran Volume 2, Issue 6, June 2012(ijarcsse)

[5]. "Thumbs up? Sentiment Classification using Machine Learning Techniques" Bo Pang and Lillian Lee

[6]. Flipkart Product Review (Naushad Shukoor)

[7]. Google Search (Definition)

[8]. Chafale, Dhanashri, and Amit Pimpalkar. "Review on Developing Corpora for Sentiment Analysis Using Plutchik's Wheel of Emotions with Fuzzy Logic. "International Journal of Computer Sciences and Engineering (IJCSE) 2 (2014): 14-18

[9]. J.Ortigosa-Hernández,J.D. Rodríguez, L. Alzate, M. Lucania, I. Inza and J.A. Lozano, Approaching sentiment analysis by using semi-supervised learning of multi-dimensional classifiers, Neurocomputing 92 (2012)

[10]. B. Keith, E. Fuentes and C. Meneses, A hybrid approach for sentiment analysis applied to paper reviews, 2017.

[11]. E. Boiy and M.-F. Moens, A machine learning approach to sentiment analysis in multilingual web texts, Inf. Retr. 12(5) (Oct. 2009), 526–558.

[12]. Tsur, D. Davidov, and A. Rappoport , " A Great Catchy Name: Semi-Supervised Recognition of Sarcastic Sentences in Online Product Reviews". In Proceeding of ICWSM. of Context Dependent Opinions,2010.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Securing Data During Transmission and Storage

Mr.Ashutosh Mane[1], Mr.Sujeet Patil[1], Mr.Akash Desai[1], Mrs.Madhuri Pote[2]
[1]MCA Student, School of Computer Science, MIT-World Peace University, Pune, Maharashtra, India
[2]Assistant Professor, School of Computer Science, MIT-World Peace university, Pune, Maharashtra, India

ABSTRACT

Shielding information from vindictive PC clients keeps on filling in significance. Regardless of whether forestalling unapproved admittance to individual photos, guaranteeing consistence with government guidelines, or guaranteeing the respectability of corporate insider facts, all applications require expanded security to shield information from skilled interlopers. In particular, as additional what's more documents are saved on circle the necessity to give secure capacity has expanded in significance. This paper presents a review of methods for safely putting away information, including hypothetical methodologies, model frameworks, and existing frameworks right now accessible. Because of the wide assortment of potential arrangements accessible and the assortment of methods to show up at a specific arrangement, it is critical to survey the whole field earlier to choosing an execution that fulfills specific prerequisites. This paper gives an outline of the unmistakable attributes of a few frameworks to give an establishment for settling on an educated choice. At first, the paper sets up a bunch of measures for assessing a capacity arrangement dependent on privacy, uprightness, accessibility, and execution. Then, at that point, utilizing these models, the paper clarifies the applicable qualities of select capacity frameworks and gives an examination of the significant contrasts.

I. INTRODUCTION

With the multiplication of put away information in all conditions, associations face an expanding prerequisite to both for a brief time and forever hold data. The capacity mechanism for lodging this data turns into a practical objective for assault by a pernicious interloper. Assuming that a pariah can effectively infiltrate the information stockpiling, the interloper might possibly acquire data that disregards protection, that uncovers important mysteries, or that forestalls the entrance of genuine clients; the injurious impacts of such an assault are really unquantifiable. On the off chance that the association goes to no capacity security lengths, the information store turns into a rewarding single mark of assault for a gate crasher. The aversion of this clearly ominous condition has produced a definite field of PC research.

Colleges have effectively sought-after choices for getting put away data, and have thusly created numerous likely plans for guaranteeing data classification, respectability, and accessibility without considerably debasing execution. See Figure 1 for a social outline of continuous examination. A significant issue related with putting

away a lot of information is the means by which to appropriately gauge the expenses and advantages related with safety efforts. The most solid frameworks are so a result of the expanded measures to ensure the information, however each extra measure accompanies an expense as far as both comfort and handling time. To successfully select the best security, conspire, clients should have a comprehension of the essential security highlights accessible in the capacity security local area and afterward have the option to quantifiably analyze the frameworks. Fostering a comprehension of these angles will help to inspire the course for future exploration and help the choice of the suitable capacity answer for a bunch of explicit prerequisites. The further paper follows. Segment 2 gives a normalized set of rules to assess secure capacity frameworks. Area 3 gives a review of eight stockpiling frameworks. Segment 4 gives an order and examination of the reviewed frameworks, and Section 5 closes.

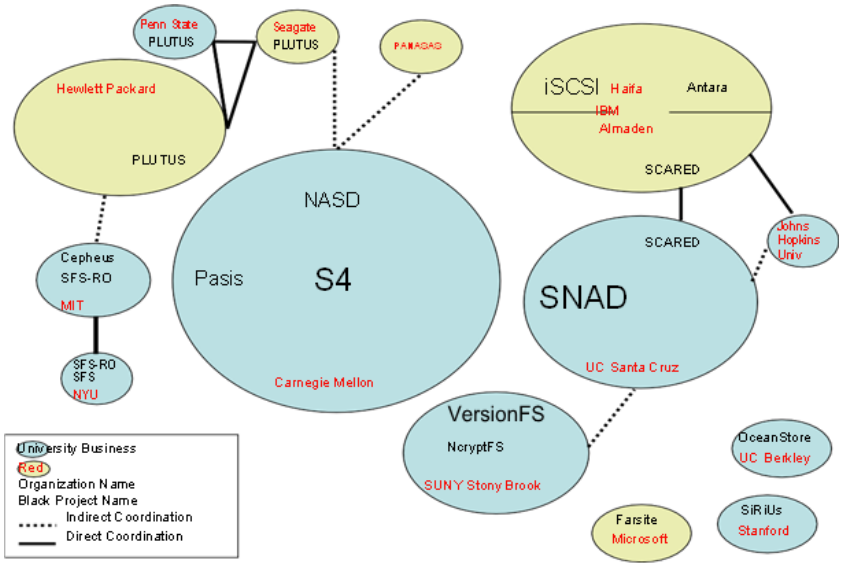


Figure 1. Relational diagram

II. CRITERIA FOR EVALUATION

This part builds up a typical arrangement of measures for assessing a capacity security framework. There are various ways of moving toward capacity frameworks however for the reasons of setting up a typical reference, secrecy, uprightness, accessibility, and execution have been chosen. While this paper doesn't move toward any measures in comprehensive detail, it is important to portray the assessment measures preceding surveying the individual frameworks. Confidentiality, integrity, and availability are generally referred to in the PC security field, and execution was added to guarantee frameworks accomplish an proper harmony among security and handling capacity. Before examining each angle in more detail, it is vital to comprehend that none of these traits is fundamentally unrelated, and, truth be told, to have a safe framework all attributes should be fulfilled.

A. Confidentiality

According to a security viewpoint, guaranteeing secrecy suggests that nobody has admittance to information except if explicitly approved. Various frameworks control this approval process in different ways. The initial phase in approving admittance to data is to appropriately distinguish clients by means of verification. The capacity framework should characterize the means for a client to be appropriately recognized before obtaining

entrance, and afterward having properly distinguished a client, the framework should permit admittance to just determined information related with that client. Appropriate approval to get to the capacity framework doesn't suggest admittance to the whole framework, indeed, the differentiating rule of least honor is for the most part applied. Information proprietors must, in any case, have a technique for permitting others to get to data when proper through an appointment of approval conspire.

As well as overseeing approval to information, privacy additionally suggests that the framework should encode information to forestall data assaults. Along these lines, the framework must require either clients or servers to apply cryptographic keys. The contrasting plan choices between client oversaw and cut off oversaw keys altogether affect the general stockpiling method. To share data, various clients should have admittance to the suitable keys - regardless of whether a brought together gathering waiter gives out keys or individual document proprietors give the keys to extra clients, the consequences for execution also client comfort should be broke down. The conversation of key administration in this paper isn't planned to detail cryptography, however a comprehension of how keys are circulated also applied is fundamental for understanding the bigger framework. Since the cryptographic tasks are frequently the most computationally costly part of getting to safely put away information, seeing how a specific framework oversees keys is proper.

An extra basic conversation concerning key administration includes how keys are denied. When a proprietor or director decides to renounce a specific client's admittance to information, the keys that the client had should never again permit admittance to the framework, or on the other hand if they do they should not permit admittance to future renditions of the documents. The expense related with denying a client shows itself in the re-encryption exertion needed to get classification. It is absurd to actually renounce a client's keys to forestall that client's capacity to perform activities since duplicates might have been delivered, so the framework must render all keys of a denied client old and yet again encode each of the information with another key.

A subsequent contention then, at that point, turns, indeed, to a tradeoff among security and execution. There are two essential techniques for getting the information after key disavowal: lethargic or forceful disavowal. When utilizing lethargic disavowal the framework doesn't reencrypt the information that the repudiated client recently had approval to access until the next legitimate client endeavors to get to the document. This basically settles the expense over the long run, yet it leaves information powerless against the renounced client for an undefined timeframe. By contrast, forceful denial quickly re-encodes all documents that the disavowed client might actually get to. When re-encoded, new keys should be appropriated to all faculty who are impacted by the changed encryption (adding extra weight to the key dispersion conspire); obviously this choice requires time. Sluggish re-encryption penances a proportion of safety to save time while forceful disavowal penances time to improve security.

B. Integrity

Integrity is a comprehensively based point that remembers keeping up with information consistency for the face of both incidental and noxious assaults on information. For the reasons for this paper, the extent of the trustworthiness investigation is restricted to the techniques used to forestall noxious change or annihilation of data. The subsequent assumption is that when a client gets to put away data, no information has been exposed to unapproved alteration. Numerous frameworks authorize honesty by guaranteeing that information comes from the normal source. For put away information, the conversation of honesty infers that records have not been changed on the plate.

Integrity authorization systems fall into two classifications: information adjustment avoidance and information adjustment discovery. Like secrecy, adjustment avoidance expects clients to get approval preceding changing records and requires that documents are just different in a supported way. Honesty changes from secrecy in that secrecy is just stressed over whether or not information has been compromised, though trustworthiness incorporates guaranteeing the accuracy of the information. Recognition plans

C. Availability

The paper thinks about availability as far as time, space, and portrayal. Data should be accessible to an approved client inside an OK time span, without hoarding the accessible extra room, and in a justifiable portrayal. A framework can not permit an enemy to forestall approved admittance to data through a refusal of administration assault.

It is essential to take note of that the objectives of availability struggle to a degree with those of confidentiality; the two should be considered inside the security space.

D. Performance

The degree of safety and the framework execution regularly struggle. To give the essential layers of safety to keep away from unsafe assaults, the framework execution endures. The two objectives of a productive framework and a safe climate inherently struggle. Each extra safety effort requires computationally costly handling that reduces the framework's capacity to perform different tasks; all security measures are overhead for the framework. Every one of the assessed stock methods endeavours to limit the exhibition cost related with the specific proportions of the framework. The most prevailing presentation cost is related with encryption because of its computationally costly nature. The two generally various ways to deal with capacity security, encode on-wire and scramble on-plate, place the weight of encryption on various parts of the framework. Riedel et al [25] give a definite clarification of the trade-offs between the two.

III. SURVEY

The following survey briefly describes several storage security approaches using confidentiality, integrity, availability, and performance as a framework. Sections 3.1-3.3 refer to encrypt on wire systems and Sections 3.4-3.8 refer to encrypt on disk systems.

A. NASD – Network Attached Secure Disks.

In customary appropriated record frameworks, a customer needing to get to information should make a solicitation to the record server. The server then, at that point, should check the customer's approval and disseminate the document on the off chance that the suitable rules are met. Since the server should cooperate with each record access demand for each customer, the server can immediately turn into a bottleneck.

NASD's essential objective is to mitigate the server bottleneck by communicating with a client one time giving a "capacity key." With the ability key the client can get to the suitable disk(s) straightforwardly with next to no further waiter communication. The actual plates should be "canny" with the end goal that they have sufficient inward capacity to process the capacity key and handle record access demands straightforwardly [10,11].

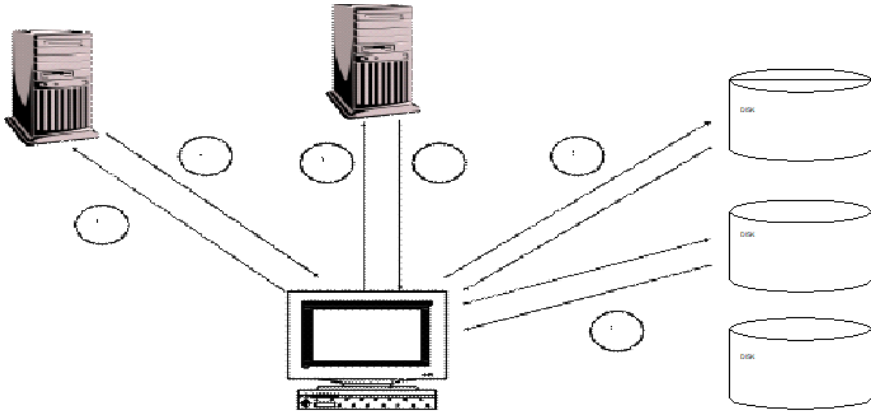


Figure 2. NASD

Confidentiality: There are two servers in the NASD plan, one to give validation and afterward the genuine record server. NASD doesn't indicate the validation plot and prescribes utilizing any current strategy like Kerberos. Endless supply of verification, a client sends a solicitation to the record server. The server confirms the genuineness of the solicitation and afterward furnishes the client with an ability key that relates to the client's freedoms for record access. Subsequent to acquiring the capacity key, a client can discuss straightforwardly with the information circle for all future access demands during guaranteed meeting. The capacity object is the basic perspective relating to both the privacy also respectability of the framework. A document chief consenting to a customer's entrance demand secretly sends a capacity token and an ability key to the customer; together these structure a capacity object. The token contains the entrance freedoms being conceded for the solicitation and the key is a message verification code (MAC) comprising of the abilities and a secret key divided among the document server and the real plate drive. Customers can then make an immediate solicitation to a NASD drive by giving the capacity object. The drive then, at that point, employments the mystery key that it imparts to the document server to decipher the capacity token to check the client's entrance privileges and administration the solicitation. Since the MAC must be deciphered utilizing the drive/server shared mystery key, any alterations to the contentions or bogus contentions will bring about a denied demand.

Integrity: The clever idea related with NASD is setting part of the information uprightness necessity on the actual circles. The "shrewd" circles decipher the abilities objects, encode information, and communicate results to customers. To guarantee honesty on the customer end, the plate utilizes the very hash MAC blend that permitted it to approve a customer access to scramble and send the information to the customer. The customer can then confirm the uprightness of the transmission during the unscrambling system.

Availability: The way that NASD permits direct admittance to the plate advances adaptability; the framework throughput scales straightly with the quantity of customers and circles. Notwithstanding, since the record server should be trusted to at first give ability keys, the server presents a solitary mark of assault. Assuming the server becomes compromised it is absolutely impossible to forestall a forswearing of administration assault.

Performance. A rousing component for utilizing NASD is the capacity to scale data transmission directly with the quantity of circles in the framework, in any case, these advantages are to some extent balance by the expense of cryptography. A huge presentation issue related with NASD is the double expense of cryptographic activities caused due to the encode on-wire plot. Each datum transmission should be scrambled preceding being sent and afterward unscrambled at its objective from plate to customer or from customer to circle. While trying to

diminish the execution punishment, NASD utilizes a "hash and MAC" cryptographic methodology rather than a standard MAC. In a conventional MAC calculation, a customer's mystery key is utilized all through the calculation. Interestingly, hash and MAC utilizes the crude information from the record to precompute a progression of message processes that are nonexclusive for the given document. Hash and MAC then, at that point, applies a customer's mystery key to the message processes just as a customer demands a record. The outcome is that the mystery key is just needed for a little subset of the generally calculation, along these lines altogether diminishing dormancy related with on-the-fly cryptography. Tests showed that the dormancy for utilizing cryptographic activities was limited by a 20% expansion in an opportunity to support a solicitation when contrasted with a solicitation with no cryptography [10].

B. PASIS – Survivable Storage

PASIS is a survivable stockpiling framework intended to resolve issues related with compromised servers; the framework accepts that compromised servers will exist and consequently addresses how to secure information in such a climate. PASIS utilizes a edge plan to disseminate trust among capacity hubs to forestall information security breaks in any event, when confronted with a compromised server. The edge conspire encodes, duplicates, and partitions data with the end goal that the bits of information are put away in various areas. To make the information dispensing straightforward to clients, PASIS requires a customer side "specialist" to decipher client level orders and the related reactions from the different PASIS servers associated with the capacity hubs [8,33].

Confidentiality: PASIS endeavors to forestall information compromise by putting away components of a document in various areas with the goal that a solitary compromised server can't unveil any pertinent data. Rather than cryptography to guarantee secrecy, PASIS utilizes a slope p-m-n limit plot that partitions information into n offers with the end goal that any m of the offers would be able reproduce the first information, yet less than p shares uncovers no data about the unique. (Cryptography and a limit plan can be consolidated to build the degree of assurance, in any case, any cryptography would need to be layered on top of PASIS). As long as not as much as p shares are ever noticeable to a gatecrasher no data will be compromised.

Integrity: PASIS gives information uprightness by not depending on a particular arrangement of PASIS servers to give the necessary m portions of the information. Since having any arrangement of m offers permits the customer specialist to recreate the first information, those m offers can emerge out of any of the different servers in the organization. To forestall information respectability an interloper must compromise the m servers overhauling the solicitation and adjust the information. On the off chance that the customer specialist does not get the essential m offers or can't reproduce the first document due to malignant intercession, the solicitation is rebroadcast

Availability: Like the contention made for the PASIS respectability improvements, the framework's prerequisite for just m offers to recover information expands information accessibility in the face of bombed servers. The quantity of servers needed in the "making due" subset of servers has an upper bound of m, to such an extent that (n-m) servers can be compromised or inaccessible and the framework will in any case effectively administration the solicitation. Also, with a

compose activity the framework chairman can decide the quantity of offers needed to acknowledge the compose. Basically m offers should be effectively composed, yet any number between n and m will give the right information. Obviously, the more effectively composed offers will accommodate more prominent accessibility

on resulting record access demands.Despite the fact that PASIS accommodates expanded information accessibility for single clients, it doesn't straightforwardly address simultaneous access or simultaneous alterations to records. This suggests that some extra instrument should be layered on top of PASIS to ensure atomicity, which thusly infers potential message passing overhead or idleness when numerous clients access a similar document at the same time

Performance: In relative correlation with a conventional conveyed record framework, PASIS is upset by an expanded number of message passes to get a similar data. A customary framework sends a solicitation to a solitary server, though PASIS should communicate solicitations to at minimum m servers and afterward consolidate the resultant messages on the customer machine. It is hard to evaluate the overhead connected with PASIS in light of the fact that there are extraordinary execution compromises related with choosing various qualities for n-m-p. The values, be that as it may, can be altered for a specific record. For instance, expanding the worth of n improves the probability that m offers will be accessible, however it additionally implies that more portions of the document are put away, in this manner expanding the potential for burglary. The advantage of this adaptability permits clients to choose suitable qualities for each record they store in the framework. During their examination, the PASIS creators found a critical presentation cost for getting to little documents, however a unimportant punishment for enormous.

C. CFS Cryptographic File System

CFS is obsolete, however it is pertinent to examine CFS since it shaped a hypothetical venturing stone for different specialists to set up framework plan objectives. An essential inspiration for CFS was to dispose of the prerequisite for client or framework level cryptography and on second thought place the prerequisite in the record framework. Manual or application based cryptographic tasks were either mistake inclined or contradictory with each other. Framework level arrangements needed convenientce brought about by implanted encryption procedures, they needed similarity because of particular server validation programming, or they left potential security openings where information was briefly put away as clear text. CFS proposed driving all document encryption into the customer record framework. It involved a/crypto mount point in Unix to veil CFS explicit tasks permitting the record framework to deal with encoded documents like any others. The framework was intended for a nearby, not circulated, use, in this manner an individual client should genuinely "hand-out" the cryptographic keys for each document [3].

Confidentiality: The main technique for controlling approval is the document proprietor's selectivity with passing imperative keys out to different clients. It is the client's liability to guarantee that the keys are dispersed in a solid way to just the right and planned faculty. The technique, while not adaptable, doesn't depend on a confided in waiter. The proprietor of a record scrambles it with a symmetric key preceding composing it to the document framework. Neither the record framework, nor any clients, at any point approaches the unmistakable text information. There are no extraordinary arrangements for guaranteeing that the information is encoded on the wire, yet one can work under the supposition that assuming the document leaves the customer machine in scrambled structure, is never altered by the server or the record framework, and afterward is sent to one more approved customer with the legitimate key that the data has been secure 100% of the time.CFS mounts a virtual document framework (/grave) to a standard Unix records framework, and afterward coordinates all framework calls connected with scrambled records through the mount point. Clients make registries under the/sepulcher

mount point with a related key which will then, at that point, be utilized to encode all information put away inside the catalog.

Integrity: CFS changes over standard NFS framework calls into CFS explicit considers utilizing a daemon on the customer machine. The daemon then, at that point, issues RPCs to the document server after the customer builds up a legitimate association with the server. Any endeavor to send a RPC straightforwardly to the record server, in this manner bypassing the CFS daemon, will be denied due to a necessity for all RPCs from a customer to have been produced from an advantaged port.This assists with keeping any noxious client from approaching adjust records, yet there is no immediate component to give extra trustworthiness insurance. CFS depends on the supposition that the record server never approaches decoded information to guarantee information uprightness.

Availability: While all documents remain scrambled on the record server, there is no instrument to keep an enemy from denying a genuine client from getting to documents assuming the server is compromised. The framework does, be that as it may, utilize the hidden document framework's sharing semantics to permit simultaneous admittance to different clients. When keys are appropriately circulated, CFS gives equivalent standard use accessibility to Unix.

Performance: CFS runs at client level and communicates with the hidden document framework by means of far off methodology calls. This infers that there is potential for critical setting switch overhead notwithstanding the additional expense of DES cryptographic tasks. CFS demonstrated to be up to multiple times more slow than standard NFS for perusing and composing enormous records, two times as slow for making little records, and 30% more slow for a blend of "standard" tasks.

D. SFS-RO – Secure File System – Read Only

SFS-RO depends on self-affirming way names to give high accessibility to peruse just information in a dispersed climate. SFS-RO utilizes a portion of the ideas from its SFS ancestor, however takes a stab at better execution by giving read-just information that doesn't require any server-based cryptographic tasks. The idea is to in any case guarantee information trustworthiness while delivering various duplicates of perused just material; customarily replicating brought about a corruption of safety [7, 17].

Confidentiality: SFS-RO depends on a common verification convention between the clients furthermore the server, performed through self-ensuring pathnames that have the public key for a record implanted in them. The maker of the record can dole out the key, subsequently offering a wide scope of cryptographic choices. To appropriately scramble documents, a director packages the substance of the record framework into an information base that is endorsed with an advanced mark containing the private part of an hilter kilter key. When marked, the information base can be reproduced and dispersed to numerous untrusted machines without the danger of give and take. To get to the documents, a client should give the area of the capacity server (either a DNS hostname or IP address) and a HostID. The HostID is a cryptographic hash of the server area and the general population piece of the hilter kilter key with which the document maker encoded the information base. The data set maker should give the public key to all potential clients separate from the SFSRO framework. Once conceded authorization to the documents through the common confirmation, the clients can then, at that point, access documents by giving the fitting handle, included a cryptographic hash of the record's squares. Gatherings of handles are recursively hashed and put away in hash trees to such an extent that the handle to the root inode gives the capacity to confirm the substance of individual record blocks, decreasing the quantity of handles needed

all through the framework. Knowing the handle of the root inode gives a customer the capacity to check the substance of a given document by recursively looking at the hashes.

Integrity: SFS-RO depends on three basic components: the SFS information base generator, the SFS peruse just server daemon, and the customer. Customary registries are changed over to a information base and carefully endorsed in a solid customer climate. This data set is then, at that point, conveyed to quite a few servers that all run the SFS-RO server daemon. The server daemon just gets demands from customers to turn upward and bring information back. The SFS customer runs on a customer machine and is a conductor between a standard document framework convention (like NFS) and the server. Endless supply of a record transmission, it changes over the SFS-RO information base "lumps" into conventional inodes and squares that a common record framework would hope to see. Furthermore the customer must gangs a private key to confirm the advanced signature on information passed from the server since SFS-RO doesn't confide in the server. This check process guarantees information respectability. SFS-RO likewise utilizes a timestamp convention to assist with identifying uprightness infringement. When a client makes a data set, the time is recorded. Furthermore, the maker should build up a no-later-than time to leave the information base with the goal that the time has an upper and lower bound. Clients of the documents keep a record of the current timestamp which they look at against all information that they get to forestall a rollback assault.

Availability: One of the essential objectives of SFS-RO is to stretch out admittance to peruse just information in a worldwide climate. To achieve this, a record framework maker can duplicate the safely produced information base onto any server that is running the SFS daemon. The outcome is a framework that scales to the quantity of servers duplicated by the quantity of associations per server. Since the framework is intended for quite a long time of perused simply material to be conveyed among numerous machines, it is coherent to conclude that obliteration of one server won't influence the accessibility of the document.

Performance: All cryptographic activities are performed on customer machines; the maker builds up the data set in a protected non-arranged climate and clients get scrambled information which they should unscramble on their customer machines. The cryptographic activities ended up being the most expensive angle in contrast with customary NFS. For little documents, SFS-RO was two times as delayed as NFS with the essential extra expense due to timestamp check (to guarantee honesty). SFS-RO causes extra dormancy when contrasted with NFS on the grounds that NFS is run in the portion while SFS-RO should depend on framework calls. In bigger records where the extent of framework calls to information passed is more modest, the dial back was around 30% which, while significantly better over little records, is still a significant exhibition punishment. SFS-RO started to perform well with exceptionally enormous documents (40MB), demonstrating 4% quicker than NFS.

E. SNAD – Secure Network Attached Disks

Secure Network Attached Disks are intended to forestall any unapproved staff from getting to put away records by encoding all information, and just permitting unscrambling on a customer machine. This kills the potential danger presented by compromising the situation manager's entrance freedoms or that presented by actually catching a plate. The singular drives need adequate data to unscramble any information themselves, and depend rather on a key administration conspire that gives an approved client with adequate keys to decode records on the distant customer machine. [5, 20, 21, 24]

Confidentiality: The basic usefulness behind SNAD lies in the lockbox system for putting away keys. Each document comprises of fluidly estimated secure information objects which are all separately encoded with a

symmetric item key. Inside the record's metadata is a pointer to a critical item for that record which, itself, can be viewed as a document. Inside the key article's metadata there are fields for a one of a kind key document ID, the client ID for the maker of the document, and an advanced mark from the last client to alter the record. The advanced mark of the last modifier of the document is given to guarantee any remaining clients that the key article itself has not been altered (any approved client can check that the key item signature coordinates with somebody approved to keep in touch with the document). The key article document itself comprises of tuples that agree with genuine clients for the first document. Each tuple contains a client ID field, the article symmetric key to get to the protected information objects, and a posting of whether or not the client has authorization to keep in touch with the key item (concurring with consent to keep in touch with the first document). The item key is itself encoded with general society part of a client's awry key so the best way to decode the item key is with the client's private key on the client's customer machine. This keeps any gatecrasher from ever having the option to get to the symmetric key that really scrambled the put away information. Notwithstanding the key articles, SNAD oversees approved clients by keeping a endorsement object with tuples containing legitimate client IDs, the client's public key, a hashed message confirmation code key to give and check client advanced marks, and a timestamp the framework refreshes at whatever point the client plays out a compose activity to forestall replay assaults.

Integrity: To give respectability improvement, SNAD stores a non-straight checksum of the unique information alongside the encoded information so a client can confirm that the document has not been vindictively different during stockpiling. The checksum is refreshed at whatever point an approved client makes a change to the record. Clients can likewise check the uprightness of composes by dissecting the record's key article document metadata and really looking at the advanced mark given.

Availability: Since the lock-box of keys is a basic part of SNAD, it should be accessible for clients to get to documents. Sadly, the lockbox is put away on a solitary confided in server which presents a solitary mark of assault for an enemy. Assuming that the lockbox server is compromised, it is absolutely impossible to forestall a forswearing of administration assault. Furthermore, the framework doesn't have a predetermined key disavowal strategy and leaves the choice and execution of dynamic or languid denial to the document proprietor.

Performance: The computationally costly encryption and decoding undertakings are performed on the customer machines and stay away from any expected bottleneck at the server. The decoding process, in any case, can in any case be extremely sluggish in any event, when performed on the moderately quicker customer machines. To offer a client choices, the originators of SNAD have eexecuted three separate plans for giving computerized marks that exchange security for execution. A document's maker can decide the granularity with which to confirm the computerized signature, the better the granularity the greater security gave as well as the other way around. The engineers have demonstrated through observational examinations that the computerized signature process is by far the most exorbitant with SNAD [5]. The most solid technique where computerized marks are given each square compose and confirmed with each square perused isn't reasonable for standard use. Just the most un-secure of the three choices (confirming the computerized signature in view of a hashed MAC rather than a public key) ended up being tantamount to a framework without security [21].

F. CFS Cryptographic File System

CFS is obsolete, yet it is pertinent to talk about CFS since it framed a hypothetical venturing stone for different analysts to set up framework plan objectives. An essential inspiration for CFS was to wipe out the prerequisite

for client or framework level cryptography and on second thought place the prerequisite in the document framework. Manual or application based cryptographic tasks were either mistake inclined or incongruent with each other. Framework level arrangements needed versatility brought about by installed encryption strategies, they needed similarity because of particular server confirmation programming, or they left potential security openings where information was briefly put away as clear text. CFS proposed driving all record encryption into the customer document framework. It involved a/crypto mount point in Unix to veil CFS explicit activities permitting the record framework to deal with scrambled documents like any others. The framework was intended for a nearby, not appropriated, use, subsequently an individual client should genuinely "hand-out" the cryptographic keys for each document [3].

Confidentiality: The main strategy for controlling approval is the record proprietor's selectivity with passing essential keys out to different clients. It is the client's liability to guarantee that the keys are conveyed in a solid way to just the right and planned work force. The strategy, while not versatile, doesn't depend on a confided in server. The proprietor of a document encodes it with a symmetric key before composing it to the record framework. Neither the document framework, nor any clients, at any point approaches the reasonable text information. There are no exceptional arrangements for guaranteeing that the information is scrambled on the wire, however one can work under the supposition that assuming the document leaves the customer machine in scrambled structure, is never adjusted by the server or the record framework, and afterward is sent to one more approved customer with the appropriate key that the data has been secure all of the time. CFS mounts a virtual record framework (/sepulcher) to a standard Unix documents framework, and afterward coordinates all framework calls connected with scrambled documents through the mount point. Clients make indexes under the/sepulcher mount point with a related key which will then, at that point, be utilized to scramble all information put away inside the catalog.

Integrity: CFS changes over standard NFS framework calls into CFS explicit considers utilizing a daemon on the customer machine. The daemon then, at that point, issues RPCs to the record server after the customer sets up a legitimate association with the server. Any endeavor to send a RPC straightforwardly to the document server, subsequently bypassing the CFS daemon, will be denied due to a prerequisite for all RPCs from a customer to have been produced from a favored port. This assists with keeping any malignant client from approaching adjust documents, yet there is no immediate system to give extra trustworthiness security. CFS depends on the suspicion that the record server never approaches decoded information to guarantee information respectability.

Availability: While all records remain encoded on the document server, there is no component to keep a foe from denying a real client from getting to documents assuming that the server is compromised. The framework does, notwithstanding, utilize the basic document framework's sharing semantics to permit simultaneous admittance to different clients. When keys are appropriately circulated, CFS gives similar standard use accessibility to Unix

Performance: CFS runs at client level and connects with the hidden record framework through distant methodology calls. This suggests that there is potential for huge setting switch upward notwithstanding the additional expense of DES cryptographic tasks. CFS demonstrated to be up to multiple times more slow than standard NFS for perusing and composing huge documents, two times as slow for making little records, and 30% more slow for a blend of "standard" tasks.

G. PLUTUS

PLUTUS is another lockbox conspire that works in much the same way to SNAD, yet the essential objective of PLUTUS is to give profoundly versatile key administration while giving record proprietors with direct command over approving admittance to their documents. All information is encoded on the plate with the cryptographic and key administration activities performed by the customers to reduce server cryptographic upward. Clients can redo security strategies what's more confirmation components for their own records utilizing the customer based key appropriation conspire. This puts the obligation regarding key administration on the client, constraining the document proprietor to guarantee appropriate secure circulation of keys to those they wish to approve access. A planned client should contact the proprietor to get the proper key. Riedel contend that this assignment can be performed with an OK expense for client accommodation..

Confidentiality: To give the freedom of proprietor customization while guaranteeing classification, PLUTUS depends on a many-sided lockbox plot with various degrees of keys. At the information level, PLUTUS utilizes a square design to scramble every individual square with a special symmetric key. These square keys are then scrambled inside a lockbox gotten to by means of a document lockbox key normal to all records inside a filegroup. The filegroup proprietor makes the record lockbox key when the document is made and afterward conveys it to all clients. PLUTUS utilizes an awry document confirm key or a record sign key convention to separate among perusers and scholars individually (see Figure 3). These keys are utilized to sign or check a cryptographic hash of the record block substance to give respectability. After mentioning a document, the server passes the scrambled lockbox and encoded block substance to the client. The client then, at that point "opens" the lockbox with the record lockbox key and unscrambles each square with its particular record block key. The multiplication of keys and the utilization of filegroups in PLUTUS entangle the key renouncement plot. At the point when different documents across the record framework (related simply by access dislike a customary index) are scrambled with a similar key, key repudiation could cause mass re-encryption and key administration issues. Nonetheless, the creators have executed a smart key pivot conspire that limits the impacts. PLUTUS utilizes apathetic repudiation with the end goal that a disavowed client can in any case peruse documents that were open at the hour of disavowal. An issue emerges because of the utilization of filegroups on the grounds that upon re scrambling a document, various records inside a similar gathering will require different keys. Since a essential inspiration for utilizing filegroups in any case was to limit the quantity of keys, Kallahalla et al [16] planned a revolution plot that guarantees that the new encryption key is connected with the keys for all documents in the filegroup. The framework perform the re-encryption with the most recent filegroup keys, yet everything substantial clients can produce past forms from the most recent key. The outcome is that everything legitimate clients can "recover" the appropriate key for a given record assuming they have the most recent filegroup key. The new filegroup key is as it were dispersed to presently legitimate clients with the end goal that disavowed clients.

Integrity: PLUTUS doesn't confide in the document server and can't, hence, depend on it to recognize journalists and per users. Rather it utilizes two sorts of keys, record sign keys what's more record check keys, to make the separate assurance. After endeavoring to peruse or compose, the client confirms the computerized signature and hashed substance of the record with these keys. Assuming the client acquires startling outcomes, the client can establish that the record has been wrongfully changed.

Availability: The whole plan of PLUTUS is expected to give adaptability. Setting the key administration obligation on the customers rather than on a believed server forestalls a server bottleneck because of computationally costly cryptographic activities. PLUTUS depends vigorously on filegroups to restrict the

quantity of cryptographic keys. Filegroups comprise of all records with indistinguishable sharing ascribes and can, thusly, be ensured utilizing something similar key. This gives clients with filegroup rights to get to a record inside the gathering regardless of whether the proprietor isn't on-line, staying away from the necessity for a client to contact the proprietor straightforwardly to get the key with each record access. The filegroup idea doesn't depend on a progressive design so the gathering is completely a result of the related records' authorization credits. PLUTUS gives a lot more noteworthy adaptability and a sharp key revolution process to limit key administration obligations related with key repudiation, yet the framework actually requires the document's proprietor to give a duplicate of the record's symmetric key to each client. Filegroups help to limit the document proprietor client correspondence, however they don't wipe out the first obligation regarding the proprietor to circulate the keys.

Performance: The creators of PLUTUS utilized OpenAFS to develop their framework. The execution of the document framework itself is practically identical to the unmodified OpenAFS framework, since the server doesn't need to play out any incidental tasks during record access. Anyway the expense for the customer framework where cryptographic activities are performed shown to be 1.4 times more slow than SFS. The creators present a dependable contention to legitimize this decline in execution, since they utilized most pessimistic scenario situations to determine their figures. This correlation just considers a solitary record read and compose blend which doesn't exploit the plan improvement presented by PLUTUS. PLUTUS is intended for versatility and to assuage server bottleneck which may emerge with various document access demands in standard SFS. reason that the normal inactivity for extended use would lean toward the utilization of PLUTUS.

H. SiRiUS – Securing Remote Untrusted Storage

SiRiUS is intended to give its own cryptographic perused compose record access on top of any current untrusted arranged record framework (NFS, CIFS, Yahoo, and so on) Through a programming daemon, the framework catches all document access framework calls and converts them appropriately. The idea is to have the option to build up a safe document sharing climate without fundamentally altering the presentation of a current organization stockpiling medium. SiRiUS can give security to a current framework without requiring any equipment changes; the designers view the framework as a "band-aid" measure to give extra security to existing frameworks. Periodically, associations can't stand to overhaul their present frameworks and should keep on working with restricted security until which time the choice to overhaul safety efforts opens up; SiRiUS can give an interval arrangement.

Confidentiality: All documents are encoded in a safe climate before being put away on the server, with the end goal that neither the server nor the server head at any point approaches decoded information. Also, the computationally exorbitant encryption activities are performed on the generally gently stacked customer machine, and the way that the information is currently scrambled blocks any necessity to set up a solid channel to send the record to the server. Each record proprietor keeps an expert encryption key (MEK) and an expert marking key (MSK). Each record has a remarkable symmetric document encryption key (FEK) given to all clients and a record marking key (FSK) gave distinctly to approved authors to the document. The framework gives a "newness ensure" by keeping a metadata newness record for every catalog. All records are isolated into two sections: a md-document metadata record and a d-record information document. The metadata document contains a square for the record proprietor's MEK, a square for each substantial client's FEK (and FSK whenever approved to keep in touch with the record), and a square with a hash of the metadata record's substance endorsed

with the proprietor's MSK. Assuming the proprietor or a client has a key kept up with in the document's metadata, that individual can decode the record. Client key disavowal is speedy and effective; the document proprietor eliminates the denied client's vital square from the metadata document, makes another FEK, re-encodes the record with the new key, and afterward refreshes the excess clients' critical squares with the new FEK. The outcome is prompt renouncement. Honesty. Notwithstanding added measures, SiRiUS keeps specific document framework explicit metadata decoded with the goal that the document framework can perform standard respectability checking activities. SiRiUS keeps all entrance control data scrambled with the document information. This works with utilizing the inheritance document framework's standard reinforcement techniques - if the framework should recuperate from an accident, all of the required admittance data is now accessible with the record. SiRiUS utilizes the "newness ensure" to guarantee that clients have the latest form of a record forestalling a rollback assault. At a client assigned stretch, the client timestamps the metadata newness document.

Integrity: The option to added measures, SiRiUS keeps specific record framework explicit metadata decoded with the goal that the record framework can perform standard respectability checking tasks. SiRiUS keeps all entrance control data encoded with the record information. This works with utilizing the inheritance record framework's standard reinforcement strategies - if the framework should recuperate from an accident, all of the required admittance data is now accessible with the record. SiRiUS utilizes the "newness ensure" to guarantee that clients have the latest rendition of a record forestalling a rollback assault. At a client assigned span, the client timestamps the metadata newness record

Availability: The plan choice to make no adjustments to the basic record server keeps SiRiUS from shielding against refusal of administration assaults; an aggressor could possibly compromise the server and erase all documents. SiRiUS has no capacity to mediate in such a situation and, along these lines, expects clients to reinforcement their own records on various servers to restrict the impacts of such an assault. To add clients, the point of view peruser/essayist of a record should send a public key to the document proprietor who will then, at that point, utilize the public piece of the MEK to scramble that key and add it to the documents metadata. When the new client's key is added to the metadata, the client approaches the document. The key passing component isn't tended to in the framework. As recently tended to, SiRiUS upholds dynamic key renouncement to such an extent that once a client's access privileges have been disavowed, the client no longer has any type of admittance to the document by means of the newness ensure. SiRiUS endeavors to enhance other secure organized document framework plans by permitting fine grained record access while giving the capacity to a document proprietor to give read-just or read-compose admittance to shared documents. Different frameworks either permi admittance to whole indexes or can't recognize perusers and essayists.

Performance: Whenever a record first is gotten to, the document framework should return the related metadata document just as the first (to help fitting approval checking). The metadata document is then reserved to forestall the upward of turning upward and sending the metadata document on ensuing recoveries for a similar record. Also, numerous SiRiUS document framework calls require checking the newness document bringing about expanded organization traffic and extra record I/O for each. 63% of the expense related with involving SiRiUS for a 1MB information read is because of the decoding cost. Essentially, 40% of the expense for composing a 1MB record is because of mark age.

IV. CLASSIFICATION

Storage System	Encryption Location	Trusted Server	Key Revocation Policy	Confidentiality Measures	Integrity Policy	Availability Policy	Estimated Performance Overhead
NASD	Wire	Yes	Active by using timestamps, key issued one time	Capability keys, separate authentication server	Hash MAC checksums to send data, not secure on disk	Scalable to many users, subject to DOS	20% increase over system with no security
PASIS	Wire	No	N/A	p-m-n threshold scheme	Data dispersed across storage nodes such that > p must be compromised	Only m shares must be available to recreate the original	Significant overhead for small files, negligible overhead for large files
S4	Wire	No	N/A	N/A	Detection scheme: Comprehensive versioning	Intrusion detection and diagnosis to provide "recent" version	Comparable to NFS
CFS	Disk	Yes	Manual active revocation	Keys handed out to users by the file owner	Privileged port combined w/ encryption	Limited to manual distribution of keys/ DOS if server compromised	30% slower than NFS for standard workload
SFS-RO	Disk	No	Revocation list	Self-certifying pathnames	Self-certifying pathnames, timestamps	Multiple distributed copies of RO files	2 times slower than NFS for small files, comparable for files > 40 MB
SNAD	Disk	No	Lazy or active revocation options, no decision	Lockbox	Non-linear checksum of original text stored along with encrypted file	Potential DOS if lockbox server is compromised	Only the least secure option is comparable to a system w/o security
PLUTUS	Disk	No	Lazy revocation, revoked user retains same file permissions as time of revocation	Lockbox with user control over key dissemination. Users must secure distribution themselves	Stored encrypted, but requires augmentation to ensure integrity	Uses filegroups, but requires file owner to distribute keys	1.4 times decrease from SFS for single file access
SiRiUS	Disk	No	Active Revocation	Combination of Master Encryption Key and File Encryption Keys	Freshness guarantee timestamp	Scalable to Internet, but requires file owner to distribute FEK	20 times slower than NFS for small files, 2-6 times slower for 1MB files

Table 1 System Description

Table 1 provides a summary of the characteristics described in the previous sections.

Security Measure	Confidentiality	Integrity	Availability	Performance	Total
Encrypt-on-disk	2	2	0	0	4
Encrypt-on-wire	1	1	0	0	2
Threshold scheme	1	1	2	2	6
Timestamps	0	2	0	2	4
Digital signatures	0	2	0	0	2
Checksums	0	1	0	1	2
Lazy revocation	1	0	2	2	5
Active revocation	2	1	1	0	4
Key distribution server	1	0	1	1	3
Manual key distribution	2	0	0	0	2
Lockbox key mechanism	2	0	1	1, 2*	4,5*
Self-Certifying pathnames	1	0	2	1	4
Filegroups	0	0	1	1	2
Comprehensive versioning	0	2	2	2	6

Table 2 Quantitative Comparison of Security Measures

The table uses a scale between 0-2 to dole out values to the degree of safety of a specific security property. 0 means that the safety effort doesn't influence the property, 1 indicates that the action upgrades security, 2 signifies that the action altogether improves security. For execution, the scale is adjusted to incorporate three qualities (0-2) due to immensely contrasting execution costs. A 0 means that the action fundamentally dials back

framework execution, a 1 signifies a huge presentation punishment, and a 2 demonstrates a restricted exhibition punishment (all frameworks experience some presentation debasement because of added safety efforts). While these figures depend on exact information got from the creators' exploration of every framework, it is essential to take note of that they are an abstract portrayal. *PLUTUS' key revolution conspire improves execution.

Security Measure	NASD	PASIS	S4	CFS	SFS-RO	SNAD	PLUTUS	SiRiUs
Encrypt-on-disk				X	X	X	X	X
Encrypt-on-wire	X	X	X					
Threshold scheme		X						
Timestamps	X				X			X
Digital signatures					X		X	
Checksums	X					X*		
Lazy revocation					X	X	X	
Active revocation	X			X				X
Key distribution server	X							
Manual key distribution				X				
Lockbox key mechanism						X	X	
Self-certifying pathnames					X			
Filegroups				X		X	X	
Comprehensive versioning			X					

Table 3 Security Measure Applications to Surveyed Systems

** Digital signatures are not considered for SNAD since the authors determined that they were too expensive*

Table 3 maps the security aspects /measures to the systems that use them. An "X" denotes that the system applies the security measure in some form.

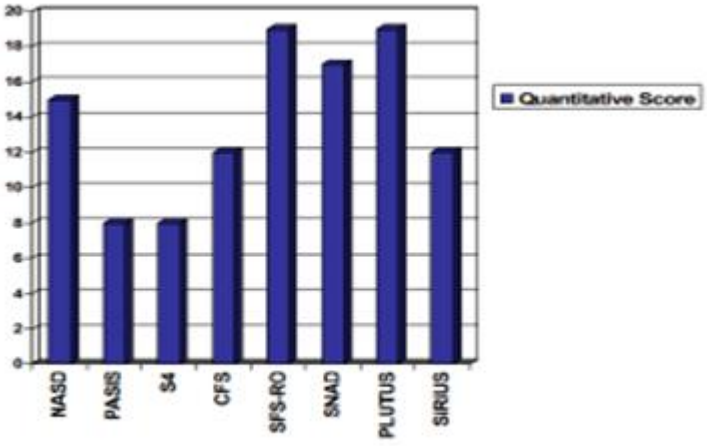


Figure 4 Quantitative Comparison of Secure Storage Systems

The quantitative qualities in Figure 4 are determined by adding the complete scores of every safety effort that applies to every framework. While the numbers give some action to correlation, one should think about the motivation behind every framework related to the assessment. For example, both PASIS and S4 are survivable capacity frameworks which ought to be utilized as a feature of a bigger, secure capacity framework. Most creators notice that involving their plan related to a survivable stockpiling framework would give the best security. Furthermore, SFS-RO gets a high quantitative score, yet it is restricted to peruse just applications.

V. CONCLUSIONS

Every one of the frameworks share a shared objective: to shield put away information from the impacts of a vindictive foe. From this shared conviction, notwithstanding, the plan ways to deal with arrive at this objective differ massively. A few frameworks plan to keep a foe from ever approaching information, while others expect that interruptions are inescapable and attempt to restrict how much harm an interloper can present. A few frameworks separate information onto numerous capacity servers to dispense with a solitary place of assault, and others depend on incorporated confided in servers to viably oversee cryptographic keys. A few frameworks store encoded information and others require encryption before sending messages on the wire. These models present enormous major contrasts that give choices to possible clients of a capacity security medium. It is extremely challenging to make direct correlations between the frameworks in light of the differed approaches, however expected clients can choose the most pertinent answer for their particular issues. The most solid arrangement will probably be a mix of the frameworks depicted. Indeed, most of the architects of the frameworks suggest that their answer be part of a bigger security plan. For instance, in the event that a client can acknowledge extra cryptographic dormancy there is no great explanation to abstain from scrambling information prior to applying a limit plot. The outcome would give the security of encryption without depending on a confided in server furthermore would build the level of accessibility. The issue with such layering, notwithstanding, is the exhibition punishment. It is subsequently a plan prerequisite to investigate the tradeoffs among security and execution

VI. REFERENCES

[1]. Mehmet Bakkaloglu, Jay J. Wylie, Chenxi Wang, Gregory R. Ganger. On Correlated Failures in Survivable Storage Systems. CMU SCS Technical Report CMU-CS- 02-129. May 2002.

[2]. Scott A. Banachowski, Zachary N. J. Peterson, Ethan L. Miller, and Scott A. Brandt. Intra-file security for a distributed file system. In Proceedings of the 19th IEEE Symposium on Mass Storage Systems and Technologies, pages 153–163, College Park, MD, April 2002. IEEE

[3]. Matt Blaze, A Cryptographic File System for Unix, First ACM Conference on Communications and Computing Security, Fairfax, VA November, 1993

[4]. Brian Cornell, Peter A. Dinda, Fabian E. Bustamante Wayback: A User-level Versioning File System for Linux. In Usenix Annual Technical Conference, Boston, MA Jun 27 – Jul 2, 2004

[5]. William Freeman and Ethan Miller. Design for a decentralized security system for network-attached storage. In Proceedings of the 17th IEEE Symposium on Mass Storage Systems and Technologies, pages 361–373, College Park, MD, March 2000.

[6]. Kevin E. Fu. Group Sharing and Random Access in Cryptographic Storage File Systems. Massachusetts Institute of Technology, Jun 1999. (Cepheus)

[7]. Kevin Fu, M. Frans Kaashoek, David Mazieres. Fast and Secure Distributed Read Only File System. In Proceedings of the 4th USENIX Symposium on Operating Systems Design and Implementation, pages 181-196, Sand Diego, CA, Oct 2000.

[8]. Gregory R. Ganger, Pradeep K. Khosla, Mehmet Bakkaloglu, Michael W. Bigrigg, Garth R. Goodson, Semih Oguz, Vijay Pandurangan, Craig A. N. Soules, John D. Strunk, Jay J. Wylie. Survivable Storage Systems.

DARPA Information Survivability Conference and Exposition (Anaheim, CA, 12-14 June 2001), pages 184-195 vol 2. IEEE, 2001.

[9]. Garth Gibson, David Nagle, Khalil Amiri, Fay Chang, Howard Gobioff, Erik Riedel, David Rochberg, Jim Zelenka, "Filesystems for Network-Attached Secure Disks" CMU Computer Science Technical Report, CMU-CS-97-118. July 1997.

[10].Howard Gobioff, David Nagle, Garth Gibson, “Embedded Security for NetworkAttached Storage”, CMU SCS technical report CMU-CS-99-154, June 1999. 20

[11].Howard Gobioff, Garth Gibson, Doug Tygar, "Security for Network Attached Storage Devices", CMU SCS technical report CMU-CS-97-185 1997.

[12].Eu-Jin Goh, Hovav Shacham, Nagendra Modadugu, and Dan Boneh. SiRiUS: Securing Remote Untrusted Storage. In the proceedings of the Internet Society (ISOC) Network and Distributed Systems Security (NDSS) Symposium 2003 .

[13].Garth Goodson, Jay Wylie, Greg Ganger & Mike Reiter. Decentralized Storage Consistency via Versioning Servers. Carnegie Mellon University Technical Report CMU-CS-02-180, September 2002.

[14].Garth R. Goodson, Jay J. Wylie, Gregory R. Ganger, Michael K. Reiter. Efficient Consistency for Erasure-coded Data via Versioning Servers. Carnegie Mellon University Technical Report CMU-CS-03-127, April 2003.

[15].Garth R. Goodson, Jay J. Wylie, Gregory R. Ganger, Michael K. Reiter. A Protocol Family for Versatile Survivable Storage Infrastructures. Carnegie Mellon University Parallel Data Lab Technical Report CMU-PDL-03-104, December 2003.

[16].Mahesh Kallahalla, Erik Riedel,Ram Swaminathan, Qian Wang, and Kevin Fu. PLUTUS: Scalable secure file sharing on untrusted storage. In Conference on File andStorage Technology (FAST'03) pp. 29-42 (31 Mar - 2 Apr 2003, San Francisco, CA). Published by USENIX, Berkeley, CA.

[17].David Mazieres, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchell. Separating Key Management From File System Security. In 17th ACM Symposium on Operating Systems Principles, pages 124-139, Dec 1999.

[18].David Mazieres, Dennis Shasha Building Secure File Systems Out of Byzantine Storage. In Proceedings of the Twenty-first Annual Symposium on Principles of Distributed Computing, pages108-117, Monterey, CA, 2002.

[19].David Mazieres, Dennis Shasha. Don’t Trust Your File Server. In Proceedings of the 8th Workshop on Hot Topics in Operating Systems, 2001.

[20].Ethan L. Miller, Darrell D. E. Long, William Freeman, and Benjamin Reed. Strong security for distributed file systems. In Proceedings of the 20th IEEE International Performance, Computing and Communications Conference (IPCCC '01), pages 34– 40, Phoenix, April 2001. IEEE

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Hacking and Its Vulnerabilities

Niraj Jain, Ishika Tiwari, C. H. Patil, Dheeraj Solankar, Hritwika Dubey, Kashish Roy, Arundhati Dhar
School of Computer Science, Dr.Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India

ABSTRACT
Hacking can be understood as any unusual manner of accessing a system, it's easy to assume that few utilizes this information to gain knowledge, while others use it to learn how to exploit it to delete or access data from computer sites or servers without the owner's knowledge. As a result of the author's study, the article examines hacking from several perspectives such as “Who are these hackers?" What motivates people to hack? Hacking's legal concerns, as well as some financial challenges, are discussed. Following that, the study also focuses on phishing attacks, DoS Attack (denial of service), and MiTM (Man in the Middle) attacks. The goal of this review is to familiarize readers with the potential hazards of hacker assaults on their mobile devices, as well as potential attacks in the upcoming wave of Internet-connected gadgets
Keywords—hacking, identity theft, extortion, phishing, measures

I. INTRODUCTION

In today's world, computers play an important role in day-to-day living. Because the digital universe is rapidly expanding and a vast amount of data is flowing online, data security is big concern[1]. The internet has accelerated the modernization of several operations such as online financial transactions, banking, and online receiving and sending of numerous types of information, raising the risk of data security. Hackers are now targeting a vast number of corporations, banks, and sites with various forms of attacks. As a results, there are ethical hackers who assists their customers and closes the security gap. So, when it comes to system security, these ethical hackers would utilise the same strategies that hackers do, but in a legal way, and they would not harm the target systems or steal data. Instead, they'd analyse the target system's privacy and communicate back to the owners with the flaws they discovered and recommendations on how to fix them[2].

II. WHAT IS HACKING

Hacking is the approach used to find weakness in computer networks and escapade it to get access to the target computer system to gain series of confidential and private information for personal or professional accomplishments[2]. Hacking is when unauthorized user barge into someone’s private space (specifically digital space) and steal the desired data without them knowing[10]. Clarifying furthermore, hacking alters the computer

software, hardware and certain computer networks for accomplishing illegal means. Hacking specifically is, disruption of privacy by finding technological loopholes in a computer system or network and then withdrawing data without consent from the authorized owner[2].

A. Types Of Hacker

The motive of a hacker's activity determines the distinct categories of hackers. We'll learn about three main categories of hackers, each with its own goals and roles within the field of data security.

B. Black Hat Hacker

A black hat hacker is someone who breaks into a computer system and attacks security holes for financial benefits[4]. These are those who seek to flaunt their great technical expertise by carrying out numerous cybercrimes. They misuse users' data to commit crimes such as burglary, forgery, scam, identity theft, and more. Because these hacktivist groups are immoral, the acts they commit are sanctioned by law[5].

C. White Hat Hacker

A hacker who has access to a system with the goal of repairing detected flaws and has authority to violate security for valid purposes such as conducting risk evaluations [4]. White Hat Hackers utilize their talents and knowledge to defend an institution prior malevolent or immoral hackers discover it and cause damage to it. They employ a variety of safeguards and precautions in order to protect systems. They are allowed to do so and are referred to as ethical hackers [3].

D. Grey Hat Hacker

Grey Hat Hackers are people who are in between White Hat Hackers and Black Hat Hackers. They have characteristics of both. They are security professional who occasionally breaks the law but does not intend to harm anyone[5]. They expose all security flaws and gaps of companies or agencies, and they don't inform anyone until the problem is resolved. While some of these hackers may just alert authorities to security flaws, Others may propose to remedy the problem for a charge[3]. As a result, they are the ones that extort money from others. Grey hat programmers may engage in practices that appear to be less than totally legal, yet they are often functioning for the greater good.

III. TYPE OF ATTACKS

After The main hazard in today's virtual world is hacking. There is no attack that can be carried out by simply passing by the computer or mobile phone and hitting a single button. The attacks of hacking are either on server or application.

A. Denial of Service (DOS)

This is the most popular sort of assault used by hackers to target web servers. There are three sorts of denial-of-service attacks are volume assaults, procedure attacks, and application layer targets are the three types of attacks. Surging may be conventional tactic chosen by hackers to servers that are online[17]. Hackers send in a large amount of incorrect data at once, causing the server to crash. A large amount of traffic occurs, and the server is forced to shut down.

B. Non-Technical Attacks

The simplest weakness within any computer or network foundation is exploits that involve managing persons, end users, and even you. Physical assaults against data frameworks are both regular and convincing. People are

naturally trusting, which may cause social designing exploitation. Hackers get access to buildings, computer rooms, or other locations containing critical data or property [17]. One sort of physical assault is dumpster diving (looking through trash jars and dumpsters for protected innovations, passwords, network blueprints, and other data). Social engineering is defined as the abuse of people's trust in gathering information for nefarious purposes.

C. URL Parsing Approach

This attack is also known as URL poisoning. The semantics of a URL are changed to allow for an attack, as the word indicates. During this type of attack, just the semantics of the URL are changed, but the syntax is normally left unchanged, so the user has no idea they're accessing the wrong URL[18]. The majority of CGI-based websites are vulnerable to attacks based on URL inference.

D. SQL Injection Attack

This form of attack is most ordinarily seen on e-commerce websites or websites that employ large databases. Some of the URL's parameters in large databases are not validated. As a consequence, specific parameters can be impersonated using SQL language in order to penetrate the database. When a database is compromised, the hacker obtains access to the information of the organisation. As a result, considerable financial loss will occur[18].

IV. TOOLS USE BY HACKERS

A. Aircrack is remote password breaking software it is mainly used for 802.11 WEP and WPA layer breaking its working is simple it gathers the packets aircrack software algorithm is used to analyze the packet once the enough packets are collected the password is guessed [15].

B. AirSnort is wireless tool well-known for decrypting WEP encryption on an 802.11b network. It is a free instrument that works on both Linux and Windows platforms. This instrument is not generally kept up with, however it is as yet accessible to download from Sourceforge [15].

C. The network protocol detector is called Wireshark. Using this software one can scan and monitor the entire network to find vulnerabilities. You may collect and examine packets in real-time. It collects packets and allows you to inspect data at the microsecond level. It is best suited with Solaris, Mac os.

D. WIFI are protected by WPA layer to crack WIFI password we use CloudCracker which is online software solution. This software solution is used to crack the password which are store in hash form, so this software cracks the hash code [15]. It is easy to use user has to upload hash store file which is called as handshake file give basic information about network like network name and click on submit.

V. ECONOMIC ASPECT OF HACKING

The Ethical hackers use hacking tools and strategies in organizations to test corporate security controls in a safe and controlled environment.

These hacking techniques allow an ethical hacker to determine which global controls apply and which global controls need to be updated. Data from these tests allows administrators to make informed decisions about how and where information security can be improved and where it needs to be improved. Ethical Hackers is aware of methods that unethical hackers can use to break into security systems. Ethical hackers can demonstrate these strategies and skills to managers. This will help you understand outsiders, terrorists, etc. By understanding the strategies and practices of unethical hackers, readers can protect sensitive information about their organization

by limiting intrusion attempts and preparing to prevent unauthorized access to their systems. Also, institutions that process sensitive data such as banks and government agencies are very vulnerable to hacking. Hackers attack enterprises that do not have sufficient resources and security measures to stop cyberattacks. Using Ethical Hacking technology, Ethical Hackers reveals the level of business vulnerability and the devastating impact of cyber-attacks. The industry has become one of the most costly and effective victims of hacker attacks. Companies are often attacked by consumer personal and business information, dissatisfied employees or simply creative people. The industry loses $ 444.4 billion annually in hacks and other laptop hacks. In many cases, the impact of a security breach can last years after the actual attack, so the actual cost cannot be estimated. Companies can lose the trust of their customers and are often responsible for losing them. The cost of an attack can quickly add up to legal costs, analytics costs, PR presentations, reputation management, customer support, and more. Companies and more recently, customers are investing more and more money to prevent attacks before they actually occur. In particular, the industry that stores the personal and economic information of consumers is taking more proactive steps to protect their records.

Microsoft MSN / Windows Live Internet Group requires no intitution to store personal data without special approval from the organization's internal security department[19]. Security assessments are often performed by companies that hold customer records, and security teams carry out their own personal security assessments. Another industry where technology may be further limited security is provided by external security professionals[19]. ScanAlert.Com works with over 75,000 trusted e-commerce sites, including leading brands such as Foot Locker, Renovation Hardware and Sony. E-commerce websites carry the "Hacker Safe" logo. It regularly checks of the websites and effectively blocks 99.9% of hacker breaching's. The scanned disclaimer is much less clear. This thread is an example of comparing this web page with staff security measures. Neither this nor any other sensitivity test can guarantee that the is still safe[19].

This actually shows that the E-Commerce Site is checking all card production pricing strategies for vulnerabilities from remote internet servers trying to protect personal information from hackers. HACKER SAFE does not mean protection against hackers. HACKER SAFE's warranty no longer protects data that may be sent to servers not certified by HACKER SAFE, such as credit card networks and offline storage, and also no longer protects users from other illegal information gathering practices[19].

Given the scale of the economic damage, policymakers and businesses must take proactive steps to prevent cyberattacks. Fines and punishing hackers are just one way to do it, just like the use of modern technology. While it is unlikely that disputes over access to encrypted messages related to information sharing will be resolved in the near future, secure communication channels between governments and businesses can certainly take a step forward.

VI. COUNTER MEASURES

To strengthen complete security in every layer of the system there are numerous types of security measures, which reduces unnecessary attacks and hardens the overall system. Furthermore, they limit the access privileges and adds extra security wherever required. Some of these measures are discussed in detail below.

- Sensitive data should be backed up and must be kept classified to guard them from danger.
- Counsel each and every personnel in the organization regarding data protection and confidentiality.
- Records irrespective of type should be backed up periodically.

- Antivirus devices must be updated and checked up on a regular basis to avoid attacks due to negligence.
- Pretty good privacy (PGP)A free email security application which permits consumers to safeguard data by encryption of files and folders. This was developed by Phil Zimmerman in 1991. This method employs the IDEA algorithm that is international data encryption algorithm and a public-private key scheme to encrypt files and emails [16].
- Kerberos is constituted using three components which are: A client, server and A trusted third party which acts as a middleman It was developed by MIT. Kerberos uses private key cryptography and acts as a network authentication protocol [16].
- Don't use public Wi-Fi to access personal or financial information, rather use a secure or a private connection.

VII. CONCLUSION

In this paper we are talking about defender and attacker of cyber space. Hacking is the great expertise yet it is used for terrible intentions. Cybercriminals in cyberspace are easily targeting people from non - technical background. All attackers use same methods and tools, the question arises are they black hat, white hat or grey hat hacker? This mystery will solve with time, known intentions and how valuable data is. Most of the attacks are never known. Nevertheless, some are known if data is corrupted. To protect pc or system framework against any cyber-attack, opposite side should know the intention, methodology and tools.

VIII. REFERENCES

[1]. Zoran Cekerevac, Zdenek Dvorak, Ludmila Prigoda, and Petar Cekerevac, “Hacking, protection and the consequences of hacking,” komunikacie, vol. 20 no 2, June 2018.

[2]. "Research Paper On Hacking," PaperAp.com, 07-Dec-2019. [Online]. Available: https://paperap.com/paper-on-computer-crime-hacking/. [Accessed: 15-Feb-2022].

[3]. A. Sarangam, “Different types of hackers: Black, White, and Gray Hat,” Jigsaw Academy, 28-Dec-2020. [Online]. Available: https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers-2/. [Accessed: 15-Feb-2022].

[4]. A. Froehlich and M. Bacon, “What is a white hat hacker?,” SearchSecurity, 29-Dec-2021. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/white-hat. [Accessed: 15-Feb-2022].

[5]. "What is a Grey Hat Hacker? Hacking without malice." [online] Wallarm.com. Available at: https://www.wallarm.com/what/gray-hat-hacker [Accessed 15 February 2022].

[6]. “What is a black-hat hacker?,” www.kaspersky.com, 09-Feb-2022. [Online]. Available: https://www.kaspersky.com/resource-center/threats/black-hat-hacker. [Accessed: 15-Feb-2022].

[7]. S. Sinha and Dr. Y. Arora, “Ethical hacking:the story of a white hat hacker,” SSRN Electronic Journal, vol. 8, no. 3, May 2020.

[8]. Vinitha K. P., “Ethical Hacking,” IJERT, vol. 4, no. 06, May 2018.

[9]. B. Sahare, A. Naik, and S. Khandey, “Study Of Ethical Hacking,” IJCST, vol. 2, no. 4, 2014.

[10].T. P. Parikh and D. A. R. Patel, “Cyber security: Study on Attack, Threat, Vulnerability,” IJRMEET, vol. 5, no. 6, Jun. 2017.

[11].D. S. Kumar and D. Agarwal, “Hacking Attacks, Methods, Techniques And Their Protection Measures ,” IJSART, vol. 4, no. 4, Apr. 2018.
[12].V. B. Savant, R. D. Kasar, and P. B. Savant, “A review on overview of ethical hacking,” International Journal of Engineering Applied Sciences and Technology, vol. 6, no. 4, Aug. 2021.
[13].Jean-Paul A., Yaacoub, H. N., Noura, O. Salman, and A. Chehab, “A SURVEY ON ETHICAL HACKING: ISSUES AND CHALLENGES,” A Preprint, vol. 1, Mar. 2021.
[14].P. K. Sahu and B. Acharya, “A REVIEW PAPER ON ETHICAL HACKING,” IJARET, vol. 11, no. 12, Dec. 2020.
[15].C. Nagarani, “Ethical Hacking and Its Value to Security,” GJRA, vol. 4, no. 10, Oct. 2015.
[16].Security countermeasure. Security Countermeasure - an overview | ScienceDirect Topics. (n.d.). Retrieved February 16, 2022, from https://www.sciencedirect.com/topics/computer-science/security-countermeasure
[17].Dr.Sunil Kumar and Dilip Agarwal, “Hacking Attacks, Methods, Techniques And Their Protection Measures,” IJSART, Vol 4 Issue 4. April 2018.
[18].Dr Amarendra K, Venkata Naresh Mandhala, SaiSri Damecharla, Praveen Gollapudi and Pavan Kumar Ponuganti “Modern Era Hacking,” IJSTR, vol. 8 issue 12, December 2019.
[19].M. Jumale, "Impact of ethical Hacking on Business and Government", International Research Journal of engineering and technology, vol. 06, no. 12, 2019.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

A Study on Vulnerability Scanning Tools for Network Security

Asst. Prof. Dipali N Railkar[1], Prof. Dr. Shubhalaxmi Joshi[2]
[1]Research Scholar, Department of Master of Computer Application, MIT-WPU, Pune, Maharashtra, India
[1]Faculty, Department of Master of Computer Application, PCCoE, SPPU University, Pune, Maharashtra, India
[2]Associate Dean, Department of Master of Computer Application, MIT-WPU, Pune, Maharashtra, India

ABSTRACT
As world is moving towards complex networks and as we are moving towards digitization its value is increasing every day. Working of organization with internet and network is leading to the vulnerabilities. As we know for every organization data is an important feature and that need to be protected against the threats. Role of the Attackers is to use these vulnerabilities and try to exploit the networks. System security is one of the major aspects when organizations are working more with the support of Internet, intranet and associated techniques. Network security upholds computer systems from unwanted threats and intrusions which lead to reducing the risk of becoming victim to sensitive information theft. Preventing the systems and network from these vulnerabilities well in advance before attack happens will improve the confidence of the organization. For this organization must have proper network audits at place which is usually underestimated. There are various tools for Vulnerability Assessment is available for network audits and support for passive action to be taken to resolve those vulnerabilities. These tools can help organization to stop possible attack. In this paper we are showing the comparative study of Vulnerability Assessment tools for better clarity of the working of Cyber Défense Technology for enhancing security of network. The study conducted is relatively insightful, covering few features and parameters of network security and audit with respect to different tools like Nmap, Nessus, etc. It explores to learn that current tools need to be organized and with enhanced likely vulnerability coverage with respect to performance analysis. Finally, this paper is covering some challenges that existing vulnerability tools are facing towards network security.

Keywords — Vulnerability Assessment, Network Security, Network Audit.

I. INTRODUCTION

The world is getting increasingly connected because of the internet and new networking technology. Network security has received a lot of attention because of the open nature of the Internet. As new technologies emerge, businesses are moving their business processes to the cloud. A substantial amount of personal, economic, and organizational information is available via public networks on networking infrastructures all around the world. As a result, some precautions must be followed. Measures are taken to ensure that unauthorized persons are

neither harmed nor unable to access the information. Unauthorized network access can be obtained by a third-party hacker or a disgruntled employee. Purposely injury or destroy secret data, causing a loss of profit and undermining the organization's capacity to compete in the marketplace. As a result, Network has gained a lot of grip is becoming increasingly critical due to the possibility of intellectual property theft. With a little effort and help from the internet one of the network security measures is scanning as well as Vulnerable Assessment and Penetration Testing (VAPT).[1-3] Computer systems and networks must be scanned to obtain information about their current state. Vulnerability scanning tools facilitate to identify vulnerabilities in different parts of network, devices, web services and applications. Whereas different static analysis tools used to find defects in code and audit tools can be used for finding different attacks on the system such as Trojan, root kit etc. The role of antivirus is to find the viruses, worms trying to damage the operating system or devices or applications. It's a technique for determining which hosts are active on a network with the goal of assessing network security. The word "vulnerability assessment" refers to the process of establishing one's security state of information systems through a systematic investigation. Both ways work well. The following services are provided for every organization's network: network auditing, penetration testing, reporting, and patching.

The importance of information and communication system security has raised to the top of the priority lists of both system developers and end users. On a daily basis, the dangers to our computer network architecture become more complex and sophisticated.[3,4] Attempts are being made by hackers to degrade or completely demolish our security system by conducting increasingly sophisticated attacks against a present vulnerability in our computer network system. It is necessary to train more cyber security professionals in order to defend our system and prevent cyber attacks. A key factor in the accomplishment of successful attacks, unreceptive offensive, and virus infections occurs when software vulnerabilities exist in computer systems, communication equipment, mobile phones, and other smart devices. An increasing number of cyber security courses are emphasizing offensive techniques such as buffer overflow attack and vulnerability exploits as opposed to exclusively defensive approaches such as encryption, intrusion detection, firewalls, and access control. It is vital to understand the many sorts of vulnerabilities that exist in computer systems before putting in place network defence measures. Therefore, vulnerability scanning is an important component of cyber security education. In the field of ethical hacking and network defence education, vulnerability scanning is one of the first procedures that must be taken. There are so many organizations that have made significant gains in the fields of automobile, electronics, physics, medicine, and applied sciences and other fields. These advancements, on the other hand, make them a prime target for hostile cyber attacks. [5, 6]

Confidentiality, integrity and availability are crucial when it comes to the sensitive data that higher education institutions manage (for example, intellectual property and financial information) (e.g., intellectual property, financial data). Because of the conflict between organizational culture, staffing, and resources, as well as the desire for effective security, businesses find it difficult to create and maintain effective security controls. [7] A considerable portion of the risk associated with enterprise network operations is accounted for by technical concerns such as software defects or misconfigurations. The use of standard vulnerability scanners (e.g., Nessus) on a regular basis can detect exploitable gaps in data-protection systems, allowing for the detection of exploitable weaknesses before they become a problem.

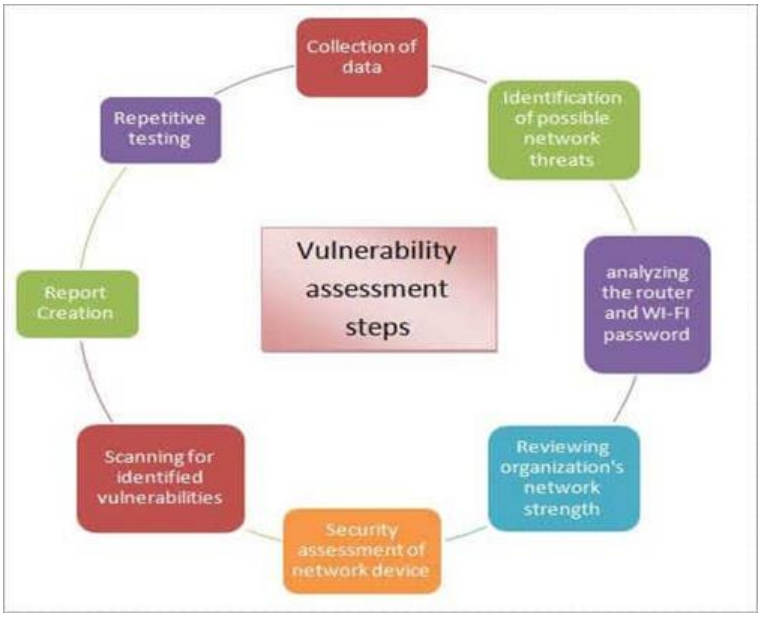


Figure 1- Network Vulnerability assessment steps

However, the security of the apps that are being migrated to the internet is a source of concern because it is directly tied to the security of the user who will ultimately use the programme. Finding software programme flaws that could risk the security of the user is therefore extremely important to ensure their protection. Identification of system faults prior to their being deliberately exploited to impose harm to the network is the goal of vulnerability assessment in information technology (IT). In this strategy, the vulnerability is detected and repaired before it is discovered and exploited by others, and it is used in combination with other techniques. Although the firewall has traditionally received more attention, internal functionality is as important. Vulnerability assessments are performed not only on a single application, but also on the platform, middleware, and operating system that the application is running on. It considers all of the variables that can lead to an accurate assessment of the system's vulnerability and security. In network systems and/or software applications, vulnerability scanners are tools that may be used to check for flaws in the system's operation.

There are two forms of scanning:

a) Inactive Scanning: Passive scanning utilizes the present network to determine whether a device is capable of detecting susceptibilities.
b) Active Scanning: Active scanning determines whether queries to the network for the vulnerability can be made.

The following are the various types of scanners:

i) Port Scanners: Using scanners, you can find out which ports are open and which ones are closed by scanning the ports. Also on their search list is information on the operating system and the services that are provided by the company.
ii) Application Scanners: It is necessary to scan a network application in order to detect vulnerabilities that could be exploited in order to compromise the entire system. Scanners for network applications are used to do this.
iii) Susceptibility Scanners: System flaws that could be exploited by a hostile user or hacker are sought after by violation scanners, which put the entire network system at risk of being hacked or otherwise compromised.

Through this paper we are focusing on the vulnerability scanning tools which are supporting to the network security. Aim of writing this paper is that individual as well as organizations are aware of different antivirus software and theses are commonly is practice for security. Vulnerability scanning tools are not extensively used in practice.

Further, this paper will support to select the proper vulnerability scanning tool as its features and coverage is varying according to different companies.

II. REVIEW OF EXISTING SURVEY ON VULNERABILITIES TOOLS FOR NETWORK SECURITY

Here author W. Alosaimi and colleagues throughout the current era of information technology, there are many new concepts to learn about, such as cloud computing, big data, the internet of things (IoT), and artificial intelligence. Customers and businesses are connected through a large number of service-related service information systems that were not designed specifically for this purpose by enterprises. [8]

Author W.M. Ma outlines information security attack and defence exercises in order to obtain a better understanding of the enterprise's external service information system. Internet penetration testing tool Hydra is well-known for identifying vulnerabilities in websites, and it is used by professionals to identify such problems. In the meantime, fresh investigators can obtain hands-on experience with website vulnerabilities, which will help them to improve their website penetration capabilities. [9]

In the research of WM Ma (William Ma) (2019) Even though they have significant limits in terms of scalability, functional engineering effort, and accuracy, old-style machine learning techniques have been frequently utilized in interruption discovery systems for years. Deep learning algorithms, which are particularly effective in the realm of enormous data, can be used to address these issues as a result of their efficiency. Deformation resistance and the elimination of the necessity for manual manufacturing are all advantages of deep learning. LSTM networks, as proposed by Diro and others, are used for dispersed network threat detection in the context of fog-to-object communication.[10] We discover and analyze important IoT device attacks and threats, focusing on the usage of wireless communication weaknesses. Experiments in two examples show that the depth model outperforms the classic machine learning model in terms of effectiveness and efficiency.

Work of Bailey C (2014)*et al.* presents trust-enhanced distributed authorization architecture as a holistic framework. When determining whether or not a platform can be relied on for permission, the technique considers both "hard" and "soft" concepts.[11] After providing an explanation of the reasoning behind the general model, the hybrid model with "hard" and "soft" trust components is detailed in further detail. Following that, the proposed architecture is put into action in the context of online service authorization. Specifically in a scattered situation, the findings indicate that the proposed technique facilitates more effective decision-making about permission. The authors of this paper investigate the possibility of authorization assets being automatically adapted to handle federated authorization infrastructures in the future (policies and subject access rights). SAAF (Self-Adaptive Authorization Framework) is a federated role/attribute management system that is based on policies for gaining access to and controlling authorization infrastructures. SAAF is a project of the National Institute of Standards and Technology.[10]

Here author R. Shanmugapriya et al. says due to the vulnerability of networks to denial-of-service attacks, security has garnered considerable attention. Although network administrators have taken every precaution to ensure network security, the system is sufficiently secure to conduct dispersion testing. This is the most efficient

method of determining whether a system is vulnerable. Network security cybercrime technologies have brought a lot of positive things to the internet. With the most technological advancements, there is also a criminal hacker. [12]

Research work W. Alosaimi and colleagues presents an organization's exploits and vulnerabilities can be discovered through penetration testing, which is carried out on their computers. The information technology infrastructure contains security measures that contribute to the efficacy or ineffectiveness of the infrastructure. When weighed against the possibility of operational system failures, the greater expenditure in security controls makes more sense than previously thought. It is critical that penetration testing be carried out in a way that closely resembles a real-world attack.[13,14]

Focusing on the work of penetration testing L. Qing and his colleagues elaborate that a penetration tester rarely has the luxury of doing so, and a real-world attacker frequently spends months researching a target before launching an assault on it. All penetration tests are carried out in the same manner, regardless of whether or not an attack profile is being replicated in the laboratory. In order to acquire a target, the tester must first gather information about it. [15]

It is possible to create a natural mapping between discrete vulnerability measures and components from the larger spectrum of security skills under consideration, which includes: technical, user-oriented, and management-oriented security competencies. This can be accomplished using the CVSS version 3 framework. The CVSS score is used by the assessor to establish the level of vulnerability based on the information that is available at the time the assessment is performed. Among the CVSS Base metrics are the CVSS Base metrics (columns CVSS and Metric description), as well as the numerous values supplied by an assessor, which are summarised in Table 2. (Column Values) With the exception of the Scope metric, these are all of the metrics that the CVSS use in order to evaluate the severity of security vulnerability. [17-19] Here we have provided a brief summary of the technical abilities connected with the specific metric (Skill set), as well as a mapping of those technical abilities to the Knowledge Units defined by the American Computer Society's Joint Task Force on Cyber security Education.

Table1. A comparison of the susceptibilities noticed by several scanners is presented. [24]

Vulnerabilities	**Nmap**	**Nessus**	**Acunetix WVS**	**Nikto**	**Burp Suite**
SQL Injection	√	√	√		√
Inadequate Error Management.	√	√	√		√
Scripting on many sites.	√	√	√	√	√
Servers acting erratically	√	√		√	
Denial of Service	√	√	√		√
Execution of Code through the Internet.		√			
Identifier for the format string.		√	√		√
IIS printer		√	√		√

Table 2. Software vulnerability assessments are subjected to an accuracy evaluation.

CVSS	Metric Description	Values	Skill Set	Mapping
attack vector (AV)	The attack vector. The maximum distance an attacker can go to deliver an attack against a vulnerable component is indicated by this value. The higher the score, the greater the distance travelled.	Physical, Local, Adjacent Network.	As a result, the assessor is knowledgeable about the technical causes and attack vectors associated with software vulnerability. Among these include an awareness of susceptible settings, the delivery of local and remote attacks, and other aspects of the attack engineering process	Software Security: This course covers topics such as connectivity security (distributed system architecture, network services, and network defence); data security (data integrity and authentication, secure communication protocols); and network security (distributed system architecture, network services, and network defence).
Privileges Required (PR)	Required Privileges. Reflects the privileges required for an attacker to exploit the susceptible component on the affected system.	High, Low, None.	The assessor is well-versed in the relationship that exists between the vulnerable system, the user, and the attack, among other things. For example, spear-phishing efforts or users who do not pay attention to alerts.	The following subjects are discussed: Fundamental Principles, Implementation, Design, and Documentation of Software Security; Data Security: Data Integrity and Authentication.
Access Control (AC)	The difficulty of the attack. This indicates the presence of circumstances	High, Low.	local and remote attack delivery	Data Security: {Data Integrity and Authentication}

	that are required for the attack to succeed but are beyond the control of the attacker.			
User Interaction (UI)	Interaction with the User is important. The requirement for user engagement in order to launch a successful attack is represented by this symbol.	Required, None.	security problem over business transaction and data transmission	Data Security: {Data Integrity and Authentication}
Confidentiality (C)	Confidentiality. This method is used to determine the effect on the secrecy of information on the impacted system.	None, Low, High.	A security breach's impact on business-critical concerns such as data filtration and system performance can be quantified by assessors.	Software Security: {Deployment and Maintenance, Documentation, Implementation, Fundamental Principles}; Data Security: {Data Integrity and Authentication, Secure Communication Protocols}
Integrity (I)	Integrity. Calculates the implications of the impacted system's failure on the integrity of data stored on the impacted system.	None, Low, High.	Vulnerable systems for Remote healthcare monitoring Evaluation with real data.	Data Integrity and Authentication, Secure Communication Protocols are some of the terms used to describe data security.
Availability (A)	Availability. This function computes the impact on the component's availability.	None, Low, High.	interplay between a susceptible system, its user, and an intruding attacker	Software security covers a variety of subjects, including deployment and maintenance, documentation, implementation, and fundamental principles.

III. DISCUSSIONS AND FUTURE DIRECTION

In this part, the Susceptibility Valuation and Penetration Testing (VAPT) of many approaches are described in depth in Table 2 along with Figure 2. From the obtained data, it is obvious that the Partially Observable Markov Decision Process (POMDP), and Reinforcement Learning techniques beat the Mixed Initiative Planning and Scheduling Agent (MIPSA) and Host Clustering models in terms of accuracy. In addition, the POMDP and RL have identified the effective VAPT process over the other methods in a considerable way. Followed by, the POMDP technique has accomplished maximum confidentially over the other methods. Finally, all the compared methods have studied equivalent performance in terms of accuracy performance.[20-23]

Table 2 Performance Analysis (%) of Various VAPT Methods

Network Size	Accuracy Performance metrics (%)			
	POMDP	MIPSA	RL	Host Clustering
VAPT on 10 Machines	91.21	89.76	90.18	88.45
VAPT on 20 Machines	91.67	89.78	90.32	88.77
VAPT on 30 Machines	91.87	89.81	90.38	88.91

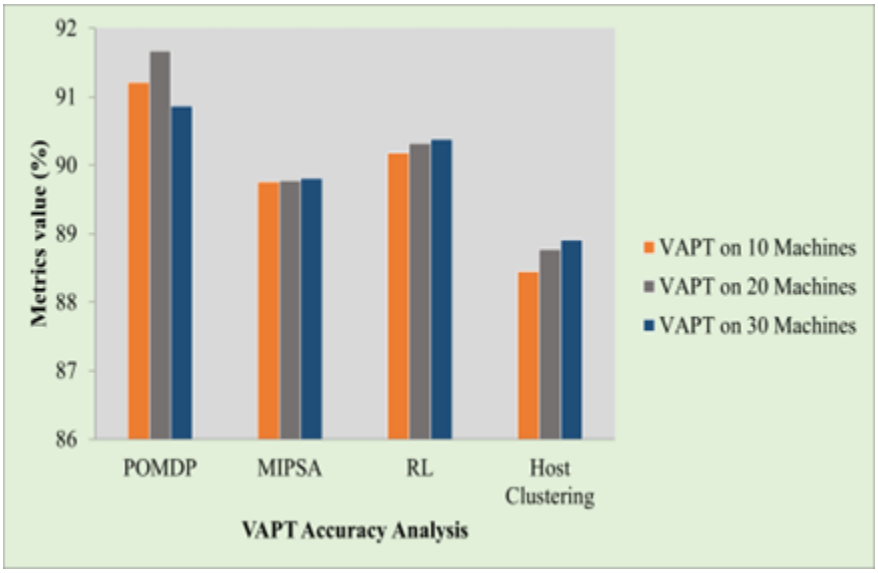


Fig.2 VAPT Accuracy Analysis of various methods

In Fig 2. For instance, the POMDP, RL methods have obtained higher accuracy of 91.21% and 90.18% for VAPT on 10 machines. whereas the MIPSA and Host Clustering methods have showcased lower accuracy of 89.76% and 88.45% for VAPT on 10 machines. Moreover, the POMDP and RL has resulted in maximum accuracy performance of 91.67% and 91.87% for the VAPT on 20 and 30 machines respectively. Finally, because VAPT continues to outperform the time typically allotted to PT experts on relatively large networks, we intend to improve on the current version by developing a hierarchical POMDP model of PT practice in which large networks are initially segmented (clusters) according to a security-oriented approach and the overall POMDP environment contains the cluster representation rather than a representation of all machines, as is currently the case. This technique is expected to address two critical testing challenges: performance optimization as a result

of the system dealing with multiple small POMDP problems rather than a single large and complex environment, and reliability optimization as a result of the system dealing with multiple small POMDP problems rather than a single large and complex environment. A different approach is to use a hierarchical technique that simplifies and optimizes the process of gathering and processing information as attack vectors at two levels: clusters and future machines, and that can be applied at two levels: clusters and future machines, depending on how the network is modified.

IV. CONCLUSION

In this study, we specifically looked at how Vulnerability Assessment and Penetration Testing (VAPT) could be employed as a form of cyber defence against various threats with respect to network of organization. Here we have covered the brief idea of network vulnerability scanning process. We went over the entire life cycle of VAPT, as well as the most common VAPT approaches and the top vulnerability assessment tools. This Vulnerability Assessment and Penetration Testing, as well as their usage as a cyber defence technique, are covered in detail in this article. Paper focuses on the different techniques that are used by the researchers in the area of machine learning and deep learning. Basic comparison of the various vulnerability scanning tools with respect to performance analysis is elaborated. This gives a clear Idea that VAPT is an essential component of cyber defence and should be considered as such. This paper explains why increasing the use of VAPT is critical for total system security. Performance Analysis gives a clear idea that the development of new VAPT approaches and tools would be beneficial for better scanning in a less duration with increased number of system or machines. This status of the paper VAPT is a cutting-edge cyber-defence technology. Compulsory VAPT testing can help prevent cyber-attacks in the future as well as bolstering network security.

V. REFERENCES

[1]. Wu YX, Wang HF. Computer network information security risks and protective measures against the background of big data. J Luohe Vocat Tech Coll. 2019;4:20–2.

[2]. Xiao-Xia W. Research on information security architecture of computer network. Digital Technol Appl. 2018;36(12):181–2.

[3]. Harshdeep Singh, Dr.Jaswinder Singh, “Penetration testing in wireless networks”, International Journal of Advanced Research in Computer Science, 8 (5), May-June 2017, pp. 2213-2216 .

[4]. Dongying L, Baohai Y. Research on information security strategy based on wireless network access. Digital Technol Appl. 2018;36(11):191–2.

[5]. Prashant S. Shinde, Prof. Shrikant B. Ardhapurkar, “Cyber Security Analysis using Vulnerability Assessment and Penetration Testing”, Presented at IEEE Sponsored World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR’16), 2016.

[6]. Wang, Yien, and Jianhua Yang. "Ethical hacking and network defense: Choose your best network vulnerability scanning tool." 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA). IEEE, 2017

[7]. Harrell, Christopher R., et al. "Vulnerability Assessment, Remediation, and Automated Reporting: Case Studies of Higher Education Institutions." 2018 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, 2018.

[8]. Alosaimi W, Zak M, Al-Begain K, Alroobaea R, Masud M. Mitigation of distributed denial of service attacks in the cloud. Cybern Inf Technol. 2017;17(14):32–5.

[9]. Ma WM. Research on website penetration test. Glob Bus Manag J. 2019;11:121–32.

[10]. Wang, Liwei, Abbas, Robert, Almansour, Fahad M., Gaba, Gurjot Singh, Alroobaea, Roobaea and Masud, Mehedi. "An empirical study on vulnerability assessment and penetration detection for highly sensitive networks" Journal of Intelligent Systems, vol. 30, no. 1, 2021, pp. 592-603. https://doi.org/10.1515/jisys-2020-0145

[11]. Bailey C, Chadwick DW, de Lemos R. Self-adaptive federated authorization infrastructures. J Comput Syst Sci. 2014;80(5):935–52.

[12]. Shanmugapriya R. A study of network security using penetration testing. 2013 international conference on information communication and embedded systems (ICICES). IEEE; 2013, February. p. 371–4.

[13]. Alosaimi W, Zak M, Al-Begain K, Alroobaea R, Masud M. Economic denial of sustainability attacks mitigation in the cloud. Int J Commun Netw Inf Security. 2017;9(3):420–4314.

[14]. Alosaimi W, Zak M, Al-Begain K, Alroobaea R, Masud M. Mitigation of distributed denial of service attacks in the cloud. Cybern Inf Technol. 2017;17(14):32–5.

[15]. Qing L, Boyu Z, Jinhua W, Qinqian L. Research on key technology of network security situation awareness of private cloud in enterprises. In 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA). IEEE; 2018. pp. 462–6

[16]. Allodi, L., Cremonini, M., Massacci, F. et al. Measuring the accuracy of software vulnerability assessments: experiments with students and professionals. Empir Software Eng 25, 1063–1094 (2020). https://doi.org/10.1007/s10664-019-09797-4

[17]. Kyriakos Kritikos *, Kostas Magoutis, Manos Papoutsakis, Sotiris Ioannidis .A survey on vulnerability assessment tools and databases for cloud-based web applications. www.elsevier.com/journals/array/2590-0056/open-access-journal. https://doi.org/10.1016/j.array.2019.100011

[18]. Jai Narayan Goela, B M Mehtre Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. Peer-review under responsibility of organizing committee of the 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015) doi: 10.1016/j.procs.2015.07.458

[19]. Sowmyashree A, Dr. H S Guruprasad, "Evaluation and Analysis of Vulnerability Scanners: Nessus and OpenVAS" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

[20]. Mohamed C. Ghanem ,Thomas M. Chen "Reinforcement Learning for Efficient Network Penetration Testing" Information 2020, 11, 6; doi:10.3390/info11010006 www.mdpi.com/journal/information.

[21]. Jonathon Schwartz, Hanna Kurniawati "Autonomous Penetration Testing using Reinforcement Learning", arXiv.org- cs- arXiv:1905.05965

[22]. Zhenguo Hu, Razvan Beuran, Yasuo Tan, “Automated Penetration Testing Using Deep Reinforcement Learning” 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)

[23]. Dean Richard McKinnel, Tooska Dargahi, Ali Dehghantanha, Kim-Kwang Raymond Choo, A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability

assessment, Computers & Electrical Engineering, Volume 75,2019,Pages 175-188, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2019.02.022.

[24].Sheetal Bairwa, Bhawna Mewara and Jyoti Gajrani Vulnerability Scanners-A Proactive Approach To Assess Web Application Security Article in International Journal on Computational Science & Applications · March 2014 DOI: 10.5121/ijcsa.2014.4111 · Source: arXiv

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Bots, Botnets and Zombies: Anatomy, Inhibitory Measures and Threat Prevention Techniques

Hrushikesh Sanjay Walvekar[1], Anuradha Kanade[2], Shubhangi Gautam[3], Shrushti Jagtap[4]
[1]EC-Council Certified Security Analyst, TYMCA (Science), MIT - World Peace University, Pune, Maharashtra, India
[2]Head MCA (Science), MIT - World Peace University, Pune, Maharashtra, India
[3]UX Intern, Hexanika, TYMCA(Science), MIT World Peace University, Pune, Maharashtra, India
[4]Intern at Tata Elxsi, TYMCA (Science), MIT - World Peace University, Pune, Maharashtra, India

ABSTRACT
Considering recent times, botnets have become the emerging and resistant threat to the cyber security world. This infrastructure has not only impacted the users, companies and organizations with loss of data and devices, but also the privacy of using the services without any fear, as well as leading to the increasing day by day cyber-attacks. This paper focuses on various trends of Bots and Botnets causing recurring damages to the systems of the people and turning those systems into zombies in order to achieve certain goals of the attacker (in other words known as a black hat hacker). What are these goals? What is the purpose of these bots and botnets? All these things are elaborated further in order to analyze certain threats and to take precautions so that the system of any person does not get infected.
Keywords— Bots, Botnets, Zombies, Cyber-attacks.

I. INTRODUCTION

We are living in a prevalent and entrenched era of digital communications, Internet of Things and all kinds of tiny mobile-like devices. It's not only very hard to corner the habit of using but also the increasing dependency on such gadgets. It has not only made our lives easier and convenient but has also given the luring environment to security challenges.
News about internet crimes is never too less and terms like “bots”, “botnets” and “zombies” are not so uncommon. It's not very tough to fathom these terms that these are network, internet or security related threats. Due to the increasing use of interconnected system devices and services the type and pattern of such kinds of attacks is constantly changing.
Spamhaus Malware Labs identified a total of 3,559 new botnet Command & Control servers in 2020 [24]. Most people have heard about these terms but very few are unaware of the fact about how they work or how big of a threat they actually are. They are not just a dangerous threat to computer networks and the Internet, but are an

open door to other types of threats and attacks (e.g. DDOS) as well. In Craig Schiller and Jim Binkley's words botnets are "arguably the biggest threat that the web community has faced" [2].
Therefore, its detection has become a bigger challenge to overall network security.

II. BOTS

The term Bot derived from "robot" is a type of automated software [2]. It was originally used by the Internet Relay Chat (IRC) Community to perform mundane tasks like the type and pattern of such kinds of attacks is constantly changing. For example- The IoT botnet Mirai had a growth of approx. 143,000 occurrences to 225,000 occurrences from 2018 to
2019 alone[3].
Some of the common bots are:

- GTbot, easy to rewrite or edit, develops its own variations. Its ports are configurable. Platforms are Windows xp, 95, 98, NT, ME, 2000[4].
- Evilbot, typical size of compressed file is 15.904 bytes. Its ports can be changed. Platforms are Windows xp, 95, 98, NT, ME, 2000[4].
- Slackbot, ports can be changed [4]. These platforms include all the windows versions with IRC software.

III. BOTNET CLASSIC ARCHITECTURE

A. BOTNET STRUCTURE:

Botnet Structure consists of three parts: Bot, Botmaster and the Command and Control Channel.
Bot- is a file that, when triggered by specific commands, performs a set of functions. When a bot is installed onto a system, it copies itself and changes the configuration of a system to start each time it bots. Notably, bots do not exploit the system directly but are the means used to install backdoors once a system has been compromised.
Botmaster- A botmaster which is also known by the name botherder, is a person or a group of people, who controls the botnet remotely as well as all the commands or directions to the compromised computers in the botnet.
Command and Control Channel- It comprises several servers and technical components which take the commands from botmasters to the bots and deliver back the information from the bots. It is abbreviated as C&C servers [5].

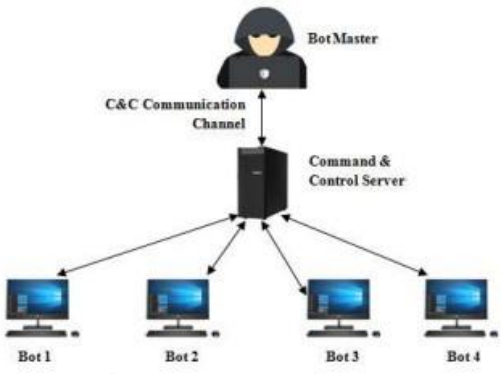


Fig. 1 Basic Structure of bot network[12]

B. CLASSIC BOTNET ARCHITECTURE

Usually, a typical user thinks that whenever his system gets compromised or attacked, he will know about it or the system's behavior will make him informed. But that's not the case [6]. When an attacker first establishes a control over the targeted computer, he does not get the access to control that system at firsthand. The common bot activity will not get visible on compromised computers, unless the victim uses any network traffic capture tools.

In a botnet, the attacker first initiates a Command & Control server. Then he sends tiny bots (in the form of codes that can be copied infinitely) to the computer, via the Internet, which acts like a carrier for botmasters. Once the bot finds a vulnerable machine and successfully infects it, the bot sends back the request to the C&C as a step to successfully complete the channel, making it clear that the machine has become a *zombie[6].*

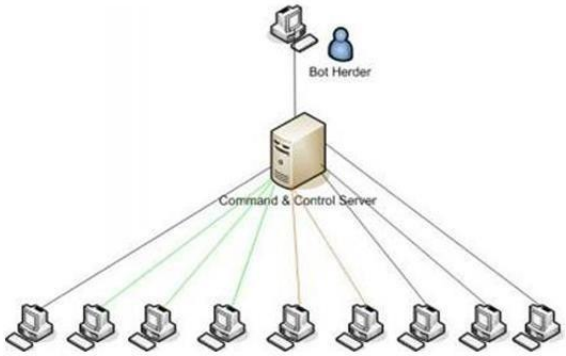


Fig. 2 Working of Botnet[23]

C. LIFE CYCLE OF BOTNET

a. Spreading and Injection
b. Communications stage
c. Attack stage

IV. CHARACTERISTICS OF BOTNETS

Characteristics of botnets can be classified on the basis of their structure, technology and behavior.

A. Structural Characteristics:

It explains the structure/topology on which the botmaster establishes the connection between him and the targeted computer[5]. It bridges the connection between the botmaster and the target computer. This characteristic explains the topology of C&C servers organised between the two points[5]. On the basis of this, there are two ways of communication between the bots and the zombies:

1- Centralized C&C: In this approach, the connection between the bots and the C&C server provides the commands which in turn helps to send back the response[5]. The botmaster and the C&C server must stay connected, which will help the bots in receiving the command to perform any task. However in this type of setting, botnets are created in a very simple way, are fast and easy to manage as well, being its point of failure[7]. This approach is further divided into two approaches based on the protocols it uses, namely: IRC-based and HTTP based. Different centralised topologies used in botnets are star, hierarchical, and multi server[7].

2- Decentralized C&C: This approach is drawn on the p2p model [5]. Here, every compromised system is represented as a C&C server and as a bot at the same time, and establishes a connection between the other bots to send and receive commands. Here no central server is present, instead every system is a server and a bot as well [5].

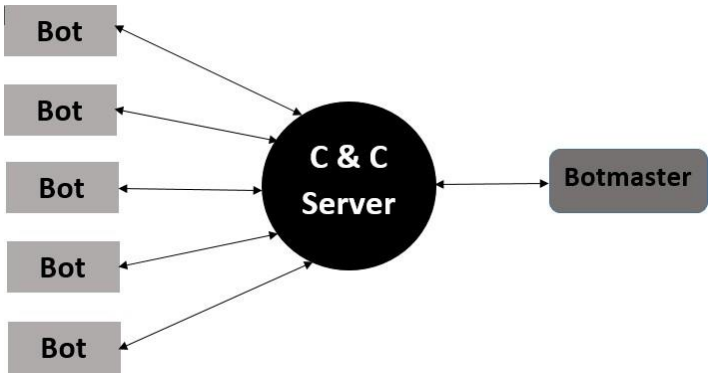


Fig. 3 Centralized C&C

V. BOTNET DETECTION

Techniques to detect botnets are divided into two categories: Honeypot-based detection and Network-based detection [9]. Honeypot is a resource which lies in unauthorized use of resources to lure the attackers and get their details [9].

VI. NEW GENERATION BOTNETS

The new generation bots and botnets are made up of advanced techniques to take over the systems of the users. Artificial intelligence and machine learning is used for creating those bots and botnets. Recent infrastructures of botnets are:

A) Cloud Botnets: Instead of spending a lot of time infecting victims having networks and computers, they have the option to rent a cloud service [10].

B) Mobile Botnets: Botnets are migrating to mobile infrastructures due to the widespread usage of mobile devices and the Internet. As a result, mobile technologies such as SMS/MMS and Bluetooth are used to develop new generations of C&C models. According to this research, over the first six months of 2011, 40,000 compromised mobile devices spoke with cybercriminal command and control sites [10].

VII. PREVENTION OF BOTNETS

There are many ways to follow in order to prevent our network from having any botnet attack. Every way is different but has its merits and demerits as the techniques are based on the network specifications and would not be compatible with the new generation of botnets. Any change in C&C architecture might make the technique inapplicable. Hence, it's a good option to develop techniques which are based on DNS traffic and data mining. So, here are some preventive measures that users can follow to prevent the system from any virus infection. So, they are as follows-

A) Install anti-virus or any good anti-spyware to secure the system from attacks [11].

B) Keep the software updated to improve the security and performance.
C) Update your passwords regularly.
D) Keep your firewall enabled [11].
E) Deploy a good IPS (Intrusion Prevention System) [11]

VIII. ZOMBIES

The zombies are created by the compromised systems which are controllable by a bot. The bots reside in a compromised system and exploit it, in other words all the controls of a particular system are handed over to the bot agent software. These zombies are used for self-launching zero-day exploits and stack overflows as well as buffer overflows in order to achieve a certain goal by attacking a target.

IX. CONCLUSIONS

The bots, botnets, zombies are very useful in certain cases if we use them for legal as well as good purposes. Botnets are very interesting subjects for any security researcher. If we focus on the features of botnets then there is a lot of variety in botnets topology and protocols which are used. Signature-based, DNS-based, anomaly-based, and data-mining-based solutions are all available. Botnets are detected using signature-based techniques based on passive network traffic monitoring. There are various loopholes and unchecked open methods in all of these techniques for preventing bots, botnets, and zombies that allow attacks to succeed.

X. REFERENCES

[1]. Prof. Predicting Number of Zombies in a DDoS Attack Using ANN Based Scheme by B.B. Gupta1, 2, R.C. Joshi1, M. Misra1, A. Jain2, S. Juyal2,R. Prabhakar2, and A.K. Singh2
[2]. Net of the Living Dead: Bots, Botnets and Zombies by David Harley BA CISSP FBCS CITP Andrew Lee CISSP Cristian Borghello CISSP.
[3]. A Survey on Botnets: Incentives, Evolution, Detection and Current Trends by Simon Nam Thanh Vu, Mads Stege, Peter Issam El-Habr,Jesper Bang.
[4]. Bots and Botnet: An Overview by Ramneek Puri (SANS/GIAC Certifications Whitepaper)
[5]. An overview of botnet and its detection techniques by Sarath R Mammunni1, Sandhya C P.
[6]. Understanding and Blocking the New Botnets, researched by Corey Nachreiner, written by Scott Pinzon.
[7]. Bots and botnets: An overview of characteristics, detection and challenges by Meisam Eslahi, Rosli Salleh, Nor Badrul Anuar.
[8]. Prediction of Number of Zombies in a DDoS Attack using Polynomial Regression Model by B. B. Gupta, R. C. Joshi, and Manoj Misra
[9]. The spread of misinformation by social bots by Giovanni Luca Ciampaglia, Chengcheng Shao, Alessandro Flammini, Onur Varol, and Filippo Menczer.
[10]. The spread of fake news by social bots by Chengcheng Shao, Giovanni Luca Ciampaglia, Onur Varol, Alessandro Flammini, and Filippo Menczer

[11]. Security threats/attacks via botnets and botnet detection & prevention techniques in computer networks: A Review by Emerald Simkhada Elesha Shrestha Sujan Pandit Upasana Sherchand.
[12]. Are social bots a real threat? An agent-based model of the spiral of silence to analyse the impact of manipulative actors in social networks by Björn Ross, Laura Pilz, Benjamin Cabrera, Florian Brachten, German Neubaum & Stefan Stieglitz.
[13]. Botnet Detection Techniques by Jihan Barazi, Ahmad Jakalan, XiaoWei Wang.
[14]. Study of Botnets and their threats to Internet Security by M. Tariq Banday, Jameel Qadri.
[15]. A Study on BOTNET Attacks and Detection Techniques by Yogita Barse1, Dr. Sonali Tidke2.
[16]. Overcoming botnets, zombies and iot security breaches by Deepinder Singh.
[17]. A Survey on Botnets and Web-based Botnet Characteristics by Maryam Rahimipour1, Dr. Shahram Jamali2
[18]. Survey on Botnet Detection Techniques: Classification, Methods, and Evaluation by Ying Xing, Hui Shu, Hao Zhao, Dannong Li and Li Guo.
[19]. The zombie roundup: understanding, detecting, and disrupting botnets by Evan Cooke, Farnam Jahanian, Danny McPherson.
[20]. A Botnets Circumspection: The Current Threat Landscape, and What We Know So Far by Emmanuel C. Ogu, Olusegun A. Ojesanmi, Oludele Awodele, Shade Kuyoro.
[21]. Could Social Bots Pose a Threat to Public Health? by Shelly Choo, Leana S. Wen.
[22]. Botnet detection using graph-based feature clustering by Sudipta Chowdhury, Mojtaba Khanzadeh, Ravi Akula, Fangyan Zhang, Song Zhang, Hugh Medal, Mohammad Marufuzzaman & Linkan Bian.
[23]. https://www.google.com/search?q=working+of+botnet&tbm=isch&ved=2ahUKEwjIo-2445P2AhUQKrcAHX_OC-8Q2-cCegQIABAA&oq= working+of+botnet&gs_lcp=CgNpbWcQAzIHCCMQ7wMQJzoGCA AQBxAeOgYIABAFEB5Q2glYkiNgoyhoAHAAeACAAccBiAH2E5I BBDAuMTmYAQCgAQGqAQtnd3Mtd2l6LWltZ8ABAQ&sclient=im g&ei=fBUVYsj1H5DU3LUP_5yv-A4&bih=657&biw=1366#imgrc=X WQu1G8A2ojHOM https://www.spamhaus.org/news/article/800/spamhaus-botnet-threat-up date-q2-2020#: ~:text=Number%20of%20botnet%20C%26Cs%20obser ved%2C%20Q2%202020

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Smart Traffic Control Signal System using IR Sensors

Parshv Meher, Tanmay Mahajan, Pranav Mandke, Prof. Vidya Patil
School of Computer Science and Engineering, Dr.Vishwanath Karad MIT-World Peace University, Pune, Maharashtra, India

ABSTRACT
Today's world is full of traffic, where everyone is in a hurry to reach somewhere. While traveling from one place to another, frustration is experienced due to the huge traffic jams but one thing which gets overlooked is how the traffic is managed at a particular traffic signal. At such times, the frequently faced problem is the need to wait on a traffic signal for a long time. Sometimes even though no vehicles are passing by and the traffic is not dense enough - people have to wait for a fixed time duration until the traffic signal goes GREEN. This might not seem like a major issue but if a bigger route is under consideration, it might turn out to consume a lot of time, fuel, and energy. The Smart Traffic Signal System provides a solution to this problem. It is designed to develop a density-based traffic signal system wherein the signal timer changes automatically according to the traffic density at that particular signal. The higher the density of vehicles – the greater is the signal timer. Infrared Sensors (IR) Sensors are used to provide an optimized solution. It dynamically calculates the traffic levels at a particular signal using IR sensors and accordingly calculates the signal timer in real-time. This not only saves time and fuel for an individual but also regulates the vehicle movement passing thereby preventing traffic accumulation. For the proposed system, the microcontroller used is Arduino Mega. Existing work makes use of image processing and data analysis - with a lot of computing as well as hardware requirements. The proposed approach as compared with the existing work is not only easy to implement but also requires fewer computations and the output obtained is just what is required.

Keywords— Infrared Sensors, Arduino Mega, Dynamic Traffic, Smart Traffic Signal.

I. INTRODUCTION

As India is becoming one of the fastest-growing economies in the world, the average income of the Indian people is growing day by day leading to an increase in the number of private vehicles. Though having wide public transport, still it is not sufficient enough for the large population of India. Often public transport services remain crowded especially in India's metro cities. To have peaceful travel people usually prefer commutation using their private vehicles. It is the main cause for more vehicles to come on the roads. This is one of the major reasons for traffic jams in India's urban cities. There are other causes like poor quality of roads, lack of parking spaces, and lack of footpaths which add up to the reason for traffic jams in India [1]. One of the solutions for this problem is

the proper management of traffic density at traffic signals. In an era where everything is going smart, it is necessary to make traffic signals smart. A smart traffic management system is proposed with an objective to dynamically allocate the waiting times at the traffic signal using signals received from the IR sensors. The sensed data from all sensors is collected by the Arduino Mega which further calculates the waiting time.

II. LITERATURE SURVEY

In the past few years, many kinds of research are going on to prevent this problem of traffic jams. For example, using various sensors and microcontrollers to automate the process of traffic light switching, manual traffic light controller, and so on. Ganiyu R induced a traffic light control system with a microcontroller and light-emitting diode (LED) in the year 2014. On passage of a vehicle, its weight was sensed by a pressure switch indicating a logic one instruction to the microcontroller. On every detected logic one, a time of 15 seconds was added to the timer which further triggered the LED to light on an additional delay of 15 seconds for that particular traffic signal lane [2].

The system proposed by Rani et al [3] consists of IR- Sensors, along with a Wi-Fi transmitter, and a Raspberry Pi microcontroller. The sensed data is transmitted by the Wi-Fi transmitter which gets received by the Raspberry pi controller. Vehicular Adhoc Network (VANET) was used which causes flooding in the route discovery phase, wasting bandwidth leading to delayed signals along with increasing network congestions. The model is quite expensive and the level of utilization is low as some of the existing models required knowing the geographical nature along with the road conditions of the implementation sites.

Dzulkefli et al. [4] detected the density of the traffic in the traffic signal system with Arduino UNO and IR sensors. This system calculates the count of the passing vehicles and assigns a time of 3 seconds to each vehicle. The traffic light changes its color in absence of a vehicle for more than 1 second. It results in the consumption of much more memory as the count of passing vehicles increases. The time allotted to the signal can be very long as it counts the number of vehicles and accordingly sets the time which can cause huge traffic jams at the other traffic signals.

Operations like monitoring of the traffic density flow and volume are done in the model proposed by Ghazal et al. [5] using mainly a PIC microcontroller, IR sensors, X Bee transceivers, etc. When an automobile passes in front of the IR sensor, the system gets activated and the value on the display is incremented. The information is collected in the form of a count on the display which further gets analyzed. Using this information, the system can detect the traffic density and segregate it in 3 ways viz soft, normal & jam. Granting an immediate passage to emergency vehicles like an ambulance or a firetruck is also supported by the system.

Raspberry Pi & OpenCV tool is used in the traffic control management system proposed by Razavi et al. in [6]. The system implemented an instantaneous feedback mechanism using traffic cameras at the crossroads. An image of the vehicle on the road in one direction is recorded by a camera and is provided to the Raspberry Pi board. The overlapping percentage is obtained between the instantaneous traffic image and the reference image. The dynamic waiting timing of the signal is decided by a scheduling algorithm once this information is fed to it.

The model proposed by S. S. R and L. Rajendran in [7] does the job of reducing the cycle time of a traffic signal & also provides a special provision for the passing of emergency vehicles. This is done by a camera-based traffic monitoring system. This model uses high-resolution cameras to get the count of the number of vehicles in the lane and determines the traffic density. When the extraction of data is completed this data is sent to the traffic

control algorithm and it automatically determines the dynamic signal timer value. The model is very efficient and easy to build.

A time-efficient traffic management system based on the traffic density was proposed by Lahari et al. in [8] enabling an emergency override feature for emergency vehicles like police vans, ambulances, etc. The system controls traffic signals based on RF communication, GPS module (for tracing the location of emergency vehicles and managing traffic control according to it for smooth operation), and IR sensors. For traffic density management different priorities were set according to sensor response values and a GPS module positions the results for emergency vehicles. The system can lead to time conservation as it is a fully automatic digital system. However, the use of a GPS module increases the complexity of the system and also tends to push the cost of the system.

Miah et al. in [9] proposed a traffic management system that is helpful for autonomous driving vehicles which are equipped with tons of features like adaptive cruise control, radar system lane keep assist, etc. Many different technologies are employed in this system such as a wireless sensor network, dynamic traffic signal controller, Radiofrequency technology, GPS, GSM to have a smooth functioning of road traffic and also to provide assistance for autonomous vehicles thereby providing intelligent path planning for vehicles. This system might need many government and location regulations. It requires a large investment for practical testing. it is a post-development and futuristic innovation as the development of autonomous vehicles is currently at level-3 and a long journey is yet to be traveled to attain the destination of completely autonomous vehicles. This system might be a boon shortly as time passes and technologies developed Some of the models turned out to be expensive and required additional hardware making the level of complexity high. In practical conditions, most of the systems are affected by human behavioural interferences.

III. PROPOSED SYSTEM

The proposed system consists of an Arduino Mega Microcontroller as shown in Fig.1- based system along with IR sensors, IR LED, and photodiode as shown in Fig.3.a and Fig.3.b.

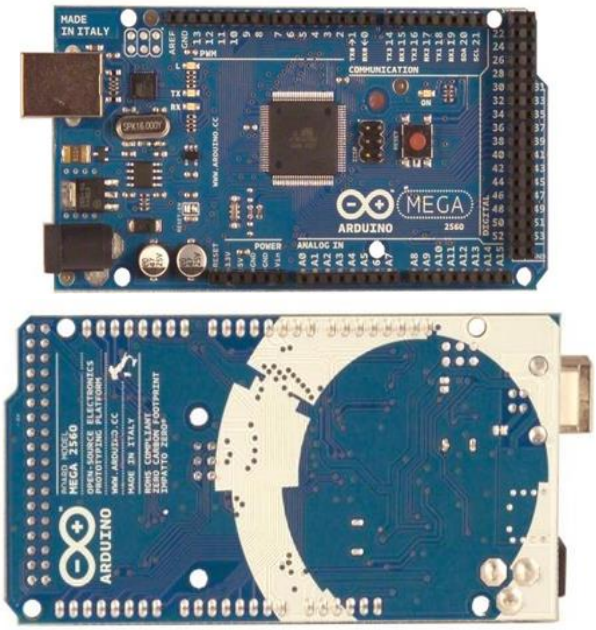


Fig.1. Arduino Mega 2560 Microcontroller

Arduino Mega 2560 is a microcontroller having 54 digital input/output pins,4 UART's, and a 16MHz crystal oscillator. It is a versatile microcontroller and can be used for a variety of applications. External system connections are relatively easy as it provides USB connections. A computer can be readily paired with this microcontroller with the help of a USB cable. Refer to Table.1 for the features of Arduino Mega and Fig.2 for the pin description.

Table.1. Arduino Mega 2560 features

Microcontroller	ATmega2560
Operating Voltage	5V
Input Voltage	7-12V
Digital I/O Pins	54(of which 14 provide PWM output)
Analog Input Pins	16
Flash Memory	256 KB of which 8 KB used by the bootloader
SRAM	8KB
EEPROM	4 KB
Clock Speed	16 MHz

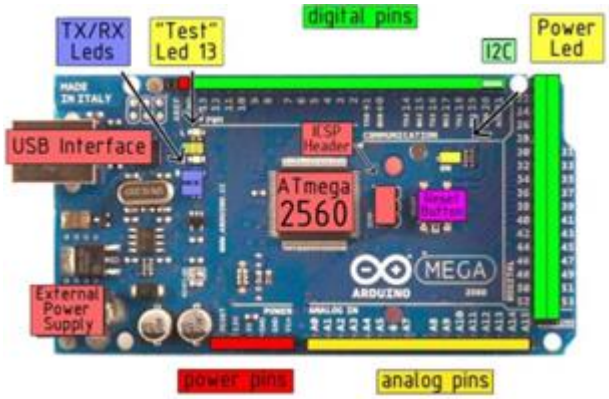


Fig.2. Arduino Mega 2560 pins

IR Sensors help in determining the traffic level and the microcontroller does all the computations to calculate the signal timer and controls the traffic signal.

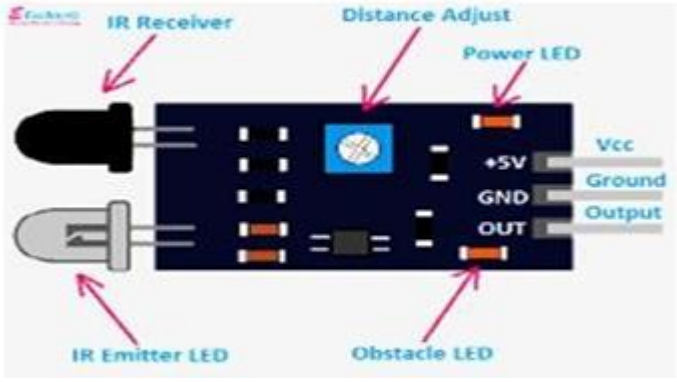


Fig.3a. Infrared (IR) Sensor

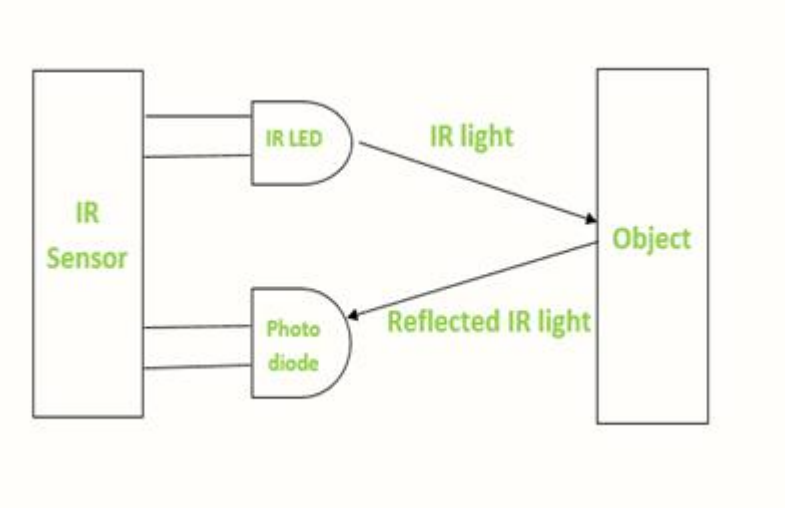


Fig.3b. Infrared (IR) Sensor working

Infrared technology has many wireless applications broadly in object sensing and remote controls. IR sensors as shown in Fig.3.a and Fig.3.b consist of a transmitter and a receiver. The transmitter transmits the light and the receiver keeps on receiving it. Whenever this connection gets interrupted, it initiates the counting process i.e., when the receiver does not receive the transmitted light anymore it is said that an object is present between transmitter and receiver. Using this approach, the traffic level and the signal timer are calculated further. In the proposed system, traffic level is calculated by using IR sensors. The sensors are mounted in the elevated part of the footpath at specific distances from each other as shown in Fig.4. Three IR sensors are used at every lane of a traffic signal as shown in Fig.6.

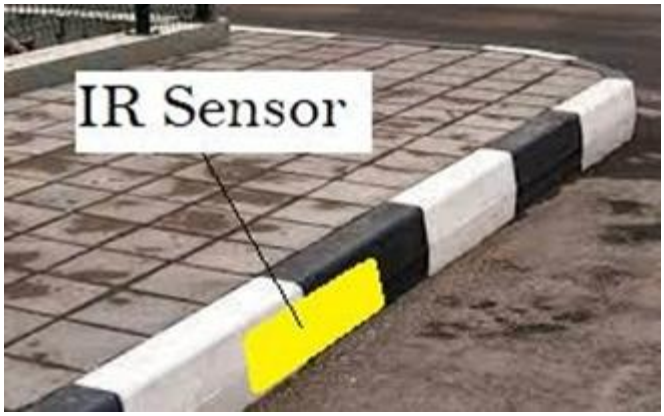


Fig.4.Mounting place of IR Sensor

The mounting of the first sensor is done at a particular distance from the traffic signal. The reason behind this is that the traffic signal has to turn GREEN irrespective of whether there are vehicles in that particular lane or not to maintain the traffic flow. The timer of the signal is kept for a minimum time of 10 seconds. This is done only to prevent the breaking of flow at a particular signal. The traffic levels are defined as NILL, LOW, MOD & HIGH. This level is calculated by checking the sensor values at frequent instances. Fig.7. shows how the signal timer is calculated.

1. If the sensor reading is " low " or " 0 " then it is considered as an object/vehicle is in front of the sensor.
2. If none of the sensor readings is " 0 " then the traffic level is considered as NILL.

3. If the 1st sensor reading is " 0 " then the traffic level is considered as LOW.
4. If the 1st and 2nd sensor's reading is " 0 " then the traffic level is considered as MOD.
5. Similarly, if all three sensors' reading is " 0 " then the traffic level is considered as HIGH.
6. Traffic levels are given integer values viz. NILL=0, LOW = 1, MOD = 2, HIGH = 3.
7. This traffic level value is then used to calculate the timer of the signal. The timer is calculated by,

Signal Timer(in seconds) = Traffic Level * 30 (1)

If the traffic level is equal to " zero ", then in that case the traffic level is considered as NILL, and the signal timer is set to 10 seconds. This is done to maintain the steady traffic flow at the traffic signal.
As shown in Fig.5 the IR sensor range is set in such a way that it will detect objects in that particular lane only and the vehicles in the adjacent lane will not affect the sensor readings.

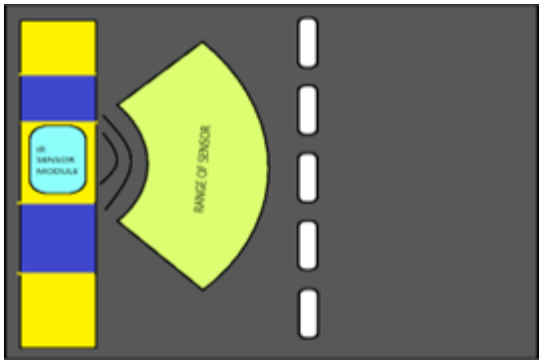


Fig.5. Range of IR Sensor.

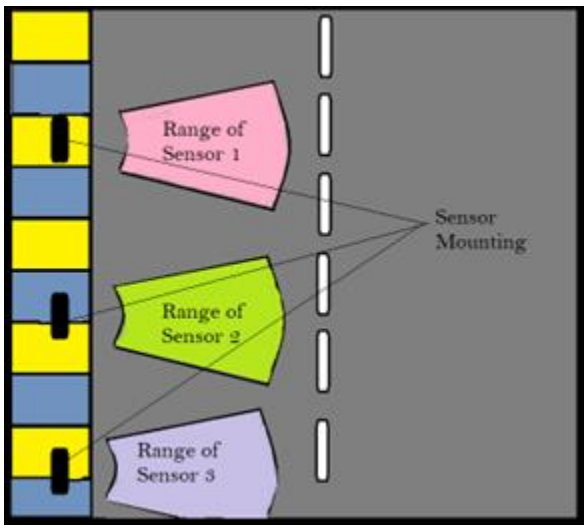


Fig.6.Sensor Mounting at a single lane

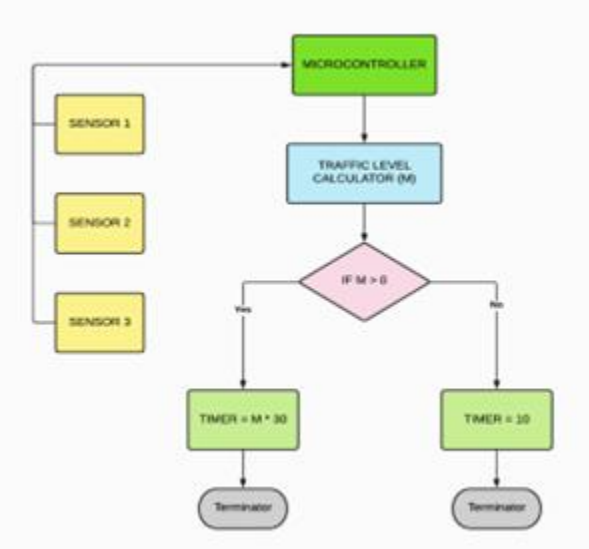


Fig.7.Flowchart for the Process

The algorithm that was used to do the calculations was :

1. set Pin Configuration
2. sensor_value_check( )
3. traffic_level_calculate( )
    a. check flag
    b. if flag =1 then
        i. timer_calculate()
4. set_traffic_timer( )

IV. OBSERVATIONS

This section describes the readings and graphs of a particular traffic signal at one of the chosen squares. From Table.3. Signal No. (i) depicts the iteration number (1 to 10). N and Traffic Level used in Table. 2 represent the count of vehicles and traffic density at that particular traffic signal respectively.

Each sensor can cover the range to fit in around 10-20 vehicles (cars, bikes, rickshaws) depending on the width of the road lane. In the scenarios considered, each sensor could cover the range to fit in around 15 vehicles and hence the traffic intensity were classified in 4 levels as given in Table. 2 below:

Table.2. Traffic Level w.r.t vehicle count

Traffic Level	N(Vehicle count)
NILL	0 < N < 15
LOW (L)	15 < N < 30
MODERATE (M	30 < N < 45
HIGH (H)	N > 45

Time 1: Total time (in seconds) of a general ordinary traffic signal when it is "RED" (in the case considered Time 1 was 60 seconds) for 10 consecutive iterations of traffic signals.

Time 2: Total time (in seconds) of a smart traffic signal when it is "RED" for 10 consecutive traffic signals.

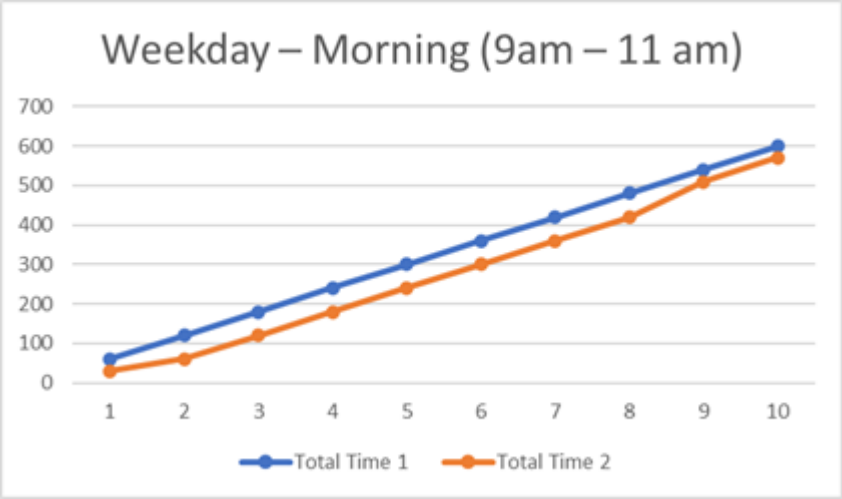
Four scenarios were taken into consideration:

1. Weekday – Morning (9 am – 11 am)
2. Weekday – Evening (9 pm – 11 pm)
3. Weekend - Morning (9 am – 11 am)
4. Weekend – Evening (7 pm – 9 pm)

Tables 3,4,5,6. and Graph.1,2,3,4 shows the observations and comparisons for all 4 cases shown above respectively from case 1 to case 4.

Table.3.Observations on Weekday- Morning (9 am-11 am)

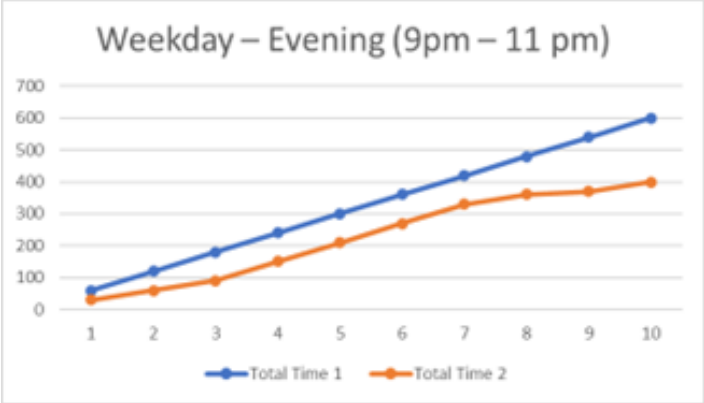
SIGNAL NO (i)	No. of vehicles (N)	Traffic Level	Time 1 (ordinary traffic signal)	Total Time 1	Time 2 (smart traffic signal)	Total Time 2
1	25	L	60	60	30	30
2	26	L	60	120	30	60
3	31	M	60	180	60	120
4	35	M	60	240	60	180
5	33	M	60	300	60	240
6	35	M	60	360	60	300
7	38	M	60	420	60	360
8	37	M	60	480	60	420
9	46	H	60	540	90	510
10	37	M	60	600	60	570



Graph.1. Observations Weekday- Morning (9 am-11 am) Table.4. Observations on Weekday–Evening (9 pm – 11 pm)

Table.4. Observations on Weekday–Evening (9 pm – 11 pm)

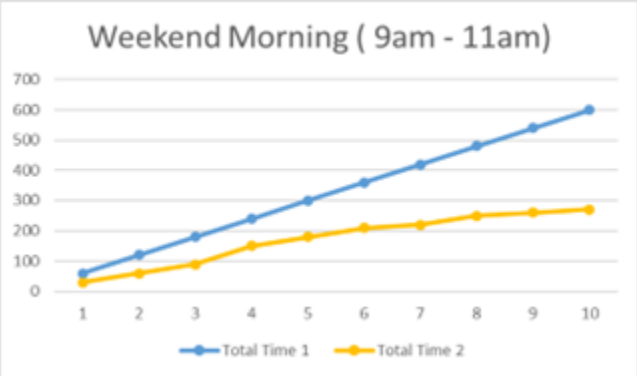
SIGNAL NO	No. of vehicles (N)	Traffic Level	Time 1 (ordinary traffic signal)	Total Time 1	Time 2 (smart traffic signal)	Total Time 2
1	26	L	60	60	30	30
2	21	L	60	120	30	60
3	29	L	60	180	30	90
4	33	M	60	240	60	150
5	31	M	60	300	60	210
6	34	M	60	360	60	270
7	30	M	60	420	60	330
8	28	L	60	480	30	360
9	13	NILL	60	540	10	370
10	22	L	60	600	30	400



Graph.2. Observations Weekday–Evening (9 pm – 11 pm)

Table.5. Observations on Weekend– Morning (9 am–11 am)

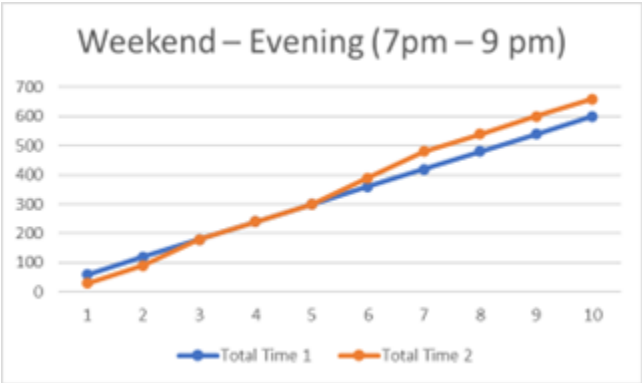
SIGNAL NO	No. of vehicles (N)	Traffic Level	Time 1 (ordinary traffic signal)	Total Time 1	Time 2 (smart traffic signal)	Total Time2
1	16	L	60	60	30	30
2	22	L	60	120	30	60
3	21	L	60	180	30	90
4	31	M	60	240	60	150
5	24	L	60	300	30	180
6	21	L	60	360	30	210
7	13	NILL	60	420	10	220
8	17	L	60	480	30	250
9	9	NILL	60	540	10	260
10	14	NILL	60	600	10	270



Graph.3. Observations Weekend– Morning (9 am–11 am) Table.6. Observations on Weekend – Evening (7 pm – 9 pm)

Table.6. Observations on Weekend – Evening (7 pm – 9 pm)

SIGNAL NO	No. of vehicles (N)	Traffic Level	Time 1 (ordinary traffic signal)	Total Time 1	Time 2 (smart traffic signal)	Total Time2
1	26	L	60	60	30	30
2	31	M	60	120	60	90
3	45	H	60	180	90	180
4	42	M	60	240	60	240
5	39	M	60	300	60	300
6	47	H	60	360	90	390
7	45	H	60	420	90	480
8	38	M	60	480	60	540
9	35	M	60	540	60	600
10	32	M	60	600	60	660



Graph.4. Observations on Weekend – Evening (7 pm – 9 pm)

From the above graphs, it was observed that traffic levels are usually higher in the mornings and evenings. Whenever the traffic levels are LOW and MOD (MODERATE) during any time of the day, the results obtained by the smart traffic signal were time efficient and resulted in less waiting time which in addition helped to prevent the traffic accumulation. Whenever the traffic levels were HIGH, the smart traffic signal resulted in

similar results in comparison to the regular traffic signal system. Thus the model helps in obtaining the optimized results.

V. CONCLUSION

Thus, a smart signal system has been developed and tested using IR sensors. This system is efficient and provides adequate results without much computation and processing. Optimized and efficient signal timer readings are observed.

VI. FUTURE SCOPE

With the increasing traffic in urban areas, a smart traffic management system will help in maintaining proper traffic flow and thereby prevent frequent traffic jams [1]. This will help in reducing fuel and time consumption. Emergency services like ambulances and fire brigades will also get a clear way easily due to the constant flow in traffic. Machine Learning concepts can be implemented by collecting large amounts of data on the number of vehicles passing through the traffic signal. Communication between the signals can be established to set priority in case of an ambulance (or any other emergency) but also if a particular signal has dense traffic in comparison to others

VII. REFERENCES

[1]. https://www.groupdiscussionideas.com/traffic-problems-in-w india/#:~:text=Lack%20of%20parking%20spaces%20is,also%20one%20of%20the%20causes.

[2]. Dzulkefli, Nik & Rohafauzi, Suziyani & Nur, Afiza & Abdullah, Rina & Shafie, Rosmawati & Selamat, Muhammad & Azman, Nazrul & Muhammad, Muhammad. (2020). Density Based Traffic System via IR Sensor. Journal of Physics: Conference Series. 1529. 022061. 10.1088/1742-6596/1529/2/022061.

[3]. L. P. J. Rani, M. K. Kumar, K. S. Naresh and S. Vignesh, "Dynamic traffic management system using infrared (IR) and Internet of Things (IoT)," 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM), 2017, pp. 353-357, doi: 10.1109/ICONSTEM.2017.8261308.

[4]. Dzulkefli, Nik Nur Shaaadah Nik, et al. "Density Based Traffic System via IR Sensor." Journal of Physics: Conference Series. Vol. 1529. No. 2. IOP Publishing, 2020.

[5]. B. Ghazal, K. ElKhatib, K. Chahine and M. Kherfan, "Smart traffic light control system," 2016 Third International Conference on Electrical, Electronics, Computer Engineering and their Applications (EECEA), 2016, pp. 140-145, doi: 10.1109/EECEA.2016.7470780.

[6]. M. Razavi, M. Hamidkhani and R. Sadeghi, "Smart Traffic Light Scheduling in Smart City Using Image and Video Processing," 2019 3rd International Conference on Internet of Things and Applications (IoT), 2019, pp. 1-4, doi: 10.1109/IICITA.2019.8808836.

[7]. S. S. R and L. Rajendran, "Real-Time Adaptive Traffic Control System For Smart Cities," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1 -6, doi: 10.1109/ICCCI50826.2021.9402597.

[8]. P. Soundarya Lahari, M. F. Mohammed, K. Lingaraju and K. Amulya, "Density Based Traffic Control with Emergency Override," 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2018, pp. 2094-2099, doi: 10.1109/RTEICT42901.2018.9012488.

[9]. M. S. Miah, R. Acharjee, M. K. Dhar, I. Ahammad, M. Thasfiquzzaman and M. N. M. Haque, "Traffic signal interactive autonomous vehicle: An approach for intelligent path planning and steering control," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), 2017, pp. 333-337, doi: 10.1109/ICPCSI.2017.8392310M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Social Engineering: Way to Bypass firewalls

Nishant Lokhande, Maitreyee Padsalgikar, Ishwari Vaidya
School of Computer Science, MIT-WPU, Pune, Maharashtra, India

ABSTRACT

During this exploration, we hope to describe and demonstrate what social engineering is, and how it can be used to manipulate humans to gain sensitive or nonpublic information. In the cyber bushwhacker world, one of the stylish ways to hack your computer or steal your words is to simply reprimand and deceive you. Throughout this story, we'll learn how these types of attacks work (called social engineering attacks) and how to guard yourself against them. Therefore, a survey has been conducted to discover the extent of social engineering. Since there's neither hardware nor computer code offered to place in-person to protect against social engineering, smart practices should be enforced. A current technical and psychological study on the topic of social engineering is presented in this article. The paper presents an assessment of social engineering - and the social environment within which it appears, a structured summary of social engineering attacks and customary defenses, an analysis of various defenses, and discusses any open challenges surrounding this topic.

Keywords: - Social Engineering, Social Engineering Attack, Social Engineering Prevention, Phishing, Information Security.

I. INTRODUCTION

There are many techniques out there to a hacker for breaching the information Security defenses of an organization. The human approach is typically termed 'Social Engineering' and is probably the foremost troublesome one to be addressed. The paper describes Social Engineering, how it is accomplished, and its impact on organizations. It discusses numerous styles of Social Engineering and the way they exploit common human behavior. The document highlights ways in which it suggests that to counter these attacks and conjointly emphasizes the importance of policy social control and user education in mitigating the risks displayed by Social Engineering. As technical attacks on systems have raised, thus have varied technology-based countermeasures getting used with success to thwart them. As a result, attackers square measure shifting their focus and square measure progressively targeting folks through the employment of social engineering strategies, typically gaining unnoted access to pc systems and sensitive information. This is often because of the wide accepted undeniable fact that individuals square measure the 'weakest links throughout a security framework. Within the era of laws and legislations like SOX (Sarbanes-Oxley), GLBA (Gramm-Leach-Bliley Act), HIPAA (Health Insurance

movability and responsibleness Act), and more, it becomes imperative for everyone to arrange, defend and react to those attacks.

A. What is Social Engineering?

Social Engineering is a set of techniques familiar with manipulating folks into playing actions or divulging classified data. Whereas the same as a cheat or an easy fraud, the term usually applies to trickery for information gathering or computing system access. In most cases, the offender never comes face-to-face with the victims, and also the latter rarely notice that they have been manipulated.

B. Why Social Engineering?

Social Engineering exploits human error or weakness (i.e., cognitive biases) to gain access to any system regardless of the layers of defensive security controls. A hacker could have to be compelled to invest a great deal of your time & effort in breaking the associate access system, however, he or she's going to notice it abundant easier in persuading someone to allow admittance to secure space or even to disclose classified data. Despite the automation of machines and networks these days, no computing system within the world isn't obsessed with human operators for one purpose in time or another. Human interfaces can perpetually be there to provide data and perform maintenance of the system. [2]

II. DEFINING CHALLENGES

Even though Social Engineering poses a massive security risk, very little is discussed about it. Shame may be to blame for the lack of discussion about it. As long as no one wants to be considered ignorant or dumb for having fallen for Social Engineering, most people view it as an attack on their intelligence, wit, and knowledge. The fact is that no matter who a person is, he/she is vulnerable to Social Engineering attacks, which is why Social Engineering gets hidden away in the closet as a "taboo" subject.

A. Social engineering behaviors to be aware of

Human nature has played a key role in the existence of social engineering in one form or another for so long. A social engineer will engage the target in these behaviours to drive them to become a victim. Social engineers exploit security barriers to extract the information while raising no suspicions about what they are doing. It is still the most effective and probably the easiest way to bypass security barriers. Social engineers exploit the following common human characteristics:

- Laziness or Ignorance
- Attitude to Trust
- Enthusiasm to get Free Rewards
- Low Perceived Cost of Information
- Desire to be Helpful
- Appeal to Authority
- Appeal to Ego
- Fear of Losing Incurring Loss

In **reverse social engineering**, however, the target is the one that initiates the communication and gives the hackers the information they require. It might seem strange that authorities could receive passwords and user IDs for their systems, but officials - particularly those in a technical or social position of authority - often have

access to this information because their position puts them above suspicion. A hacker's job is made simpler when the victims themselves provide access or information, without being manipulated by anyone.

B. Categories of Social Engineering

Social engineering can be divided into two main categories: technology-based deceptions and human-based deceptions. Technology-based deceptions involve deceiving the user into thinking he's interacting with a 'real' system or application and then obtaining the user to provide personal information. As an example, the user receives an alert informing them that the computer application is having problems and that they need to re-authenticate to continue. After the user inputs his ID and password on its pop-up window, the harm is done. Now, the hacker who created the popup has access to the user's ID and password and can access that user's network and computer system using the credentials he has obtained. The majority of non-technical attacks are conducted through deception; that is, by exploiting the victim's inherent weaknesses (as pointed out earlier). As an example, the attacker may pretend to be a senior manager; call the help desk, ask to reset the password, and ask for it to be reset right away. A help desk representative resets the password and gives the new password to the customer waiting at the other end of the phone. Once the new password is given, the attacker has access to the user's credentials and can perform any malicious activity.

2.1. Technical Attack Vectors

A. Phishing

Emails that appear to come from legitimate firms, banks, or MasterCard companies and request "verification" of information and threaten dire results if not performed are known as "phishing emails." A fraudulent website is linked in the letter with company logos and content and the form asks for usernames, passwords, credit card numbers, or PINs.

B. Vishing

VoIP phishing is a method of tricking personal and financial information out of the public by leveraging technology such as Voice over Internet Protocol (VoIP). It is a combination of phishing and voice calls. By exploiting the trust of the public in landline telephone services, which traditionally terminate at a physical location that is known to the phone company, and is associated with a customer, many telephone scams are committed. In contrast, with the advent of VoIP services, telephone services may now be terminated by computers, which are far more vulnerable to fraud attacks than traditional "dumb" telephony endpoints.

C. Spam-Mails

Malicious code is planted on the web using e-mails that offer friendship, diversion, gifts, and numerous free pieces of footage. Employees open e-mails and attachments via Trojans, Viruses, Worms, and other uninvited programs find their way into systems and networks. A person is compelled to open the message as a result of it seems to supply vital information, such as security notices or receipts, guarantees amusing entertainment, such as jokes, gossip, cartoons, or photos, reveals free software, such as music, videos, or software downloads. An attack may range in severity from a simple nuisance to system slowdown, destruction of entire communication systems, and data corruption. [2]

D. Popup Window

As part of the attack, the scoundrel program generates a popup window informing the user that the connection between the appliance and the network has been interrupted due to network issues, and the user should reenter

his id and password to continue along with the session. To continue operating, the unsuspecting user quickly does as requested, and forgets about it. He/she heard that the system was attacked, but never realized he/she had been the one who opened the gate!

E. Interesting Software

In this case, the victim is fooled into downloading and installing a very useful program or application that might be marketed as a CPU performance optimizer, a great system utility, or a code for an upscale software package. An example of this would be spyware or malware (such as a key logger) which is installed by a computer virus disguised as a legitimate program or message.

2.2. Non-Technical Attack Vectors

A. Pretexting / Impersonation

This technique aims to create and exploit a fake situation (the pretext) to induce someone to divulge information or take action which is often conducted over the phone. An easy lie that usually involves some kind of analysis or setup and utilizes pieces of illustrious information (e.g. date of birth, mother's last name, billing address, etc.) to determine legitimacy in the minds of the target.

B. Dumpster Diving

Most people wouldn't think that discarding spam or routine company documents without shredding them could be hazardous? Nonetheless, that is exactly what would happen if the spam contained personal information, or MasterCard offers that a dumpster diver might use to commit fraud. The unsuspecting 'trash thrower' might become the Dumpster Diver's lifeline. A hacker frequently impersonates management-level employees to benefit from phone books, organization charts, and locations of employees. An unshredded policy and procedure manual can enable a hacker to familiarise himself with the company's policies and procedures, and thus convince the victim that they are authentic. Hackers can make official-looking correspondence by using corporate letterhead. Hackers can gather information from hard disks of computers as there are numerous ways to retrieve information from disks, even if the user believes the data has been 'deleted'.

C. Spying and Eavesdropping

A clever spy will capture a user typing in the ID and password by watching his fingers on the keyboard (Shoulder Surfing). All they need to do is position themselves behind the user and observe his fingers on the keyboard. If the policy is for the helpdesk to speak the password to the user via the phone, then if the hacker can eavesdrop or listen in to the conversation, the password has been compromised. An infrequent person may even be within the habit of writing the id and password down, thereby providing the spy with another avenue to urge the knowledge.

D. Acting as a Technical Expert

Here, an intruder poses as a network technician working on a network problem and requests the user to let him access the workstation to resolve the problem. The unsuspecting user, especially if not technically savvy, will probably not even ask any questions, or watch while the pc is appropriated by the so-called ‘technician’. Here the user is trying to be helpful and doing his part in trying to repair a drag within the company’s network.

E. Support staff

Here, a hacker may trick a member of a facility into supporting employees. Someone dressed like the cleaning crew enters the work site carrying cleaning equipment. As he appears to wash your desk area, he will snoop

around and steal valuable information - like passwords or a confidential file you forgot to lock up or create a decision impersonating you. The deceptive phone trained worker is another example. An intruder will pretend to be a serviceman and walk up to your phone, fiddle around with the equipment, inspect the wiring, and spy on your company for valuable information that has been left unsecured.

F. Authoritative Voice

A hacker can pretend to have trouble accessing the system by contacting the company's help desk. In an attempt to understand the password over the phone, the individual claims to be in a hurry and wants his password reset immediately. If the attacker supports his / her story with information gathered from other social engineering methods, then the assistance desk personnel are more likely to trust the story and comply with the request.

G. Hoaxing

Hoaxes are attempts to fool people into believing that something fake is real. A hoax on the other hand is usually conducted as a practical joke, to cause embarrassment or to inspire social change by bringing awareness to a cause. Having a fear of an untoward incident may also lead to making sudden decisions.

III. METHODS AND MATERIAL

A. Survey:

We gathered the insightful opinions of participants by conducting a questionnaire as part of this research. To understand the awareness of social engineering attacks around the world, we conducted the following survey with 30 users. We asked them the following questions:

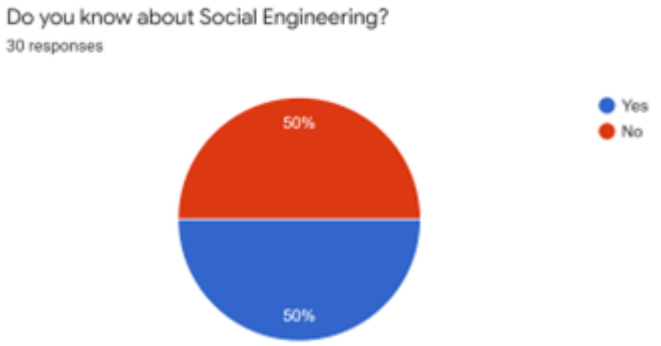
1) Do you know about Social Engineering?
2) Do you share all your details on social networking sites?
3) Do you ever reply/click/like against any unknown friend request/post/message/video received?
4) Do you read the terms and conditions whenever you register on any website?
5) Are your all login ID and password are different?
6) Do you use the same passwords for all accounts you sign up?
7) Has anyone you know asked for your password? If yes what was your response?
8) Do you know what a phishing attack is?
9) Is anti-virus currently installed, updated, and enabled on your computer?
10) Do you think your computer has value to hackers so that they can target you?
11) Upon receiving notification that you've won their lottery prize, you'll be notified over the phone or by email. All that is a processing fee to obtain the huge amount of money that they have won. What will you do in that case?
12) Do you know whom to contact in case you are hacked or if your computer is infected? Do you feel that your computer is secure?
13) Have you ever had your email account hacked or stolen?
14) When you receive an unwanted email, do you ever reply to it?
15) If you received a call and they introduce themselves that they are part of the Bank where your Bank Account is there. They asked you to answer some questions such as your (Bank Account Number, ATM Number, ATM Password, etc.).Then what will you do in that case?

IV. RESULTS AND DISCUSSION

A. Result:

Data Analysis of Surveys: We create a questionnaire and record responses from users.

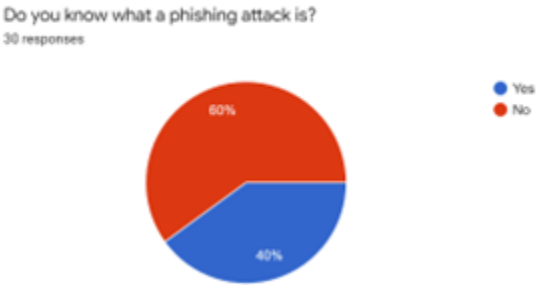
i. We found that 50% of people are familiar with social engineering after surveying 30 users.



ii. There are 73.3% of people who use different login IDs and passwords for each website, 16.7% using the same ID and password for every site, and 10% forgetting their passwords.

iii. We were pleased to see people are aware that they should not disclose their personal information on social media sites as a result of this response.

iv. A phishing attack is not aware of by 60% of people.



V. SOCIAL ENGINEERING AND ITS IMPACT ON ORGANIZATIONS

Information Security is a key aspect of business as usual (BAU) for any association. If information security is not prioritized, especially in today's landscape where there are so many pitfalls that are brewing, even a small lapse in security can bring an organization down. The financial costs could be devastating if the association is not prepared. In addition, a company's reputation can suffer, which can erode its foundation over time. For instance, a malicious entity can access credit card information that an online seller receives from guests. Once the guests find out that their credit information has been compromised, they will not want to do any further business with the seller, as they would consider that point to be insecure. The company may also file suits against them, which would lower its character and discourage prospective or existing clients. According to experts, although the hacker might be a stranger, most violations are due to either dissatisfied workers or employees who have licit access to the system as part of their job. Companies invest billions of dollars each year in perfecting software and tackles to protect themselves from vicious attacks. It all goes to waste if end-users are not properly educated and security practices are not followed.

In 2013, an American former computer intelligence consultant, Edward Snowden leaked a piece of highly classified information from the National Security Agency (NSA) when he traveled to Hong Kong. He provided a lot of top-secret documents about U.S. intelligence agencies' surveillance of American citizens to three journalists. Snowden social engineered his colleagues at a spy base in Hawaii, by telling them he required their login to do his work as a computer systems administrator. Surprisingly, these people, within the NSA, fell for a basic hacker trick like this and provided their login details to Snowden. He used these usernames and passwords to access some of the classified materials he exfiltrated.

According to Snowden, the classified information he shared with the journalists in Hong Kong, exposed privacy abuses by government intelligence agencies and saw himself as a whistleblower. But the U.S. government considered him a traitor because according to the legal experts, his actions violated the Espionage Act, hence his passport was revoked by the Department of State. After meeting with the journalists, Snowden left for Ecuador, where he would seek asylum. But when his plane landed in Moscow, he was restricted to the airport terminal by the Russian authorities after observing the canceled passport. Snowden had to spend more than a month, about 40 days, in the Moscow airport, trying to negotiate asylum in various countries. After being denied asylum by 27 countries, he settled in Russia. These revelations by Snowden crystal rectifier to changes within the laws and standards governing American intelligence agencies and therefore the practices of U.S. technology corporations, that currently write in code abundant of their internet traffic for security. Snowden was able to do this because the employees of NSA broke an abundance of basic security rules by providing Snowden with their passwords. Even in highly secure environments, employees are eager to please their coworkers by helping each other, causing security breaches. These types of situations can be prevented with security awareness training among the employees. [12]

VI. SAFETY & COUNTERMEASURES

Among the most difficult pitfalls to defend against are social engineering attacks because they include the 'mortal' component, which is relatively vulnerable. Social engineering is a threat, but some measures will reduce it to something respectable. The modern security defense systems are vulnerable to attacks on human judgment, but

a full life security culture throughout the organization that keeps on evolving as the trouble globally changes will eliminate the threat of social engineering.

A. Well-established security policy

Good security strategies are based on a well-tested Security Policy, associated norms, and guidelines. It should state in simple terms it's compass and content in each of the areas that it applies to. Every policy should contain the norms and guidelines to follow when misbehaving under that policy. As a general guideline, policies should include policy statements on the following disciplines:

- Respectable operations policies-for respectable operations of dispatch, computers, telephones, networks, etc.
- Information brackets and running - to relay critical information and instructions
- Make sure prospective workers and contractors don't pose security problems to the association if hired
- By employing sign-in procedures, electronic security biases, biometric security biases, etc., physical security can be enacted to prevent unauthorized physical access to an installation.
- Creating secure passwords, authorization procedures, securing remote access via modems, etc. Information access control - how to create secure passwords, access authorization, responsibility procedures, etc. The use of automated tools for resetting and synchronization of watchwords eliminates the need for tech support and the help desk to manage watchwords, and the end-users will no longer be burdened with the task.
- Mindfulness training in information security - to make sure that workers are aware of pitfalls and countermeasures and their liabilities in securing the company's information
- Monitoring compliance with the security policy - to ensure it is being followed.
- A system or information must be protected from contagions and analogous risks.

B. Risk Assessment

An organization's operational capabilities can be negatively impacted by threat factors that are identified in the risk assessment process. Besides that, it can also help in determining the extent of action that is necessary to mitigate the threat. Based on the threat associated with each information means, it is important to prioritize them. The association is helped by identifying the most critical means in the association, focusing energy and concern on protecting those means, and identifying the most important means in the association. When a threat assessment is effectively conducted in an organization, the controls and safety procedures should cover the most important asset against attacks. [2]

C. Education and mindfulness

The strategy of defending against social masterminds involves building consciousness among addicts about the methods and actions used by them. Educating employees about the consequences of similar theft is also essential. Social engineering isn't a cover for enforcing the rudiments of a security policy with a good mindfulness campaign. Communication within the company is vital to making a mindfulness crusade successful. Implementing programs becomes more successful when caution is reinforced within the programs. An effective way to produce similar mindfulness in a general non-security professional is to provide real-life examples of companies that have been impacted by bad information, or even just ignorance and negligence on the part of the security professional.

D. Checkups and Compliance

When users ignore the policy, having the policy and educating them isn't enough. Therefore, auditing the usage throughout the enterprise is necessary. It is also imperative that a project undergo thorough security policy compliance verification as part of its quality assurance process. You need to establish audit procedures, for example, to ensure the help desk person is not communicating customer passwords over the telephone or through unencrypted email. Management should periodically check their employees' access rights. A security audit should confirm that no access is granted to employees who are no longer required. Points of access such as entrances and exits should be routinely monitored. Using this method, you will be able to ensure that employees are following the location access policy. The workplaces of employees should be inspected at random to ensure that confidential information is always secured behind locked cabinets. The workstations should be locked down, and screensavers should be password-protected.

E. Identity Management

A unique identifier must be assigned to all employees in an organization. This serves as the employee's login to all computer systems, as well as his/her identifier within the organization. It may lead to additional work, but keeping the base for personal identification separate from the one used for computer systems can mitigate this problem. It may result in some additional work, but that's a small price to pay to limit the damage from an attack.

F. Operations procedures

When granting access to security or concurring with it, standard operating procedures should include a callback or cross-verification step. By doing so, a hacker will have a harder time impersonating a legitimate user.

G. Security Incident Management

You should ensure the team managing the incident knows how to handle a social engineering attack. Each attack provides useful input for ongoing security reviews within the incident response model. When dealing with an incident, staff at the service desk must use a robust incident reporting procedure that includes the following details:

- Target name
- Target department
- Date
- Attack vector
- Attack description
- Attack outgrowth
- Attack effect
- Recommendations

If incidents are recorded, it's possible to identify patterns and exclude future attacks.

H. Insurance Protection

Associations can eventually buy insurance against security attacks, however, most insurers will look for company programs and procedures that work to reduce the impact of attacks. It is more important for insurers to focus on

the hand mindfulness, physical and logical access controls, and security programs an association takes to protect themselves from attacks than the security products they use to prevent attacks.

VII. CONCLUSION

Regardless of the size of a business, social engineering poses a serious threat. In social engineering attacks, the weakest link is a human being. He must be educated about the dangers of social engineering. He must be trained on what social engineering is and how it appears in an organization. Traditionally, defensive security entails the use of intrusion detection systems, firewalls, antivirus software, and other solutions to ensure perimeter security. There are no software systems that you can attach to your employees or yourself to remain secure when it comes to social engineering. In other words, it is very easy for a good attacker to gain information about that organization by building up trust and being friendly to the user. An employee's awareness and training are the keys to protecting themselves from Social Engineering. A comprehensive campaign against social engineering includes policies, procedures, and standards. It is less likely for people to become victims of social engineering attacks if they know what types of attacks might be used.

VIII. REFERENCES

[1]. Social Engineering: The Art of Human HackingBook by Christopher J. Hadnagy
[2]. Thapar, A. Social Engineering : An Attack Vector Most Intricate to Tackle, Infosec Writers,
[3]. http://www.gartner.com/gc/webletter/sec urity/issue1/article1.html
[4]. http://www.microsoft.com/technet/securi ty/midsizebusiness/topics/complianceandpol icie
[5]. http://en.wikipedia.org/wiki/Dumpster_d iving
[6]. http://en.wikipedia.org/wiki/Social_engi neering_%28security%29
[7]. http://www.cisco.com/web/about/security/intelligence/mysdn-social-engineering.html
[8]. http://www.windowsecurity.com/articles/ Social_Engineers.html
[9]. http://www.cert-in.org.in/
[10].https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia
[11].https://en.wikipedia.org/wiki/Edward_S nowden
[12].https://blog.knowbe4.com/bid/351948/edward-snowden-used-social-engineering-to-hack-nsa

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Comprehensive Study of Child Programmers and Dyslexia

Riyansha Shahare, Mr Chaitanya Tambolkar, Ms Sheetal Rajapurkar
School of Computer Science, MIT WPU, Pune, Maharashtra, India

ABSTRACT

This paper examines how and why dyslexics are good computer programmers. The most common of the strategies that dyslexics develop to survive are outlined. Major issues confronted by dyslexics are considered. In this paper huge IQ ranges and extraordinary abilities possessed by the dyslexics are discussed. Mind mapping method and different strategies adapted by dyslexics to decode the blobs (alphanumeric characters unidentified by dyslexics) are inscribed. Introductory evidence, from each the broader dyslexia body with computer programming experience and a few early interview consequences are presented to support the dyslexics and recognize the problems faced by them as well as acknowledge their genetic endowments and developmental trajectories.

Keywords: Programming and Dyslexia, Dyslexia in Programming, Disability in Education, Accessibility in Programming

I. INTRODUCTION

In this study we shall investigate the complexities of dyslexic students who are studying in the computer programming curriculum. We shall see such topics where student having dyslexia can excel and perform better. This paper begins with outlining the causes and common symptoms of dyslexics. Specific issues associated with computer programming and dyslexia are then outlined. With focus on doing this, first the features of dyslexia are presented. After that, a model of the computer programming processes is proposed.

1.1 What is Dyslexia?

Dyslexia can be explained as a general term for disorders that involve difficulty in learning to read or to interpret words, letters, and other symbols, but do not affect general intelligence. Dyslexia is a condition that affects around 20% of the global population. It is the most common of all the neurocognitive disorders in the world. Dyslexia is a common condition that makes it difficult to work with language. Some experts believe that between 5 and 10% of people have this condition. Others say that as many as 17% of people show signs of dyslexia.

1.2 What are its causes?

Dyslexia generally tends to run in families. It is perceived to be related to certain genes that affect how the brain processes reading and language, as well as risk factors in the environment.

Risk factors for dyslexia include:

- Dyslexia or other learning disabilities in the family
- Premature or low birth weight
- Exposure to nicotine, drugs, alcohol, or infections during pregnancy can inhibit foetal brain development
- Individual differences in the brain regions that enable reading

1.3 What are the symptoms of dyslexia?

- Student having it are often diligent and brilliant.
- Students with dyslexia have a difficult time connecting letters to sounds they make and then blending those sounds into words. So, to someone with dyslexia, the word "saw" might read as "was" or “how” as “who”.
- Reading can be a slow and difficult task as a result of these mix-ups.
- Dyslexia can vary from one-to-one.
- Some people have a mild form of the disease that they learn to manage over time.
- Others have a harder time getting over it.

Signs of dyslexia may be hard to apprehend earlier than your baby enters faculty, however a few early clues may also suggest a problem. Once your baby reaches faculty age, your baby`s trainer can be the primary to be aware a problem. Severity highly varies; however, the circumstance will regularly become obvious as a baby begins off evolved getting to know to read.

Signs that a younger baby can be susceptible to dyslexia include:

i. Late talking
ii. Learning new phrases slowly
iii. Problems forming phrases correctly, inclusive of reversing sounds in phrases or perplexing phrases that sound alike
iv. Problems remembering or naming letters, numbers and colors
v. Difficulty getting to know nursery rhymes or gambling rhyming games

School age:

Once your baby is in faculty, dyslexia symptoms and symptoms and signs may also turn out to be greater obvious, which include:

i. Reading nicely beneath the predicted stage for age
ii. Problems processing and information what she/he hears
iii. Difficulty locating the proper phrase or forming solutions to questions
iv. Problems remembering the series of things
v. Difficulty seeing (and every so often hearing) similarities and variations in letters and phrases
vi. Inability to sound out the pronunciation of an strange phrase
vii. Difficulty spelling
viii. Spending a strangely long term finishing responsibilities that contain studying or writing
ix. Avoiding sports that contain studying

Teens and adults:

Dyslexia symptoms and symptoms in teenagers and adults are just like the ones in youngsters. Some not unusual place dyslexia symptoms and symptoms and signs in teenagers and adults include:

i. Difficulty studying, which include studying aloud

ii. Slow and labour-in depth studying and writing
iii. Problems spelling
iv. Avoiding sports that contain studying
v. Mispronouncing names or phrases, or troubles retrieving phrases
vi. Trouble information jokes or expressions which have a that means now no longer effortlessly understood from the particular phrases (idioms), inclusive of "piece of cake" that means "easy"
vii. Spending an strangely long term finishing responsibilities that contain studying or writing
viii. Difficulty summarizing a story
ix. Trouble getting to know a overseas language
x. Difficulty memorizing
xi. Difficulty doing math troubles.

Dyslexia can cause to a variety of issues, including:

- **Difficulty in learning:** Reading being the foundational skill for most other school subjects, a child with dyslexia will be at a disadvantage compared to his peers in most grades and may have trouble keeping up with his competitors.
- **Social Issues:** If left untreated, dyslexia can gradually lead to low self-esteem, behaviour problems, anxiety, aggression, and withdrawal from friends, parents, and teachers.
- **Problems in adulthood:** An inability to read and understand can prevent a child from reaching its true potential as they grow up. This can have long-term educational, social as well as economic consequences. Children with dyslexia are most likely to develop Attention Deficit Hyperactivity Disorder (ADHD) and vice versa. ADHD can lead to difficulty sustaining attention as well as hyperactivity and impulsive behaviour, which can make dyslexia even more difficult to treat.

1.4 How common dyslexia is?

Dyslexia is a common learning disability that causes difficulty with language processing. About 1 in 10 people have dyslexia. In “decoding” letters and words people with dyslexia face difficulty.

What percentage of the global population has dyslexia?

Dyslexia affects 20% of the global population which accounts for 80-90% of all people with learning disabilities. In neurocognitive disorders, it is the most common.

1.5 Who is most affected by dyslexia?

Dyslexia affects people from all economic and ethnic backgrounds. It is estimated that 10% of Indian children are affected, with approximately 35 million children worldwide suffering from this learning difficulty. About 2 million children, receive special education services for people with reading disabilities. In reading, writing, and spelling difficulties dyslexia is the most common cause.

1.6 What are strengths of Dyslexics?

- Puzzles are something that dyslexics enjoy and excel at.
- Dyslexics have a high level of comprehension when it comes to stories that are read to them or narrated to them.
- Most dyslexics have a superior awareness of spatial relationships and use their right brain more effectively.

- Dyslexics excel at conceptualization, reasoning, imagination, and abstraction, among other things.
- Dyslexics have a good ability to see the larger picture when it comes to concepts.
- Dyslexics flourish in areas that are not dependent on reading.
- For their age, dyslexics usually have a big verbal vocabulary.
- Dyslexics are more inquisitive, imaginative, and intuitive than the ordinary person.
- The gift of mastery comes naturally to dyslexics because of their unique way of thinking.

II. DYSLEXIA AND EDUCATION:

The term "dyslexia" refers to a mismatch between IQ and language skills. Dyslexic students have several complications in education like:
poor handwriting;
poor spelling;
poor reading;
poor composition and writing skills;
poor short-term memory;
poor organization.
Due to this, dyslexic students experience substantial educational and legal stigma, and there is a lack of information about their and their families' health situation during this health crisis.
But there are some measures which could be taken by teachers to support and encourage dyslexic students in school:

i. **Multi-Sensory Techniques:** As a sort of active learning in which students actively participate in their education, kinesthetics exercises will assist dyslexic students to employ their strongest learning channels in the classroom.
ii. **Overlearning:** To compensate for poor retention, students should have the chance to overlearn through a variety of different and complementary learning strategies.
iii. **Metacognition:** Students should be encouraged to be aware of the learning process so that they can set personal goals and effectively self-regulate their learning. The dyslexic student will be actively encouraged to map prior knowledge through discovery learning.
iv. **Personal Motivation:** Students will be more engaged and motivated if they are presented with a real-world scenario that can be applied outside of the classroom.
v. **Short Concentration Span:** Lessons should be compartmentalised into manageable portions that allow dyslexic pupils to concentrate for short periods of time, as they can lose concentration fast.

III. DYSLEXIA AND PROGRAMMING:

3.1 What is Computer Programming?

Computer programming is the process of designing/building an executable computer programme to execute a given computation (or, more broadly, to get a specified computing result). Programming entails duties such as analysis, algorithm generation, algorithm accuracy and resource use profiling, and algorithm implementation (usually in a chosen programming language, commonly referred to as coding). A program's source code is written

in one or more languages that are intelligible by programmers, rather than machine code, which is immediately executed by the central processing unit. The purpose of programming is to create a set of instructions that will automate the execution of a task (as complex as an operating system) on a computer, aiming to problem-solving. As a result, effective programming frequently necessitates knowledge of a variety of areas, such as the application domain, specialised algorithms, and formal logic.

The paradigm for the design or problem-solving cycle can be summarised in the following steps when designing a computer program:

- Recognition of a Need
- Problem Definition
- Synthesis
- Analysis
- Implementation
- Evaluation

Individuals must meet specific prerequisites when programming in general, which include:

- Concept Acquisition
- Underlying System Knowledge
- Abstract Thought

3.2 Advantages of Dyslexics in computer Programming

i. Dyslexics have the ability to see connections between different components of the system that others do not, and this ability can considerably simplify and optimise the system's operations, which leads to effective code.

ii. The syntax and notation of computer code is completely predictable, which makes coding easier.

iii. Because of their genetic endowment and developmental paths, many dyslexics go on to develop exceptionally talented brains, they make excellent software designers and programmers.

iv. They excel at static holistic analysis in particular, visualising the entire system in their heads, spotting patterns that others miss, spotting possibly cost-effective short cuts in their 3D mental maps of the proposed code, and avoiding inconsistencies.

v. Dyslexics are right-brained, therefore can figure out what the full programme, class, or method needs to do at various levels of abstraction. (Synthesis)

3.3 Disadvantages of Dyslexics in computer Programming

i) Analysis	Dyslexics may have difficulty breaking down the system into component pieces and perceiving these parts in a logical manner, because these are predominantly left-brained activities
ii) Implementation	Dyslexics may have problem with coding, testing and correction of syntax or spelling until the program both compiles and functions in the expected manner.

iii) Evaluation	Dyslexics are at a disadvantage when it comes to determining the source of erroneous behaviour in a program or even re-conceptualizing the problem.
iv) Concept Acquisition	Students' capacity to learn new concepts will be hampered because they lack implicit learning skills.
v) Underlying System Knowledge	Due to their restricted working memory, dyslexic children will struggle to retain information of more than one language or system without becoming confused.
vi) Abstract Thought	Due to their short working memory, dyslexic students may struggle to manage complicated activities.

IV. COMPUTER PROGRAMMING ACCESSIBILITY GUIDELINES FOR DYSLEXICS:

Many acts, law and guidelines have been made for better experience of dyslexics in Computer Programming. Some of them are mentioned below:

- The Special Education Needs and Disability Act (SENDA, 2011)
- IMS Global Learning Consortium (IMS, 2002)
- The W3C's Web Accessibility Initiative (WAI)
- Section 508 of United States accessibility law Section 508
- DDA, (1995), Disability Discrimination Act.
- CITA, (1998), Section 508 Standards, Center for IT Accommodation.

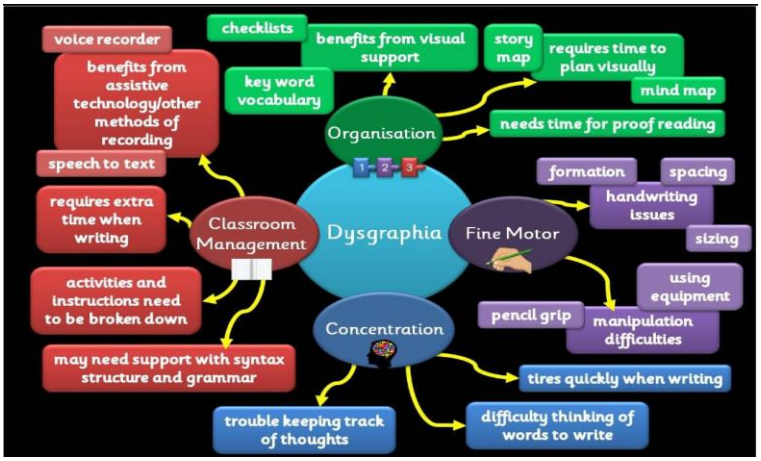
In addition to these standard-setters, a number of organisations, such as WebCT and TechDis, have endorsed the aforementioned providers' standards.

The following guidelines were chosen from generic accessibility guidelines and connected with dyslexia symptoms:

- The dyslexic coder should have flexibility over font sizes, styles, and background and text colours.
- Contrasting colours can help students read text more easily, while particular fonts can be challenging for dyslexics.
- Cascading style sheets enable students to customize a webpage to their preferred visual learning style.
- Active Avoidance is the opposite of passive avoidance. The dyslexic coder may be distracted by a brightly coloured or patterned background, which can conceal text.
- Structuring for the dyslexic programming learner, left justified paragraphs will provide a clear framework.
- Linguistics language used should be clear and succinct, and the graphics should be simple to understand.
- Web pages should be made to function with assistive devices such as screen readers.
- The learner will be able to compensate for his or her lack of reading abilities by receiving knowledge through a more accessible medium.
- Turning Off the Lights Distractions like moving or timed components, blinking or scrolling text may be challenging for dyslexic students who have trouble reading text.
- Consistency Students' cognitive burden will be reduced by consistent layouts and formats, allowing them to focus their attention

- To offer a foundation of knowledge for the dyslexic student, information should be contextualised and orientated
- On the page, the text should not be cluttered.
- Hyperlink sentences should include a brief summary of the page to which they lead and why it is significant.

Supplementary Information:



V. RESULTS AND DISCUSSION

This is the result of measuring the cognitive abilities of students with dyslexia before and after brain training, with particular attention to the cognitive abilities associated with auditory processing.

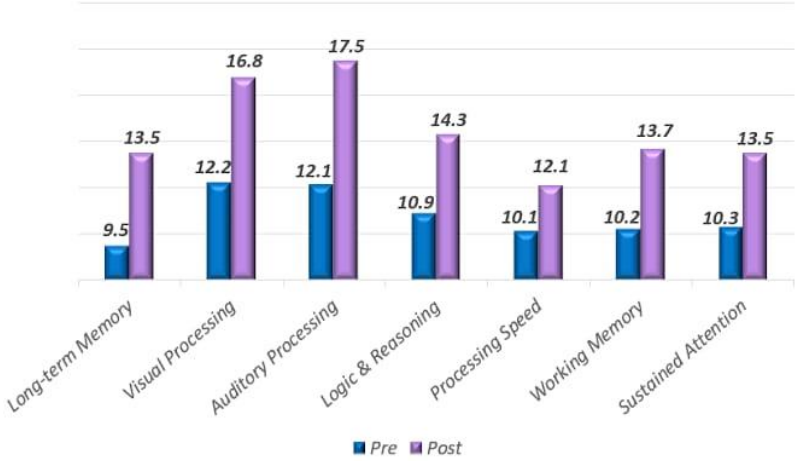
After results we have learned that:

i. The greatest benefits after brain training have been seen in processing auditory, long-term memory, and broad attention.

ii. After only 6 months of training, age-equivalent cognitive ability improved by an average of 3.7 years.

iii. The IQ score after brain training also improved.

These improvements are as follows on the graph.



VI. CONCLUSION

The accessibility standards discussed in this paper should assist both dyslexic and non-dyslexic users by boosting intelligibility of page and allowing users to concentrate on the material's content. The research implies that dyslexic students bring their visualization and creative problem-solving skills to programming, as well as their more generally recognized spelling, organisation, and short-term memory challenges. Until now, no attention has been paid to the auxiliary skills needed to learn how to program in various languages, algorithms, or concepts. These abilities should be taken into account in future work. The delivery of teaching materials was a key concern, as evidenced above. The whole motto of this research is to imply that rather than being viewed as a hindrance in this sector, dyslexia could possibly be useful. Indeed, making dyslexic computer science students aware of these positive viewpoints may be useful. This may provide additional motivation to overcome initial difficulties when learning to program. Programming appears to be a place where persons with dyslexia may use their talents, work around their deficiencies, and even design their own Assistive Technologies.

VII. FUTURE WORK

In the future, we will extend this work by reducing the limitations and improving this model as well.

VIII. REFERENCES

[1]. https://www.bcs.org/articles-opinion-and-research/why-dyslexics-make-good-coders/
[2]. British Dyslexics, (2003), What is Dyslexia? http://www.dyslexia.uk.com/ (Accessed: 28/10/03)
[3]. CITA, (1998), Section 508 Standards, Center for IT Accommodation. http://www.section508.gov/ (Accessed: 28/10/03) DD, (1995),
[4]. Disability Discrimination Act. Chapter 50. www.hmso.gov.uk/acts/acts1995/1995050.htm (Accessed: 14/10/03)
[5]. IMS, (2002), IMS Guidelines for Developing Accessible Learning Applications, Version 1.0, IMS Global Learning Consortium. http://www.imsglobal.org/accessibility/index.cfm (Accessed: 14/10/03)
[6]. Powell, N.J., Moore, D., Gray, J., Finlay, J. and Reaney, J., (2003), Dyslexia and Learning Computer Programming, In 4th LTSN-ICS Annual Conference Proceedings, Galway, LTSN-ICS. www.ics.ltsn.ac.uk/pub/conf2003/index.htm (Accessed: 14/10/03)
[7]. SENDA, (2001), Special Educational Needs and Disability Act, In Chapter 10. www.hmso.gov.uk/acts/acts2001/20010010.htm (Accessed: 14/10/03)
[8]. W3C, (1999), Web Content Accessibility Guidelines 1.0, World Wide Web Consortium. http://www.w3.org/TR/WAI-WEBCONTENT/ (Accessed: 14/10/03)
[9]. ResearchGate. 2004. Dyslexia and learning computer programming. [online] Available at: http://www.researchgate.net/publication/26467406_Dyslexia_and_learning_computer_programming [Accessed: 9 Jun 2013].
[10].https://r4dn.com/how-common-is-dyslexia/
[11].https://www.mayoclinic.org/

[12].https://www.indiatoday.in/education-today/featurephilia/story/how-parents-and-teachers-can-help-dyslexic-children-with-learning-1861124-2021-10-05#:~:text=Dyslexia%20is%20a%20brain%20disorder,normal%2C%20even%20above%20average%20intelligence.

[13].https://www.bing.com/images/search?view=detailV2&ccid=kPDRc%2B0D&id=54FBF0BE6C6E2A1765804891CE4C93D71CC1A4C0&thid=OIP.kPDRc-0D40Ib3XUowqiYwQHaFh&mediaurl=https%3A%2F%2Fi.pinimg.com%2Foriginals%2Fd8%2F12%2F4e%2Fd8124e1df0650ad61c7b0795a2f15764.jpg&exph=1131&expw=1515&q=Dyslexia+Dysgraphia&simid=608054059494563187&form=IRPRST&ck=2DDFD39DD9CA8D3BB793616858D078C8&selectedindex=1&ajaxhist=0&ajaxserp=0&vt=0&sim=11

[14].https://www.learningrx.com/who-we-help/reading-struggles-dyslexia/

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Optimal VM Placement Approach Analysis Using FSRL and RLVMP in Cloud Computing

Abdul Razaak MP[1], Gufran Ahmed Ansari[2]
[1]Department of Computer Application, B.S. Abdul Rahman Crescent Institute, Chennai, Tamil Nadu, India.
[2]School of Computer Science, MIT World Peace University, Pune, Maharashtra, India

ABSTRACT
The environmental sustainability and energy cost extant an important challenge for cloud computing practitioners and the growth of next generation data centers. Today, RM (Resource Management) contributes to significant energy usage in data center operations. The deployment of virtual machines (VMs) is used to reduce energy and improve resource management. Due to the energetic nature of cloud application, VM (Virtual Machine) Placement algorithm faces a challenge to exactly forecast upcoming resource difficulties. This paper presents and compares a FSLR (FUZZYBASED SARSA (STATE-ACTION REWARD-STATE-ACTION) REINFORCEMENT LEARNING) algorithm with a RLVMP (REINFORCEMENT LEARNING BASED VIRTUAL MACHINE PLACEMENT) strategy for energy savings in cloud data centers to address VM placement problem. This paper proposed a relative study of commonly used prediction models and introduces a predictive VMP approach based on workload traces.
Keywords: Cloud Computing, FSLR, SARSA, RLVMP Resources Management, Virtual Machine, Virtual Machine Placement.

I. INTRODUCTION

Around the world, advances in virtualization technologies and commercial computing are powering a large portion of internet applications and enabling the low-cost implementation of large-scale data centers. Cloud data centers offer several benefits including mobility, elasticity, disaster recovery, flexibility and on-demand resources [1-3]. One of the most important features of the cloud paradigm is elasticity. Elasticity enables an application to scale its resource requirements at any time[4], [5]. It has enabled the trend of renting of hardware, software and network resources rather than buying and managing computation resources. User can leverage complete computation infrastructure with an internet connection. It has wide range of applications like financial management, manufacturing, marketing, business management, academia, hospital management and many more [6], [7], [8].
The goal of this research is to find a way for minimizing energy usage in cloud computing for resource provision and development, but it may also be used to edge computing. Other alternative technologies, like edge computing,

can significantly lower energy use be owing to their nature. As a result, Virtual Machines are regarded as allocatable resources in data centers. The distribution of Virtual Machines (VMs) is deemed critical in order to regulate the data center's energy consumption over time.

The main contribution of this study is as follows.

- Proposed a model for getting result VMR
- The aim of this study is to equivalence technique for energy-aware VM scheduling while taking resource constraints into account.
- Comparative Analysis have done for both algorithm

This Paper work flow organized as follows

- Related study
- Methodology
- Discussion

II. RELATED WORK

Son et al. [9], To increase both energy efficiency and performance, an energetic resource overbooking technique based on previous resource consumption data was implemented. In [10], For requests for VM allocation, no time beginning points were considered. The hill-climbing technique was also used to resolve optimization complications. This approach's convergence speed is slow when dealing with high-dimensional issues. lt's also more prone than meta- heuristic techniques like ant colony optimization, which is also examined in this paper, to get trapped in the local optimum.

In [11], The idea of a limit wasn't examined, and VM beginning ideas were assumed to be constant. The greedy heuristic methods were employed to reduce the overall busy time f servers and resolve the energy-aware scheduling of virtual machines, which may not have found the ideal answer. In [12 - 14], Approximate heuristic approaches were provided to handle the challenge of reducing overall busy time in real-time task scheduling while taking resource restrictions into account.

Li et al. [15] propose Pareto-based MOVMrB (Multi-Object Virtual Machine Rebalance Solution), a new VMP method that aims to maintain load balance between machine loads of hosts.

Guddeti et al. [16] advise an algorithm that outperforms both the benchmark and the ant colony algorithms. The performance loss of PMs in comparison to Virtual Machines is not examined in most of the associated work, although limits like that threshold values are applied.

Zhao et al. [17] Evaluate the Performance Loss (PL) and solve it with the ant colony algorithm. However, their algorithm's solution is very intricate, and the pace with which it is solved is poor.

III. METHODOLOGY

The first technique for analysis is the RLVMP algorithm, which treats the early virtual machine placement as a continuous decision problem and then solves it using the enhancedRLtechnique.

This model defines the set of PMs as PMS= {PM1, …,PMj,...,PMN},

N -Number of PMs.
This model defines the set of VMs as VMS = {VM1,...,VMi,...,VMM},
M –Number of VMs.
S- State Space
V (Sij) and R(Sij) indicate the state value and the return of placing V Mi on PMj for each state Sij in the State Space, respectively. Each VM may only be allocated to one PM. Each PM must meet the memory requirements of the Virtual Machines (VMs) running on it. This model doesn't take into account central processing unit restrictions, but rather restricts the central processing unit in terms of performance loss.

A. RLVMP MODEL

To develop a placement approach that reduces real energy consumption while accounting for recognized State Values and Performance Loss gained through extensive learning. Then, to resolve the goal problem, the RL (Reinforcement Learning) approach is applied. In order to arrive at a final answer for Reinforcement Learning, we must first define state values before exploring and evaluating techniques.

Steps of RLVMP model

- The parameters are set to zero during the initialization phase, and initialized the Q value matrix.
- The Greedy–After the last update ε algorithm is used in the exploration strategy iteration, and respectively plan choice is only connected to the SV (State Values).
- When the placement is finished, the Number of States and Status Values are updated.
- Once the iteration termination condition is fulfilled, the F Greedy algorithm is used to execute the final placement. The row strategy is chosen mostly by the greedy algorithm based on the SV (State Values). Because of the nature of virtual machine placement, we employ the Greedy algorithm as the VM's decision-making method.

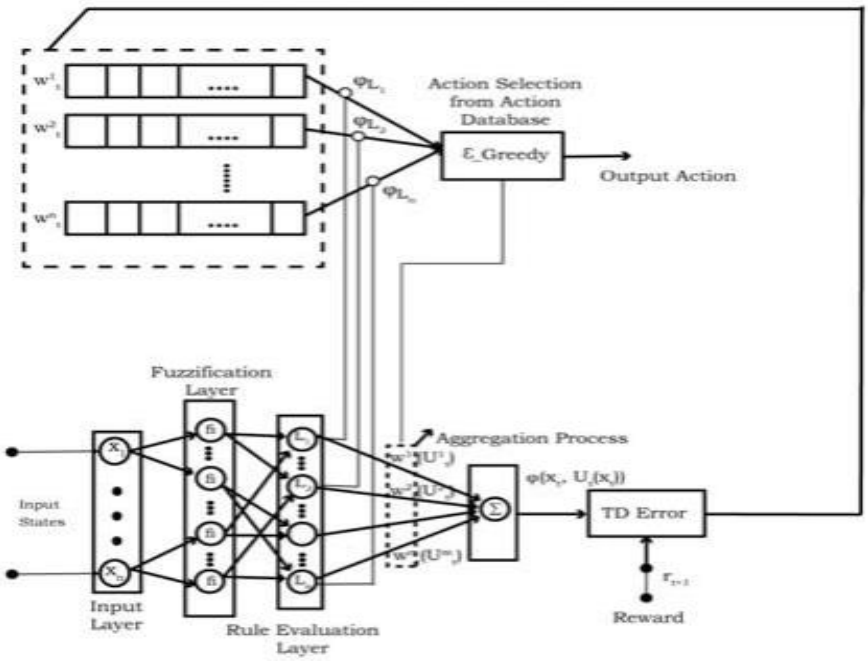
B. FSRL (FUZZY SARSA LEARNIG) ALGORITHM

The research expands the well-known reinforcement learning technique SARSA by incorporating a fuzzy controller for dynamic VM placement. SARSA has an advantage over other RL techniques in these techniques compares that the current state to the next state. SARSA is an on-strategy learning environment in which strategy is optimized and learning is accelerated as a result of carrying out the action one stage to next stage. In general, RL approaches are hampered by the Q-table and the table is used to accumulate the SAV (State Action Value). The FUZZY algorithm provides an excellent result to reinforcement learning by dropping its state-space and allowing it to study closer. During mapping of fuzzy algorithm that true state level to a set of FUZZY labels, and also.
In this work, the set X = x1, x2, xk
xk-The set of resource consumption of active hosts
t-time slot
t= 1, 2, ….,k
k- Number of Time Slots.
n+1 – The maximum Time Slot
The Number of time slots(k) is set to the maximum time slots(n+1)

Where n – Number of virtual machines

When the agent reaches the xn+1 state, all VMs are put. It is sometimes referred to as the ending stage of the learning process.

Fig 1: Architecture diagram of FSRL method



Steps of Fuzzy SARSA Learning Method:

1) Fuzzy Membership: A fuzzy is a subjective regular of the rules' repercussions

$$a = \sum_{l=1}^{p} \mu_l(x) \times a_l$$

μl(x)) - the degree of membership

x -Input State and

p -Number of Rules

2) Quality Function Calculation: The calculation of state x and reference rule1 as follows:

$$\mathbb{Q}(x, a) = \sum_{l=1}^{p} \left(\mu_l(x) \times q[l, a_l] \right)$$

3) Error estimation:

$$\Delta \mathbb{Q} = r + \gamma \times \mathbb{Q}(x', a') - \mathbb{Q}(x, a)$$

r-Reward of New State level
γ ∈(0, 1)- Discount Rate
Above parameter affects the significance of upcoming benefits in relation to present rewards.

4) Updating q-values with each iteration:

$$q[l, a_l] = q[l, a_l] + \varphi \times \mu_l(x) \times \Delta \mathbb{Q}$$

Where [0, 1] -Learning Rate

Table 1: Comparison of simulation parameters

Parameters	**RLVMP**	**FSRL**
Learning rate	0.85	0.1
number of VM's	500	300
Energy Efficiency	18%	24%
Discount factor	0.5	0.8

IV. RESULTS AND DISCUSSION

The simulation is used to develop the FSRL method, and the results are contrasted with the RLVMP approach, which has a single target for the VM placement problem in terms of energy use and resource waste across different scenarios. For VM placement, the CloudSim is utilized to execute both the fuzzy SARSA RL technique and the RLVMP model. The discount factor is the parameter that influences the learning impact of the reinforcement learning algorithm. The closer to Discount Factor is (1), the more weight is placed on future returns, and the further away it is from one, the less importance is placed on imminent returns. As a result, adjusting the magnitude of the discount factor is required to make learning simpler to converge or to become improved outcomes. The FSRL on-policy absorbs fast and progresses to the process of controlled examination-manipulation, that is, it completes the learning stage of virtual machine placement rapidly in accord with the features of both virtual machine and host and arrives at the last examination level, preventing further examination while selecting action.
Overall, the FSRL approach outperforms the RLVMP in terms of energy usage and resource waste.
Advantages of FSRL algorithm

1) FSRL algorithm for virtual machine placement.
2) The usage of a FUZZY inference system to construct a collection of FUZZY sets based on the quantity of virtual machines and host utilization helps to reduce the Exploration Rate and speed up Convergence.
3) FSRL's on-policy learning method, which aids in system learning and action selection, yielded improved results in relationships of Energy and Resource use.

Figure 2 depicts the percentage of energy consumed by FSRL and RLVMP.

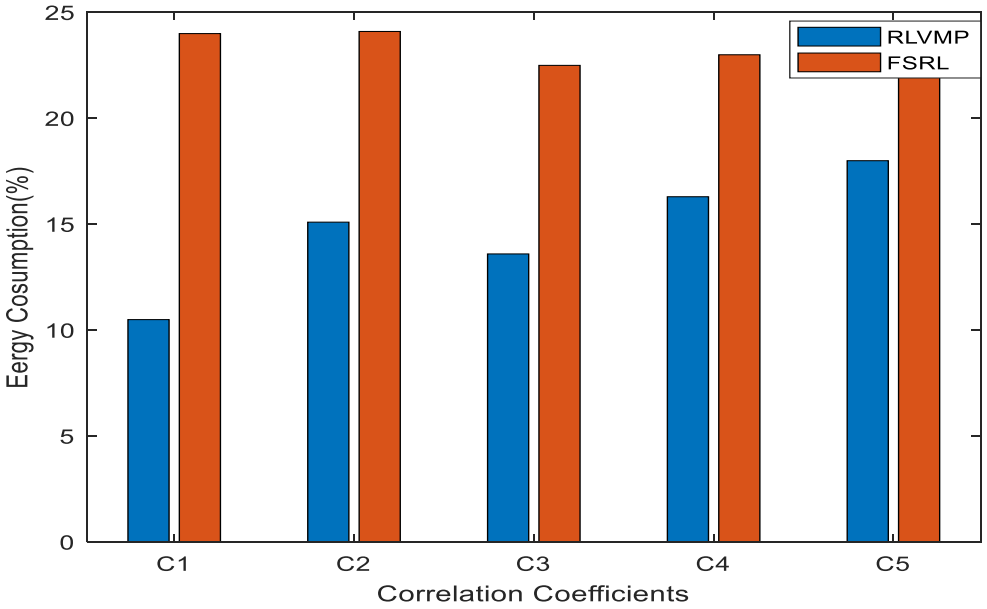


Fig 2: Comparison of energy consumption

V. CONCLUSION

In cloud data centers, energy usage accounts for the lion's share. Modern data center is energy costs and environmental sustainability have emerged as key considerations for cloud computing practitioners and the creation of next-generation data centers. In this study, we give a comparison of the FSRL and RLVMP algorithms for VM placement. The experimental findings reveal that FSRL efficiently uses energy, which is a major difficulty for virtual machine placement algorithms. FSRL is also accomplished of attaining better energy efficiency of at least 24 percent, demonstrating that it outperforms RLVMP. Furthermore, when compared to certain well-known VM placement algorithms, it reduces service violations by more than 45 percent, boosting practitioners' capacity to accomplish considerable improvements in the quality of service offered.

VI. REFERENCES

[1]. Buyya, Srirama, Casale, Calheiros, Simmhan, Varghese, Gelenbe, Javadi, Vaquero, Netto. et al., "A manifesto for future generation cloud computing: research directions for the next decade," ACM computing surveys (CSUR), vol. 51, no. 5, p. 105, 2018.

[2]. Saxena, Singh, and Buyya, "OP-MLB: An online VM prediction based multi-objective load balancing framework for resource management at cloud datacenter," IEEE Transactions on Cloud Computing, 2021.

[3]. Saxena, Chauhan, and Kait, "Dynamic fair priority optimization task scheduling algorithm in cloud computing: concepts and implementations," International Journal of Computer Network and Information Security, vol. 8, no. 2, p. 41, 2016.

[4]. Dabbagh, Hamdaoui, Guizani, and Rayes, "Exploiting task elasticity and price heterogeneity for maximizing cloud computing profits," IEEE Transactions on Emerging Topics in Computing, vol. 6, no. 1, pp. 85–96, 2015.

[5]. Saxena and Saxena, "Highly advanced cloudlet scheduling algorithm based on particle swarm optimization," in 2015 Eighth International Conference on Contemporary Computing (IC3). IEEE, 2015, pp. 111–116.

[6]. Gai, Qiu, Zhao, and Sun, "Resource management in sustainable cyber-physical systems using heterogeneous cloud computing," IEEE Transactions on Sustainable Computing, vol. 3, no. 2, pp. 60–72, 2017.

[7]. Saxena, Vaisla, and Rauthan, "Abstract model of trusted and secure middleware framework for multi-cloud environment," in International Conference on Advanced Informatics for Computing Research. Springer, 2018, pp. 469–479.

[8]. Saxena and Singh, "Energy aware resource efficient-(EARE) server consolidation framework for cloud datacenter," in Advances in communication and computational technology. Springer, 2021, pp. 1455–1464.

[9]. Son,Dastjerdi, Calheiros, and Buyya, "SLA-aware and energy-efficient dynamic overbooking in SDN-based cloud data centers," IEEE Transactions on Sustainable Computing, vol. 2, Apr. 2017, pp. 76- 89.

[10]. Qiu, Jiang., Wang, Ou, Li, Wan, "Energy aware virtual machine scheduling in data centers, Energies", Multidisciplinary Digital Publishing Institute, Vol.12, pp.646(2019).

[11]. Haghighi,Maeen, Haghparast, "An Energy-Efficient Dynamic Resource Management Approach Based on Clustering and Meta-Heuristic Algorithms in Cloud Computing IaaS Platforms", Wireless Personal Communications, Springer,vol.104(4), pp.1367-1391, (2019).

[12]. Qin, Wang, Zhu, Zhai, "A multi-objective ant colony system algorithm for virtual machine placement in traffic intense data centers",IEEE access, vol.6,pp.58912-58923(2018).

[13]. Chau. V, Li. M, "Active and Busy Time Scheduling Problem: A Survey, Complexity and Approximation, Springer", pp.219-229(2020).

[14]. Mertzios. G. B, Shalom.M, Voloshin. A, Wong P. W, and Zaks. S, "Optimizing busy time on parallel machines, Theoretical Computer Science", vol. 562, pp. 524- 541(2015).

[15]. Li. R, Zheng. Q, Li. X, and Yan. Z, "Multi-objective optimization for rebalancing virtual machine placement," Future Generation Computer Systems, vol. 105, pp. 824 – 842, 2020.

[16]. Domanal. S. G, R. Guddeti. M. R, and Buyya. R, "A hybrid bioinspired algorithm for scheduling and resource management in cloud environment," IEEE Transactions on Services Computing, vol. 13, no. 1, pp. 3–15, 2020.

[17]. Zhao, Wang, Liu, Wang, Zhang. W, and Zheng. Q,"Poweraware and performance-guaranteed virtual machine placement in the cloud," IEEE Transactions on Parallel & Distributed Systems, no. 99, pp. 1–1,2018

[18]. Pooyan Jamshidi, Amir M Sharifloo, Claus Pahl, Andreas Metzger, and Giovani Estrada., "Self-learning cloud controllers: Fuzzy q-learning for knowledge evolution", In 2015 International Conference on Cloud and Autonomic Computing, pages 208–211. IEEE.

[19]. Long, Li, Xing, Tian, Li, & Yu., "A Reinforcement Learning-Based Virtual Machine Placement Strategy in Cloud Data Centers."IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). doi:10.1109/hpcc-smartcity-dss50907.2020.00028

[20]. Cloudsim. http://www.cloudbus.org/cloudsim/.Accessed04J

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Impact of Physical Infrastructure on Virtual Web Server Performance

Nitin R. Suradkar[1], Dr. Santosh S. Lomte[2]
[1]Department of Computer Science, Shankarlal Khandelwal College, Akola, Maharashtra, India
[2]Principal, Radhai Mahavidyalaya, Aurangabad, Maharashtra, India

ABSTRACT
The Virtualization technology is base of most of cloud computing services as well as online based services, this research focus on creation of virtual web server with the help of Vmware Esxi 6.7 hypervisor i.e. full virtualization tool used to virtualizes the server machines. This paper states about effect of physical hardware environment on virtual environment that directly impacted on performance of virtual servers. The experiments conducted via Test bed-1 and Test bed-2 against thread-1 and thread-2 to identify performance level of virtual web server. Test bed experiments rely on hardware of server machine that's why multithreaded system considered and Vmware Esxi 6.7 virtualization application deployed as type-1 hypervisor and weighttp benchmark as a workload generator that mimic real time workload. The experimental results define the well-equipped physical hardware system outperform with minimum configured system.
Keywords—Virtualization, Web Server, weighttp Benchmark.

I. INTRODUCTION

The Server machine or any basic computer system normally used to perform the general works or some type of scientific work. To do any task concern system does not utilize their most of the resources and those resources remain unused, to build new physical infrastructure is not easy that requires number of equipment's such as memory, processor, storage, networking devices, I/O components etc., to handle this issue virtualization plays an important role. Virtualization means creating virtual instances of physical system hardware that are logical components likewise any computer hardware system may have and these virtualized resources available to perform most of the task according to user needs [2]. The virtualization categories into two main type para virtualization and full virtualization that mostly applicable at virtualization of servers, networks, storage etc., resources as well as application and device virtualization [1][2]. The para virtualization that virtualize the system through guest O.S. that is known as O.S. assisted VMM (Virtual Machine Monitor) and full virtualization comes under type-1 hypervisor category that directly install on machine hardware and create VMs that is more beneficial in research and development context. Nowadays IT industry fulfill their most of the needs through Cloud computing services that dynamically changed the working environment and it ensure several tasks

completing their work via online based activity through cloud computing model (SaaS, PaaS, IaaS). Virtualization is key at cloud computing models which works at each model with respective functionality, IaaS (Infrastructure as a Service) is main model that majorly affected with the virtualization technology because it virtualizes their physical infrastructure and enhance their quality and quantity of requirements assigned by users. To build virtual environment is cost and time efficient as compared to create physical environment, most of the cloud computing features such as elasticity, scalability, resource pooling etc. are deliverable with help of virtualization technology [1].

Traditional IT infrastructure deployment required large amount of space, resources like storage, network, cooling devices etc., electricity as well as efforts to incorporate server machine to deploy web servers to accomplish requirements of clients [3]. Virtual web server helps in this situation to reduce density of workload, when physical servers migrated to virtual ones and virtualization firstly introduced by IBM in 1972 release first VM named as VM/370[4]. To design and develop a virtual web server using minimum hardware i.e. local system is main goal of this paper, several kind of hardware machine available in market but to decide which is more suitable to work and cost effective is main problem. Two server machine considered in this research work and deployed the virtual web server with required configuration and studied impact of hardware infrastructure on virtual web server alongside their performance level at thread-1 and thread-2.

The article organized as literature review that given appropriate understanding of previous work in desired field, methodology defines approaches followed for research work, result and discussion and conclusion.

II. LITERATURE REVIEW

Several research papers are studied to know the facts and figures of virtualization area, web server and benchmarks used as stress tools. Given below are some papers and their findings are main source of information, those are organized in tabular format as follows,

TABLE I. LITERATURE REVIEW

Author and Year	Workload / Stress Tool	Method	Result
Sun et.al. (2017) [5]	NSFNET simulation tool	RVDCE Algorithm	Algorithm reduced resource consumption
A. Iyengar et. al. (2002) [6]	Web Stone and SPECweb96	ICAPI, NSAPI,ISAPI, Fast CGI	Server satisfy up to 95% client requests
Lu et. al. (2006) [7]	Pareto distribution	Microsoft IIS	M/G/m queue provides a reasonable estimate
Nahum et. al. (2002)[8]	Web Stone, SpecWeb	socket functions acceptex(),transmitfile(),	HTTP throughput enhanced up to 40%
Almurayh et. al. (2014) [9]	XEVA	Xen Server	Improve Xen usability and accessibility.
J. Wang et. al. (2011)[10]	Local dept. database	Citrix Xen Server	Improve utilization rate of server

Few papers mentioned above, rigorous review carried out that find out most of the research held with Xen server hypervisor i.e. available in para virtualization and full virtualization. httperf, Web Stone, Spec Web etc. workload generator used in research, many of them are single threaded not suitable for multithreaded system performance evaluation. According to literature review full virtualization areas need to be explored as well as things related to design and development of virtual web server.

III. METHODOLOGY

Virtualization method is counted in this research, it is backbone of cloud computing, Type-1 hypervisor (VMM) is implemented in experiments which is also called as full virtualization technique. General idea of virtualization elaborated in given figure [4],

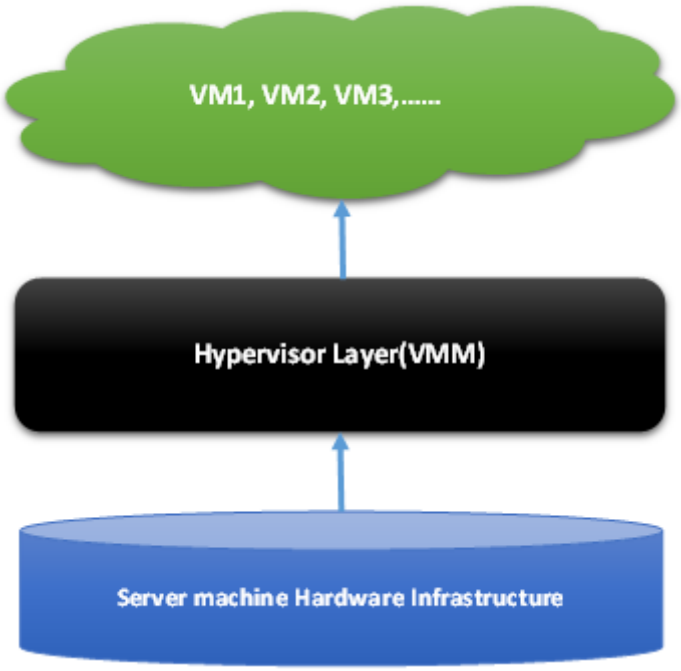


Fig.1.1 Type-1 (Bare metal) Virtualization

The type-1 hypervisor is also called as Bare metal virtualization because it is installed directly on machine hardware of server, there no intermediator between hypervisor and system hardware that ensure the performance efficiency [15].

A. Physical Layer

First layer is server machine hardware specifically base of the virtualization responsible for deliver appropriate environment to deploy VMM or hypervisor on it. This layer is pool of resources such as memory, processor, storage, network, i/o devices etc. that will be virtualizes for achieve desired level.

B. Hypervisor Layer (VMM)

This is second layer of virtualization; it is type-1 hypervisor which is also called as bare metal hypervisor that install on hardware of system that are going to virtualize that virtualizes the kernel of system that effect on performance of virtual environment and ready to serve VMs.

C. Virtual Machines (VMs)

It is main part where virtual machines (VMs) are created and design for deployment of several kinds of server application that fulfill client requests. These servers are called as virtual server and act as a separate machine in networks to handle requests of users regarding their respective tasks.

IV. PROCESS LIFE CYCLE MODEL

Virtualization is fundamental object of this research, that build a virtual environment whose native purpose is to satisfy the need of clients. In this article virtual web server is developed with help of open source application and two different kinds of physical infrastructure is considered to install hypervisor and perform comparative study to identify most suitable environment.

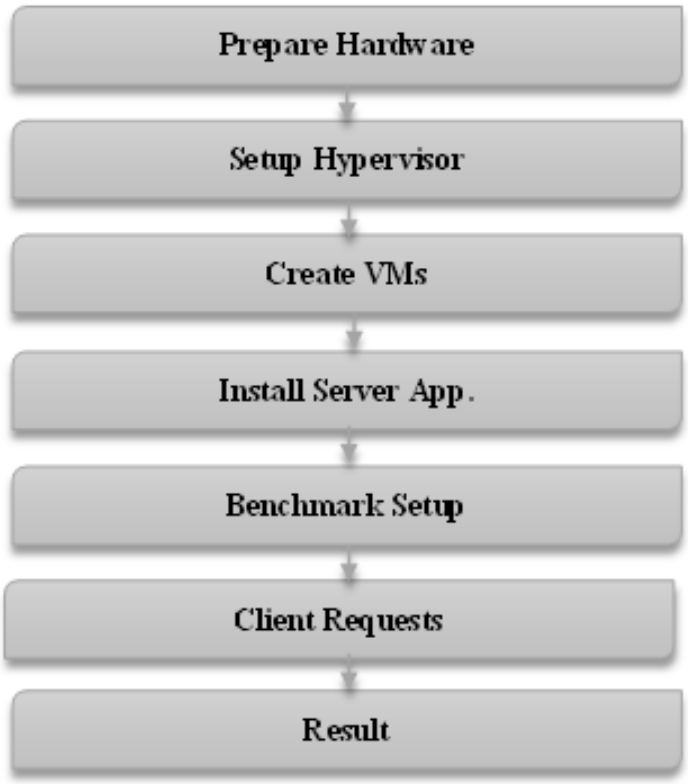


Fig.1.2 Process Flow Model

The life cycle of process also known as process flow diagram that states about each procedure necessary to include to perform specific duty. As mentioned in above diagram step1-Prepare Hardware accountable for maintaining entire physical setup of the desired system. Likewise, step2- Setup Hypervisor level install suitable VMM in this case Vmware Esxi 6.7 used for virtualization. Step3- Create VMs are virtual instances of physical system that play an important role in virtual server creation that defines the working environment and basic configuration of virtual server. Step4- Install Server Application is vital step which deliver actual server that will be used for computing services. Step5- Benchmark Setup required to generate anticipated workload that useful for testing a virtual server, there are several benchmark applications are available such as httperf, netperf, sysbench, Spec web etc. In this research weighttp benchmark used for test bed experiments. Step6- Client Request and Step7- Result are last two procedures of model that depends on earlier mentioned steps.

V. EXPERIMENTAL SETUP

According to methodology experiments are categorized into two parts i.e. Test bed-1 and Test bed-2. Each Test bed liable to perform most of the job assigned in methodology, the Test bed designs are given below,

A. Test bed-1

The hardware and software configuration applied in this research are given below,

TABLE II. SOFTWARE CONFIGURATION

Item	Specification
Operating System	Ubuntu 18.04
Hypervisor (VMM)	Vmware Esxi 6.7
Web Server	Apache
Benchmark	Weighttp 0.4v

TABLE III. HARDWARE CONFIGURATION

Item	Specification
Processor	Intel Core i7-2860QM 2.5 Ghz
RAM	8 GB
HDD	500 GB
Multicore System	Yes
Internet	40 Mbps

The above system configuration is implemented in Test bed-1, Linux Ubuntu 18.04 operating system used as guest O.S. on that desired sever applications will install and do their tasks. As stated earlier Vmware Esxi 6.7 tool operated for virtualization layer that is bare metal hypervisor get utilize most of the resources of the system, it is a full virtualization approach directly communicate with kernel of the system to accomplish client requests. It is mostly used at enterprise level to virtualize their infrastructure due to its customer support and features. The web server is developed with help of Apache application that handle http requests of clients, it normally intended to host basic website. To generate the workload weighttp 0.4v benchmark applied that imitate real time workload through this virtual web server testing accomplished [11]. The hardware configuration for Test bed-1 given above on which all software installed and tested, in this experiment virtual web server created and tested against single and double threaded system [12].

Fig.1.3 weighttp system call

As shown in Fig.1.3, weighttp benchmark implemented for generate the requests and test the virtual server, where - n refers to number of requests, - c concurrent clients, - t number of threads, - k keep request alive at fetching desired destination or url.

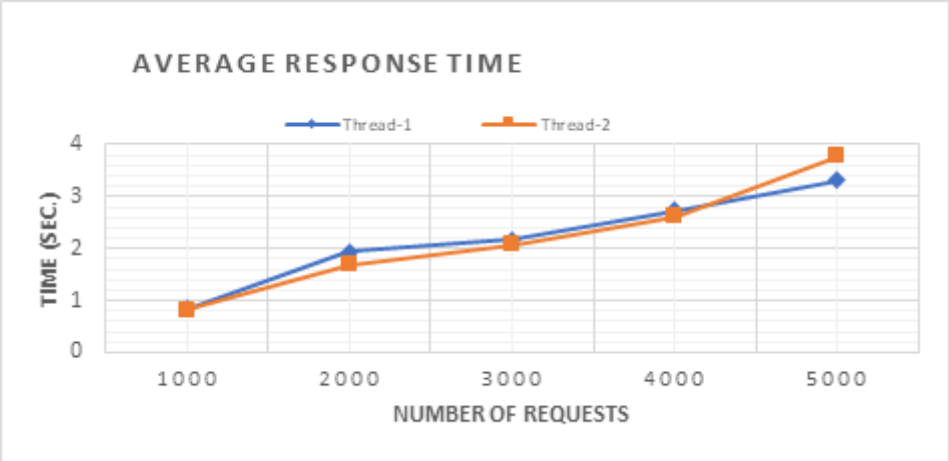


Fig. 1.4 Average Response Time

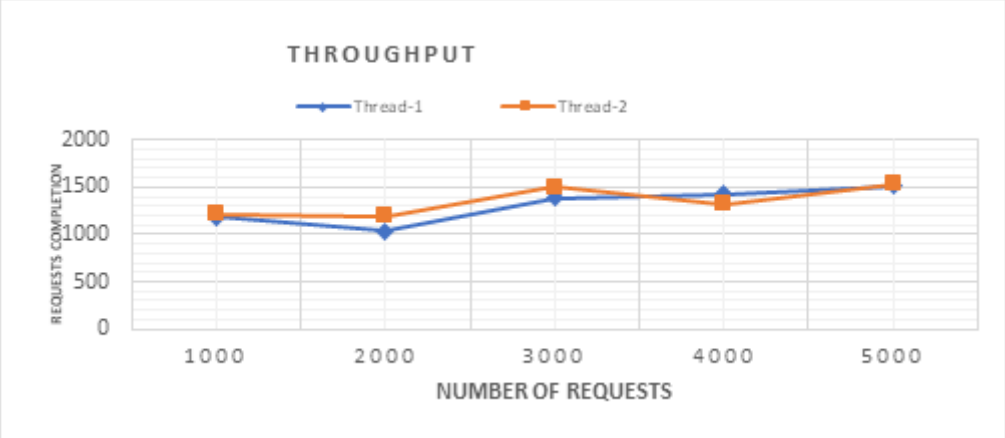


Fig. 1.5 Throughput

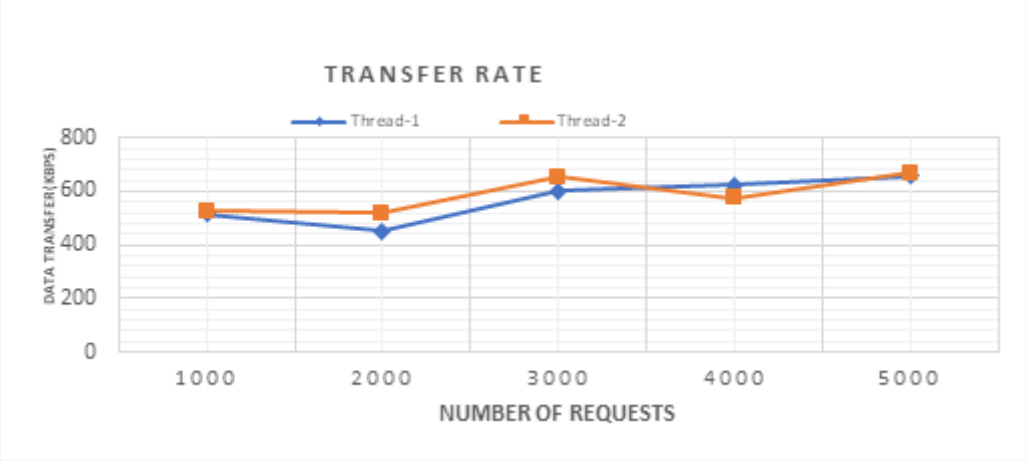


Fig. 1.6 Transfer Rate

The Average Response Time, Throughput and Transfer Rate are calculated against virtual web server created in Test bed-1 and requests range from 1000, 2000 to 5000 are generated to test server and Fig.1.4, Fig.1.5 and Fig. 1.6 are shown the results respectively. ART is a time took by server to respond to every requests assign to it and it used to measure the efficiency of server, minimum time specify better performance [14]. There is slight difference between Thread-1 and Thread-2 performance level are 2.5820 Sec. and 2.6485 Sec. respectively. Throughput is the measurement of how much requests completed amongs the clients and server, it is another important aspect of assessing virtual web server. The average request completion rates of Thread-1 and Thread-

2 are 1378 req/s, 1403 req/s respectively. Transfer rate define number Kilo Bytes data transfer per second in given requests amount for Thread-1 is 600.0667 Kbps and Thread-2 is 611.0667 Kbps. In next test bed another hardware configuration studied and explained in details.

B. Test bed-2

The software configuration is same as applied in Test bed-1, in this experiment physical infrastructure changed and created a virtual web server and tested against Thread-1 and Thread-2, hardware configuration is given as follows,

TABLE IV. HARDWARE CONFIGURATION

Item	Specification
Processor	Intel Core i3-9100 CPU 3.60 Ghz
RAM	8 GB
HDD	1 TB
Multicore System	Yes
Internet	100 Mbps

This is more advanced hardware machine as compared to Test bed-1, 9th generation i3 processor with 3.60 Ghz clock speed and 1 TB HDD. The virtual web server also created with help of apache software and tested using weighttp benchmark testing is given below,

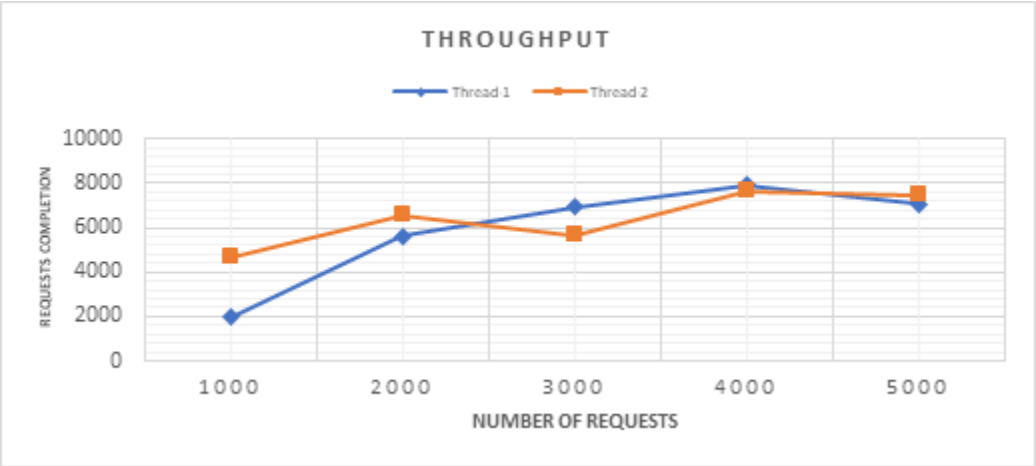


Fig. 1.7 ART_TB2

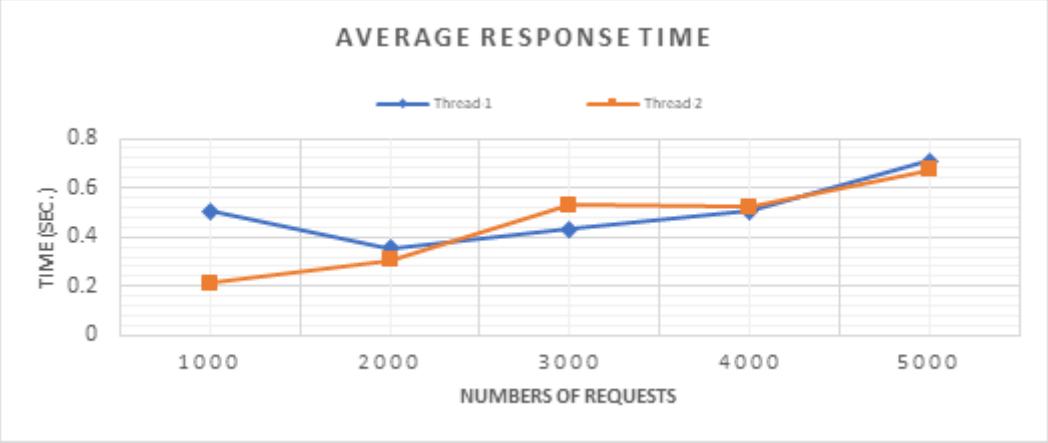


Fig. 1.8 Throughput_TB2

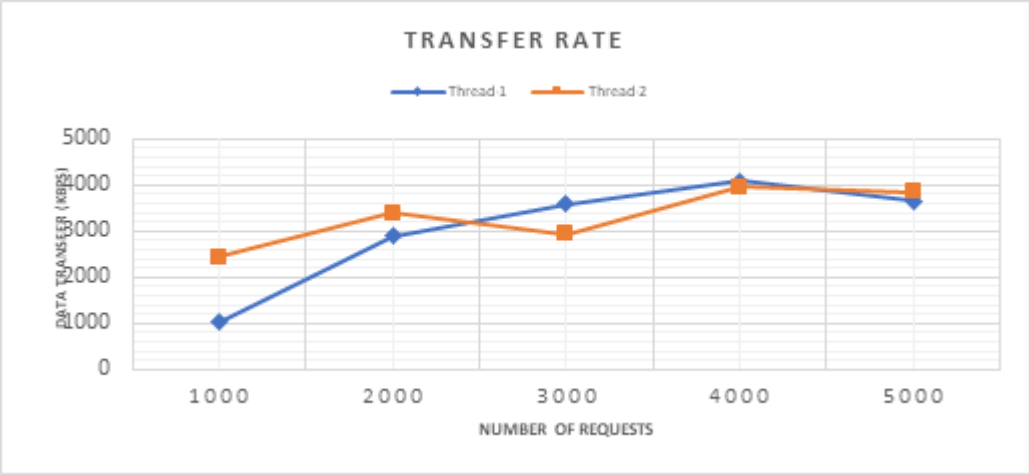


Fig. 1.9 Transfer Rate_TB2

The average response rate of Test bed-2 of Thread-1 is 0.5387 Sec. and Thread-2 is 0.5236 Sec., average throughput of Thread-1 and Thread-2 are 6726 req/s and 6846 req/s respectively and transfer rate is 3472.667 Kbps for Thread-1 and 3534.2 Kbps for Thread-2. The results acquired using this infrastructure is far ahead of Test bed-1 experiment, it explained in upcoming section in details.

VI. RESULT AND DISCUSSION

The purpose of this article is to find out effect of physical infrastructure on virtual web server and rigorous experiments carried out against threads as well as in machine hardware. The following table showing the comparative analysis of results of Test bed-1 and Test bed-2,

TABLE V. COMPARATIVE ANALYSIS OF TEST BED-1 & TEST BED-2

Threads	ART_WA		Throughput_WA		Transfer Rate_WA	
	Test Bed-1	Test Bed-2	Test Bed-1	Test Bed-2	Test Bed-1	Test Bed-2
Thread-1	2.582	0.5387	1378.2	6726.87	600.07	3472.67
Thread-2	2.6485	0.5236	1403.53	6846.2	611.067	3534.2
Total	**2.6152**	**0.5312**	**1390.87**	**6786.53**	**605.57**	**3503.43**

The final comparative result shown in above table include all three aspects and their value represents performance level of each thread at Test bed-1 and Test bed-2 respectively [13]. WA stands for weighted average of response time, throughput and transfer rate that identify exact performance achieved by virtual web server at both the physical hardware infrastructure.

$T2 < WAvg \longrightarrow$ T2 is better (1)

Where, T2 refers to Thread-2, WAvg: weighted average.

Equation (1) is states that Thread-2 performs better at each point as compared to Thread-1 because of its value is lower than weighted average except ART_WA of Test bed-1 at this situation Thread-1 outperform Thread-2.

$T2 < T1 \longrightarrow$ T2 is better (2)

Equation (2) is defines Thread-2 better than the Thread-1 as compared their value with each other except Test bed-1 average response time.

The Test bed-1 experiments score explain at each level their virtual web server performance is far behind the performance score of Test bed-2 experiments and this reveals that impact of physical infrastructure implemented for developing virtual web server.

VII. CONCLUSION

The main aim of this research is to discover the efficient way to design and develop a virtual web server for academic institution through they enhance their productivity and become independent to fulfill their own requirements. To achieve this target foremost task is to choose a right hardware system for virtualization and check their scope and limitation. In this article two experiments namely Test bed-1 and Test bed-2 incorporated, Test bed-1 physical infrastructure is minimal i.e. 2nd generation i7 processor with 2.5 Ghz & 40 Mbps internet facility utilize for developing virtual web server as compared to Test bed-2 experiments i.e. 9th generation i3 processor with 3.60 Ghz & 100 Mbps internet facility. The results shown that Test Bed-2 Average Response Time increased up to 492%, Throughput enhanced with 487% and Transfer Rate improved to 578%. It clearly discovered well prepared infrastructure is more suitable than using local system but it also beneficial to utilize resources of available infrastructure. Consequently, results find out multithreaded system is better than single threaded system, in this research Thread-2 performance is better than Thread-1at most of the levels. Network virtualization overhead may consider for further research to enhance performance of virtual environment.

VIII. REFERENCES

[1]. I. Odun-Ayo, O. Ajayi and C. Okereke, "Virtualization in Cloud Computing: Developments and Trends," 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS), pp. 24-28, 2017.

[2]. Ding, Wei & Ghansah, Benjamin & Wu, Yan, “Research on the Virtualization Technology in Cloud Computing Environment”, International Journal of Engineering Research in Africa, pp. 191-196, 2015.

[3]. Ahmed, Monjur, “Physical Server and Virtual Server: The Performance Trade-offs” European Scientific Journal, 2013.

[4]. N. Suradkar and S. Lomte, "VMware ESXi: Virtual Web Server performance evaluation with weighttp Benchmark," 2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI), pp. 1-4, 2020.

[5]. Sun, Gang & Xu, Zhu & Hongfang, Yu & Chang, Victor & Du, Xiaojiang & Guizani, Mohsen, “Toward SLAs Guaranteed Scalable VDC Provisioning in Cloud Data Centers”, IEEE Access, pp. 1-1, 2019.

[6]. A. Iyengar, E. MacNair and T. Nguyen, "An analysis of Web server performance," GLOBECOM 97. IEEE Global Telecommunications Conference. Conference Record, vol.3 pp. 1943-1947, 1997.

[7]. Lu, Jijun & Gokhale, Swapna, “Web server performance analysis”, 2006.

[8]. Nahum, Erich & Barzilai, Tsipora & Kandlur, Dilip, “Performance issues in WWW servers” IEEE/ACM Trans. Netw, pp. 2-11, 2002.

[9]. Almurayh, Abdullah & Semwal, Sudhanshu, “Xen Web-based Terminal for Learning Virtualization and Cloud Computing Management” Lecture Notes in Engineering and Computer Science, pp. 329-333, 2014.

[10].J. Wang, L. Yang, M. Yu and S. Wang, "Application of Server Virtualization Technology Based on Citrix XenServer in the Information Center of the Public Security Bureau and Fire Service Department," 2011 International Symposium on Computer Science and Society, pp. 200-202, 2011.

[11].Mariela Curiel and Ana Pont, "Workload Generators for Web-Based Systems: Characteristics, Current Status, and Challenges", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 20, NO. 2, SECOND QUARTER, p.p. 1526-1546, 2018.

[12].Arshdeep Bahga, Vijay Krishna Madisetti, "Synthetic Workload Generation for Cloud Computing Applications", Journal of Software Engineering and Applications, p.p. 396-410, 2011.

[13].Raúl Peña-Ortiz, José Antonio Gil, Julio Sahuquillo, Ana Pont, Josep Domènech, "Chapter 8 - A new testbed for web performance evaluation", Modeling and Simulation of Computer Networks and Systems, p.p. 225-251, 2015. https://doi.org/10.1016/B978-0-12-800887-4.00008-0.

[14].Xiaoning Ding, Jianchen Shan, "Diagnosing Virtualization Overhead for Multi-threaded Computation on Multicore Platforms", IEEE 7th International Conference on Cloud Computing Technology and Science, p.p. 226-233, 2015.

[15].Reddy, P. & Rajamani, Lakshmi, "Virtualization overhead findings of four hypervisors in the CloudStack with SIGAR", Fourth World Congress on Information and Communication Technologies, p.p. 140-145, 2014. 10.1109/WICT.2014.7077318.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

The Need of Automatic Water Dispenser for the Visually Impaired

Ketaki Bhagat[1], Swarali Borkar[1], Vibhuti Shimpi[1], Prof. Ganesh Jadhav[2]
[1]School of Design, Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India
[2]Assistant Professor, School of Design, Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India

ABSTRACT
People with visual disabilities, who have limited vision, will face numerous challenges in carrying out activities and interacting with others. In general, equipment is still not user-friendly for them. The purpose of this study was to create “An Automatic Dispenser” design that provides convenience and safety for visually impaired people when taking hot water to the dispenser. The data collection was done through interview and using a survey questionnaire. A total of 25 people participated in this study from all classes with an understanding of the study and consenting for the same. To meet their needs the concept of an 'Automatic Water Dispenser' was proposed, which would have more functions and be safer.

Keywords— Water, Automatic, Visually Impaired, Equipment, Research, Dispenser

I. INTRODUCTION

According to WHO (World Health Organization) key facts for October 2018, it is estimated that approximately, 253 million people have visual impairment, and 36 million are blind [1]. Refraction errors (that your eye's shape doesn't bend light properly, resulting in a blurry image) and cataracts (a form of the disease in which the eye's lens becomes increasingly opaque, causing blurred vision) are the leading causes of visual impairment in the world, accounting for 80% of all cases [2]. The term "blindness" refers to a condition in which one's vision is impaired. In 1997, the World Health Organization updated the estimate of blind youngsters to 1.4 million [3]. Everyday social interactions will present numerous challenges for people with disabilities [Fig 1]. Blind people with limited vision, in particular, will have difficulty carrying out their activities [4].Taking water from a dispenser is a simple example. If the water to be taken from the dispenser is cold, the risk is also minimal. However, if the visually impaired happens to drink hot water, it is extremely dangerous because the hot water may spill on the body causing injuries.

Fig. 1 Visually Blind performing tasks independently

Technological advancements in a variety of fields are used to make human labor easier. One of the technological innovations that functions as a drinking water storage is the water dispenser. Apart from being a place to store water, the main purpose of the water dispenser is to provide access to drinking water. The water dispenser is one of the electronic devices that is in high demand in both homes and offices [Fig 2].

Some of the advantages of using special dispensers for the visually impaired include: (1) It can reduce the risk of taking hot water from the dispenser; (2) It can train independence and help blind people's activities in meeting their water intake; (3) Dispensers can fill water to a certain level so the water doesn't spill; and (4) It provides a sense of security and ease of use because sound indicators tell blind people when the water has finished filling. (5) It can select the appropriate water temperature based on the needs of the user.

There have been many different types of dispensers in use, each with its own set of benefits. Dispensers for the visually challenged, on the other hand, are still underdeveloped. For this reason, research will be carried out by making “Automatic Dispenser for the Visually Impaired ". A dispenser that can automatically fill glasses up to a certain height and it can choose the water temperature as needed with a set point of 50° C, the temperature of 70° C and 80° C and sound indicator which would warn the user when the glass is full.

Fig. 2 Fetching water from the dispenser

II. METHODOLOGY

1. Field Survey: A field survey was conducted at NGO in Ahmednagar. Vision School and Rehabilitation Centre was visited.
2. Detailed examination of present workstation – face-to-face interviews were conducted at the workstation for genuinely understanding the problems faced by the visually impaired. Around 12 visually impaired people were being interviewed.
3. Detailed examination of present automatic water dispenser- The study was conducted utilizing a survey questionnaire for non-visually impaired people and an interview for visually impaired people. Various difficulties encountered during the interview were noted down.
4. Generating and segregating numerous design concepts—different automatic water dispenser concepts (for both ordinary and visually handicapped individuals) were created. The concepts were separated into Should Have's, Must Have's and Nice to have for providing better solutions.
5. Selection of the Final Concept and Prototyping-A final concept was selected for the water dispenser and a working prototype would be developed.

III. RESULTS

A. Field survey

Anam Prem NGO which is one of the leading business in the NGO was visited in Ahmednagar. It is known for physically challenged people, visually blind people and much more. The NGO is in the suburb environment with organized sector. It was observed that there were all age group of people living in the NGO. Coordinators working there were helping the visually blind people with major activities and accomplishments like taking daily exercise, teaching them, computer training, braille library, giving monthly magazines(prakashwata braille literature as well as audio) to read and communicate, helping them to explore their talent through many activities. Taking them for a picnic to enjoy and spend time with others and nature

B. Detailed examination of the present Workstation

During the field visit, it was observed that visual impairment is a significant health problem affecting the common man. A total of 25 people participated in this study from all classes with an understanding of the study and consenting for the same. Demographic data of the 25 visually impaired people are presented in the table below. The age ranged from 7 to 72 years (mean=56.4 years). In the study 15 males and 10 females participated. Majority of the people were in school (56%) where as others were getting their undergraduate degrees (16%). Illiterate people (20%), working individuals (8%) were also included in the study. When they were asked about the reason of their impairment it was noticed the major causes of blindness included cataract, uncorrected refractive errors, glaucoma, and corneal opacities due to infections, diabetic retinopathy, vitamin A deficiency and hereditary diseases of the eye.

Background of visually impaired people	
Study variable	
Age (years) Range	7 -72 years
Gender (M/F)	Male - 15 Female - 10
Profession	
Schooling UG Working Illiterate	6 people 4 people 10 people 5 people

Table. 1 Demographic details of the people present at the NGO

C. Detailed examination of the current product

The water dispenser is one of the electronic devices that is in high demand in both homes and offices and many commercial places. The main challenge related to dispensers is faced by the people with disabilities as they face numerous problems in everyday social interactions. People who are blind or have limited eyesight will find it challenging to carry out their daily routines since they rely on support. A basic example is getting water from a dispenser. The risk is likewise small if the water to be taken from the dispenser is cold. If a visually impaired person drinks hot water, however, it is dangerous since the hot water may spill on the person's body, causing damage. Technological advancements have been done in various products but dispensers still lack behind in terms of features. Their problems in terms of getting water from the dispenser include:

a) Not understanding the placement of the glass.
b) Not having a clear idea about the water level.
c) Setting the water temperature.
d) Huge size of the dispenser causes confusion.
e) Absence of sound indicators in the dispenser.

D. Generating and segregating various design concepts

1) Collection of Data and Information:

It's simple to operate a dispenser; simply place the glass under the tap and turn the water faucet to release the water. Using a dispenser, on the other hand, might be difficult for the blind because they must touch the glass to place it in the correct position and know when the water is full. To assist blind individuals, a visually challenged dispenser may be customized to meet their needs. In order to meet this need, various ideas were studied out of which 3 of them were finalized. The first idea was to incorporate magnet mechanism for auto filling the glass. [Fig 3]

Fig. 3 Concept 1

In this method the glass will be filled till a certain level with the help of magnets placed on the top of the dispenser. The second method was to have an elevation on the dispenser design to stop the water from spilling. Here, the spilled water would automatically get collected inside the dispenser itself and thrown out with the help of an outlet [Fig 4].

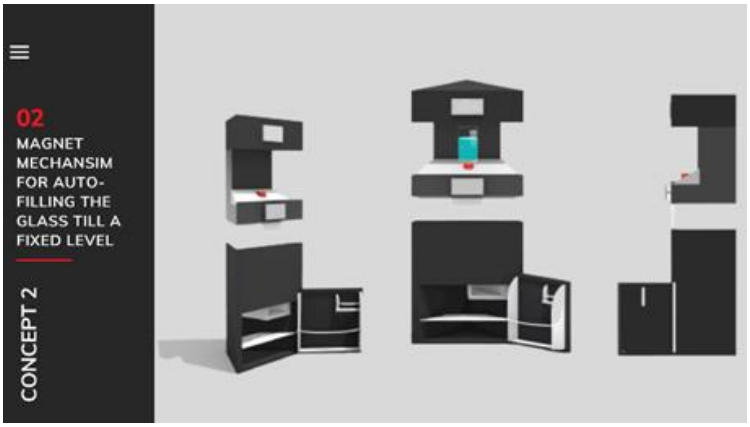


Fig. 4 Concept 2

The final concept was to have a fully automatic water dispenser which will have features such as temperature control, auto-filling, drainage compartment, LCD display, sound indicators and many more Fig [5].

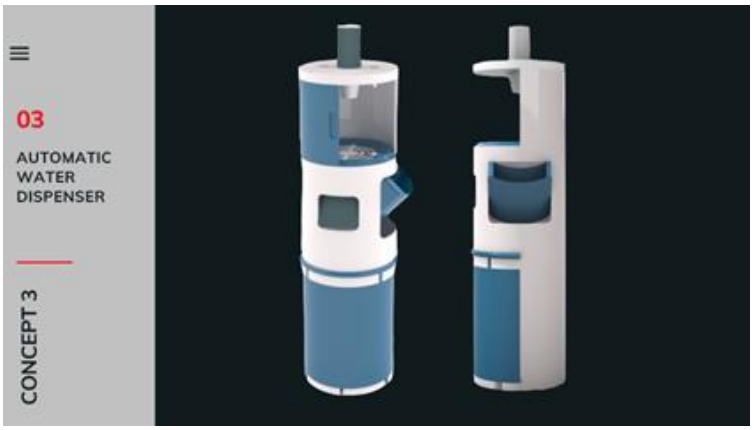


Fig. 5 Concept 3

Then, from those 3 ideas the best solution which is the 3rd concept was selected with the help of Spider-web method (voting) and put into progress for prototyping [Fig 6].

ATTRIBUTE	C3	C2	C1
1	5	3	4
2	3.5	1.5	1
3	5	1	4
4	4	4	5
5	4	3	3.5
6	5	3.5	4.5
SCORE	26.5	16	22

CONCEPT 1 MAGNET FILL MECH.
CONCEPT 2 ELEVATION
CONCEPT 3 DIGITAL TOUCH SCREEN DISPLAY

1. EASE TO USE
2. ROBUST
3. EASY TO INSTALL
4. EFFICIENCY
5. WEIGHT
6. PRACTICAL

ATTRIBUTE	WEIGHTAGE	C1	C2	C3
1	5	25	15	20
2	3.5	12.25	5.25	3.5
3	4	20	4	16
4	5	20	20	25
5	3.5	14.0	10.5	12.25
6	4	20	14	18
SCORE		137.7	68.75	94.75

CONCEPT 1
CONCEPT 2
CONCEPT 3

1. EASE TO USE
2. ROBUST
3. EASY TO INSTALL
4. EFFICIENCY
5. WEIGHT
6. PRACTICAL

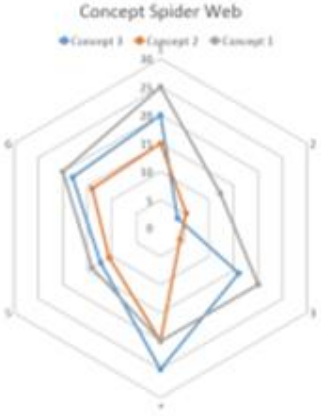


Fig. 6 Spider web concept voting

2) Design Manufacturing:

A cavity is placed on flat top of the dispenser to make it easier for the blind to place the glass in the correct location. The glass can be placed on either the right or left side, with the right side for cold or fresh water and the left side for hot water. A proximity sensor [Fig 7] is installed in the front to detect the presence of the glass as well as its height.

Fig. 7 A proximity sensor

When the water is about 1-2 cm from the glass's surface, the HC-SR04 ultrasonic sensor [Fig 8] is placed on top of the glass to determine the water's height. In this manner the water can be filled till 80% of it's the glass's capacity.

Fig. 8 HC-SR04 Ultrasonic Sensor

The water heater system in the dispenser can be set to 50° C, 70° C, or 80° C by pressing the button, which will create a sound when the set point is selected. The temperature and state of the glass are monitored using a 16x2 LCD, depending if the glass can be read by a dispenser or not.

The dispenser's main controller is an Arduino Mega microcontroller with software for accessing ultrasonic, DS18B20 sensor, and push-button sensor data. For determining the height of the glass and the existence of a glass sensor, as well as a keypad to select the temperature a Photodiode [Fig 9] will be used.

Fig. 9 Photodiode

Following that, the data from the sensor is processed by a microcontroller [Fig 10]. The water level in the glass is monitored by the ultrasonic sensor HC-SR04, while the water temperature is measured by sensor DS18B20 in the dispenser [Fig 11].

Fig. 10 Microcontroller

Fig. 11 DS18B20

The heating element, hot and cold water pumps, and the MP3 Module are all controlled by the Arduino, which sends signals to the AC relay/driver control. The cold/neutral water operating system and the hot water working of operating automatic dispenser system are both used by the automatic dispenser for visually impaired users [Fig12/13/14].

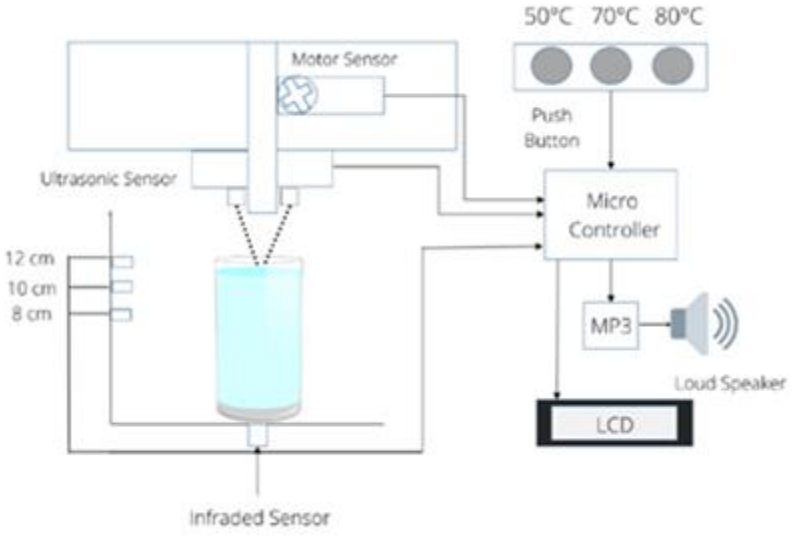


Fig.12 The working of operating automatic dispenser systems.

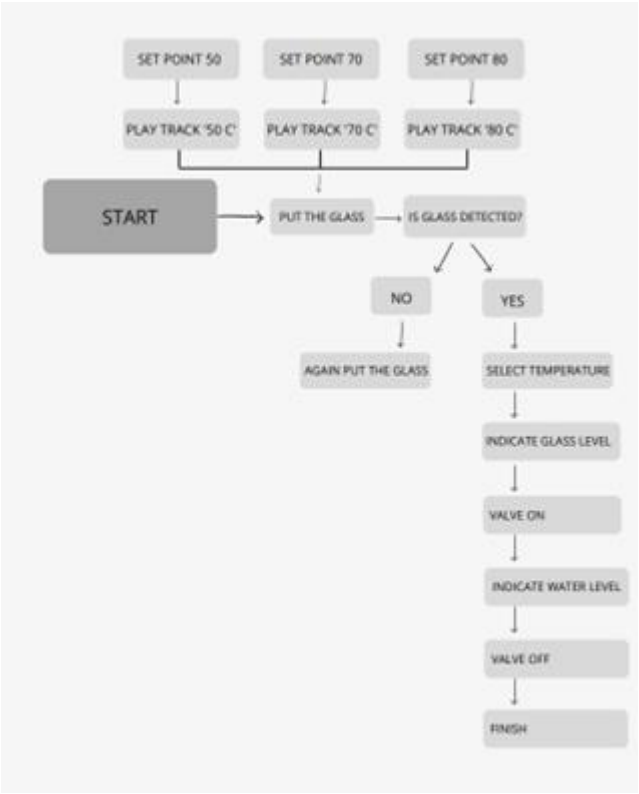


Fig.13 Hot water system

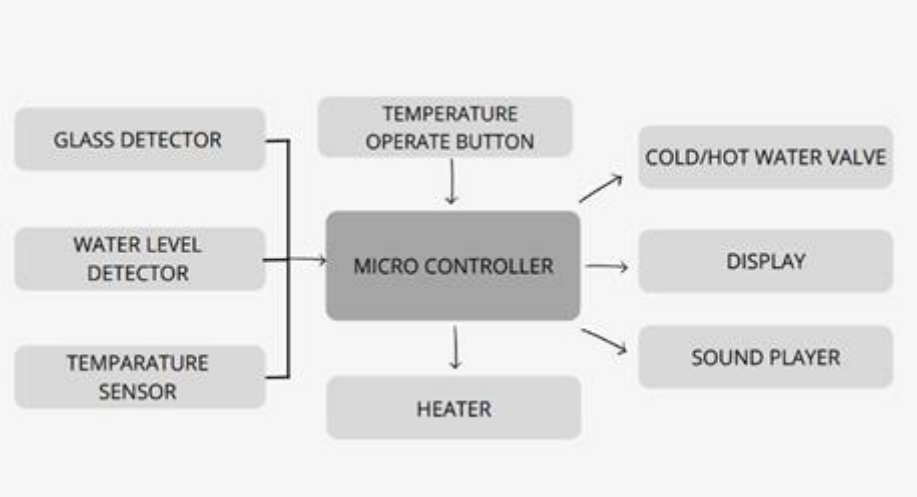
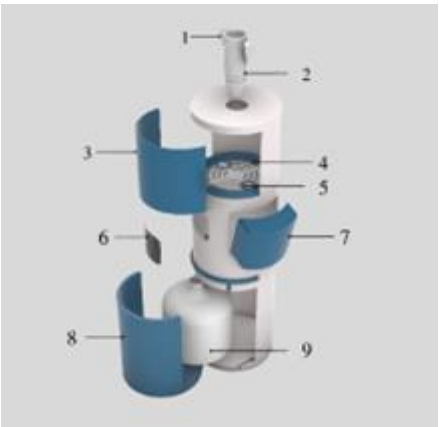


Fig.14 Flow chart of the working of the dispenser

E. Selection of the Final Concept and Prototyping

A Blind Friendly Automatic Water Dispenser [Fig 15] was created with additional features which include:

(1) Reduce the risk of taking hot water from the dispenser.
(2) Training independence and helping blind people's activities in meeting their water intake.
(3) Filling water to a certain level so the water doesn't spill.
(4) Providing a sense of security and ease of use because sound indicators tell blind people when the water has finished filling.
(5) Selecting the appropriate water temperature based on the needs of the user.



1. Cavities
2. Disposable Glasses
3. Sliding door for Dust Prevention
4. Drainage
5. Cavities for holding glasses
6. LED Touch Screen
7. Disposable Compartment
8. Trolley
9. Bottom Loading Tank

Fig. 15 Parts of Automatic Water Dispenser

IV. VALIDATION

Out of the adjustable screen, trash compartment, voice control, drainage to catch spills, and two slots to retain the glass in it, we asked users which feature they found the most useful. Adjustable screen (40 percent) and voice control were the most preferred choices (40 percent). 60% of the time 73.3 percent of voters chose the comfortable size of the water dispenser, with 26.7 percent selecting "MAYBE" and 0 percent voting "NO." We received a resounding "YES" when we asked individuals if they thought our dispenser design was truly useful for blind people. People with 80% say YES for our easy-to-clean water dispenser, while 13.3% and 6.7 percent say NO and MAYBE, respectively. On a scale of 1-10, the majority of people rated our new water dispenser features as 8-9, with some rating them as 10 on a scale of 10.The last question asked in the survey was how satisfied people are with our water dispenser design on a scale of 1-10, with many of them giving an 8-10 rating, the majority giving a 9 rating, and 2-3 people giving a 5 and a 6rating. [Fig16]

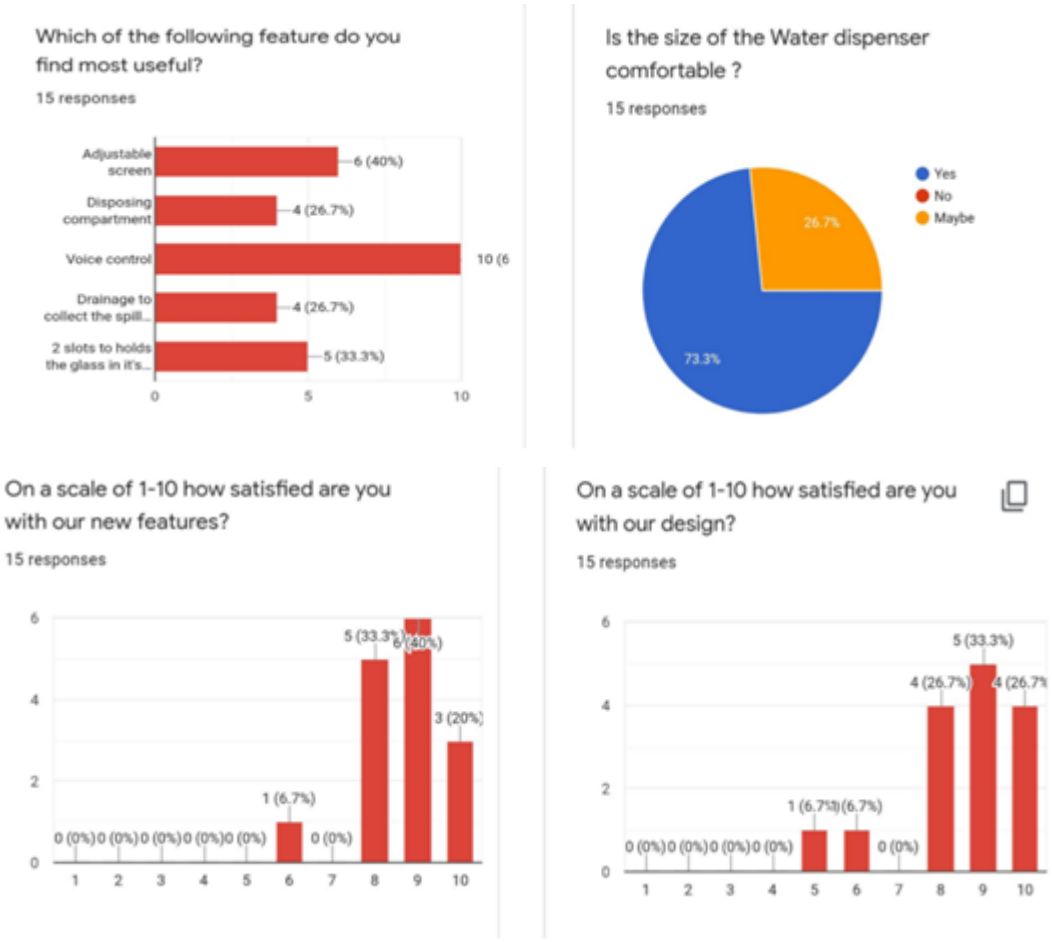


Fig. 16 Survey Insights

V. DISCUSSION

The water dispenser is a popular electronic equipment in both households and offices, as well as many commercial establishments. Considering that the number of dispensers are automated, it's surprising that our primary research revealed that the main obstacle associated with dispensers is faced by people with disabilities, who face multiple difficulties in everyday social interactions. When compared to the research done for Automatic

Dispensers, we discovered that the majority of the features we presented were identical. Similarities in the components were discovered, such as the usage of Arduino Uno, ultrasonic sensors, photodiode, and microcontrollers, as they serve as the product's key components. In terms of features, similarities such as temperature control, a hot and cold water system, and two independent water exits were observed. The major findings were considered, and it was discovered that the main issue was a lack of understanding of the water level and sound indications. To address this issue, some suggestions were presented, such as having cavities inside the dispensers, braille embossing on the dispensers, voice help, and sound indicators. Overall, the findings of this study indicate the necessity for Automatic Water Dispensers to meet the needs of the visually impaired.

VI. CONCLUSION

According to the findings of research into the design of an automatic dispenser for the blind, the automatic dispenser for the visually impaired can work by automatically filling glasses of various sizes (8 cm, 10 cm, and 12 cm) and turning off the tap when the water level reaches 1-2 cm above the glass surface. As a result, there is no spillage. The dispenser can then choose the temperature. A temperature range of 50° C, 70° C, and 80° C is required by the user. Following the completion of the research report, we find that our device has the potential to be highly beneficial to the visually handicapped.

VII. REFERENCES

[1]. Bourne,Rupert RA, et al. “Magnitude, temporal trends and projections of the global prevalence of the blindness and distance and near vision Impairment: a ststematic review and meta-analysis.“The Lancet Global Health 5.9 , 2017, e888-e897.

[2]. R. Pineda, “World Corneal Blindness.” Foundation of Corneal Disease, 2019, pp 299-305.

[3]. Burton, Matthew J. "Corneal blindness: prevention, treatment and Rehabilitation." Community eye health 22.71 (2009): 33

[4]. Saputra, Indra Gunawan, Erwin Susanto, and Ramdhan Nugraha. "Implementasi Metode Jaringan Saraf Tiruan (JST) Pada Alat Deteksi Nilai Nominal Uang." eProceedings of Engineering 3.1 (2016)

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

The Impact of Decentralized Finance and Their Services: A Review

Vaibhav Phadtare, Prof. Navnath Shete
School of Computer Science, MIT World Peace University, Pune, Maharashtra, India

ABSTRACT
There is a growing interest in the digital economy, including blockchain technology, around the world right now. Decentralized financial services should not be provided by centralized intermediaries, but by users for users. The decentralized Finance sector improves services offered by banks, traditional markets, and financial institutions. The main contribution work lies in two parts which are analysis of total value locked and decentralized financial services. This study shall help to understand the opportunities, problems, and future of decentralized finance.
Keywords—Cryptocurrency, Smart Contract, DAOs, Total Value Locked, FinTech, Bitcoin

I. INTRODUCTION

In 2008, an anonymous person named Satoshi Nakamoto build a peer-to-peer electronic cash system called bitcoin cryptocurrency. Cryptocurrencies are not controlled by any authorities and from here blockchain technology came from. Blockchain gives decentralized ownership, immutability as well as cryptographic security of data.

Since bitcoin was launched in the market, enthusiastic people understanding the challenges in blockchain technology. In 2013 Vitalik Buterin published white paper "A Next Generation Smart Contract & Decentralized Application Platform" [1] where he presented the idea of Ethereum blockchain where any person can develop their own application. Later Ethereum protocol comes up as a cryptocurrency. In January 2014, Ethereum was officially announced.

Smart contracts are the backbone of Decentralized Finance (DeFi). Smart contracts refer to a self-executing contract with the conditions of the agreement between buyer and seller being written into pieces of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls everything including the execution, and transactions are trackable and irreversible. In a nutshell, code is a law [2].

In this paper, we will review the overview of decentralized finance also analysing Total Value Locked and detail information about different types of decentralized financial services.

II. DECENTRALIZED FINANCE

In centralized finance (CeFi) traders and asset owners depended on some centralized institution to manage their funds as well as transactions with anyone. In centralized finance (CeFi) there are some problems like fraud, corruption, inappropriate financial management. These problems we can solve through the help of decentralized finance (DeFi).

Due to blockchain technology and Ethereum. New architecture decentralized finance (DeFi) emerged in recent years. Which offers similar services like banks to users. Decentralized finance become very popular since project-related DeFi satisfies the needs of different types of cryptocurrency users. Since the details on fulfillment of smart contracts, requirements are available to all stakeholders. Decentralized Finance (DeFi) is a set of decentralized applications (dApps) that helps to automate financial services without any central authority.

In DeFi software is open-source so code is available to everyone for free. Which ensures the platform's credibility. Anyone can check the code and ensure whether any malicious coding is concealed in the software. Also, people can improve the code and can give better solutions.

Peer-to-peer transactions are the core principles of DeFi. It means all who participate in the market have equal rights. For example, consider you need a loan from centralized finance (CeFi). You'd have to apply for one at your bank or another lender. If you're approved, you'll have to pay interest and service fees to use that lender's services. Through a decentralized finance application (dApp) to enter your loan requirements, an algorithm will match you with peers who can help you. After that, you'll have to agree to one of the lender's terms in order to get your loan.

III. TOTAL VALUE LOCKED

Total Value Locked (TVL) is a metric term used to analyse the total number of assets that are being stacked into decentralized finance (DeFi) protocol. In order to get data about the current market cap, we need to multiply the circulating supply by the current price. In order to get to the total value locked ratio, we need to take that market cap number and divide it by the TVL of the service [3].

The data of DeFi Pulse site were used in order to find the latest analytics as well as rankings of DeFi protocols. DeFi pulse tracks also total value locked in the smart contracts of most popular DeFi applications and protocols. At the time of writing, the market is worth nearly $79 billion in total value locked. Below as we can see the movement of DeFi market in TVL from the past three months the market has dropped nearly 21% from 4 January 2022.

Fig. 1. *Three months behavior in DeFi market [4]*

IV. DEFI SERVICES

A. Lending and borrowing

Lending and borrowing is the most popular service which holds a big share of the market is made up of projects and platforms that provide different ways to borrow or lend funds. Compound, Aave and Maker are the most popular DeFi platforms.

In DeFi lending platform offer cryptocurrency in a trustless manner i.e. without any person users allow enlisting their crypto coins on the platform for lending purposes. A borrower can obtain a loan directly from a decentralized platform known as peer-to-peer (p2p) lending. Also, the lending protocol allows the lender to earn interest [5].

In the lending model, Maker represents over 62% of the DeFi market and TVL of nearly $17 billion dollars [6]. It also has the advantage of being a structure that supports trading rather than holding which sustains a good hash rate for their corresponding blockchains.

B. Asset Management

In 2019 investors and asset management professionals caught the attention of DeFi. Because it is a good way to attract potential users to give benefits of DeFi attributes like derivatives, protocols, composability, security tokens, and decentralized exchange. When all of these factors are considered together, they provide promising results for developing innovative solutions for investors.

The main focus of these projects are offering traders more freedom and allowing them to reach a larger market. Therefore, transparency, trustlessness, and composability are three important characteristics that DeFi uses to empower asset management.

For example, Dharma is a semi-centralized peer-to-peer (p2p) borrowing/lending platform which is based on Ethereum. It allows lending and borrowing for 90 days with a fixed interest rate. Also lending as well as borrowing rates are equal. Because Dharma is non-custodial, all trades are handled manually. A user requests that his asset be lent, and then must wait for a borrower to match his offer. This is a platform for direct matchmaking.

C. Derivatives

A derivative is a contract between two or more parties in which the value of the contract is determined by an agreed-upon underlying financial asset or set of assets. In DeFi derivatives, users can create their own contracts with synthetic assets linked to other securities. Derivatives are not new in the cryptocurrency world. First BitMex was founded in 2014 which is a peer-to-peer trading platform.

Every expanding market develops its own derivatives market, which is generally orders of magnitude greater than the underlying market. Unlike traditional finance, in DeFi derivatives can be created by anyone also can be used by anyone.

Synthetix is an Ethereum based protocol for synthetic crypto assets. Synths tracks prices of fiat currencies, cryptocurrencies, stocks, or commodities. A debt pool is the foundation of the Synthetix model. Collateral in the form of $SNX tokens is used to issue a specific asset. These synthetic assets can then be traded for real ones, with the prices being recalculated using an oracle. Synthetix is bringing non-blockchain asset exposure to DeFi, giving users more options and assisting in the maturation of the crypto ecosystem. Investors can transfer Synths to other protocols because they are issued on Ethereum [7].

D. Other services

Besides the previously mentioned sectors, DeFi also can be helpful in insurance, energy management, real estate, voting, and lots of other sectors.

The insurance market is based on trust. The DeFi is an innovative way to manage trust that may be used to verify a variety of data in insurance contracts, including the identity of the insured individual. So oracles can be used to combine real-world data with smart contracts on the DeFi.

In the energy management industry, consumers and energy producers cannot purchase directly from each other. So, TransactiveGrid is an Ethereum-based startup that allows users to purchase and sell energy directly from one another.

V. RESEARCH GAP

Sr. No.	Name of research paper	Research gap
1	Blockchain disruption and decentralized finance The rise of decentralized business models [8].	Blockchain provides extreme transparency which may be dangerous to privacy, as well as decentralized Finance, may lack accountability. So, any problems arise, no central authority can fix the problem.
2	Blockchain technology and trust relationships in trade finance [9].	If 51% attack happens in any blockchain network then the group of miners will take full control of the blockchain network.
3	Cryptocurrency, a successful application of blockchain technology [10].	A legal system must be required because private cryptocurrencies provide privacy during transactions which gives advantages to cybercriminals to hide their identity.
4	The challenges and countermeasures of blockchain in finance and economics [11].	In a blockchain network, transactions are very slow. So only 8 to 10 transactions can process in one second. While other companies like Visa, PayPal processes thousands of transactions per second.

5	How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees [12].	Cryptocurrency transactions consume lots of electricity than normal transactions companies like PayPal, Visa, etc.

VI. DISCUSSION

After studying research gaps, this paper recommends we should focus on privacy protection even though blockchain transactions are encrypted and anonymous but still there is a risk of data being hacked or taking 51% control of the blockchain network which will cause big loss for users.

Second, there should be regulations and laws because blockchain gives anonymity which gives benefits to criminals, drug dealers to sell illegal things on the internet.

Also, cryptocurrency transactions are very slow compared to other normal transactions as well as it consumes lots of electricity which is harmful to the environment.

VII. CONCLUSION

In this paper, we have seen the history and information about decentralized finance have been summarized and organized. Understanding the concepts and importance of DeFi, opportunities, as well as problems, will create awareness among young people. So, they can contribute to DeFi and it will motivate researchers and developers to work on new innovative ideas and conduct research in a decentralized finance sector.

VIII. REFERENCES

[1]. V. Buterin, "A next-generation smart contract and decentralized application platform," GitHub, 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper. [Accessed 19 January 2022].

[2]. J. Frankenfield, "Smart Contarcts Definition - investopedia.com," Investopedia, 26 May 2021. [Online]. Available: https://www.investopedia.com/terms/s/smart-contracts.asp. [Accessed 19 January 2022].

[3]. "Total Value Locked (TVL)," CoinMarketCap, [Online]. Available: https://coinmarketcap.com/alexandria/glossary/total-value-locked-tvl. [Accessed 2 February 2022].

[4]. "DeFi Pulse," DeFi Pulse, [Online]. Available: https://defipulse.com. [Accessed 2 February 2022].

[5]. "How does Defi Lending Work? | DeFi Lending and Borrowing," LeewayHertz, [Online]. Available: https://www.leewayhertz.com/how-defi-lending-works. [Accessed 2 February 2022].

[6]. "DeFi Pulse," DeFi Pulse, [Online]. Available: https://www.defipulse.com. [Accessed 7 February 2022].

[7]. "The Protocols Bringing Derivatives to DeFi," Quantstamp, 25 May 2021. [Online]. Available: https://quantstamp.com/blog/the-protocols-bringing-derivatives-to-defi. [Accessed 8 February 2022].

[8]. C. B. Yan Chen, "Blockchain disruption and decentralized finance The rise of decentralized business models," Journal of Business Venturing Insights, vol. 13, p. 8, 2020.

[9]. Z. W. L. T. K. C. Michał Kowalski, "Blockchain technology and trust relationships in trade finance," Technological Forecasting and Social Change, vol. 166, p. 9, 2021.

[10].Y. N. K. D. Mohammad Hashemi Joo, "Cryptocurrency, a successful application of blockchain technology," Managerial Finance, vol. 46, no. 6, p. 19, 2019.

[11].Y. X. Y. Z. W. X. X. Z. Li Zhang, "The challenges and countermeasures of blockchain in finance and economics," System Research and Behavioral Science, vol. 37, no. 4, p. 8, 2020.

[12].P. B. H. Z. Q. X. J. Z. M. A. Victor Chang, "How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees," Technological Forecasting and Social Change, vol. 158, p. 12, 2020.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Analysing the History and Future of Self-Driving Vehicles

Ketaki Narkhede, Anish Wadekar, Deepali Sonawane, Vinayak Magdum
School of Computer Science, Dr. Vishwanath Karad MITWPU, Pune, Maharashtra, India

ABSTRACT

In the modern age, vehicles are focused on being automated in order to give human drivers a relaxed driving experience. A variety of factors have been considered in the field of automobiles that provide automated vehicles. In this work, we discuss the dominant narratives and ideologies surrounding self-driving vehicles, as well as their historical antecedents.

We focus on both the media's depiction of self-driving vehicles and the sources of the idea. Taking a look at the history of autonomous vehicles reveals just how far they have come. From science fiction in the early 1900s to the present technological reality, autonomous vehicles have come a long way. Some semi-autonomous features in modern cars, like automatic braking and adaptive cruise control, are based on such systems.

The future of autonomous vehicles lies in extensive networks of cameras and network guided systems. Companies are expected to launch fully autonomous vehicles by the turn of the next decade. Autonomous vehicles are poised to bring safe and comfortable transportation to the future. Low-income households and persons with mobility issues can benefit from AV technology by lowering transportation costs and increasing accessibility.

Keywords— Automated Vehicles, Autonomous, Semi-autonomous features, Artificial intelligent, Auto-pilot.

I. INTRODUCTION

Over the years, automotive technology has become a lot more sophisticated, and autonomous cars, also known as self-driving Cars will be the next big thing. These vehicles use advanced technology to operate independently. They do not require the input or supervision of a human driver. Some of the giant motor vehicle manufacturers have actually produced dozens of these vehicles by now, but it seems there will be a long wait before we can have these driverless cars everywhere.

Usually, this car is referred to as an autonomous car or a driverless car. It is a vehicle that travels without a human operator, but it is equipped with sensors, cameras, radar, and artificial intelligence (AI). A fully autonomous vehicle must be capable of navigating without human intervention over unadopted road networks to its predetermined destination Autonomous cars are being developed and tested by Audi, BMW, Ford, Google, General Motors, Tesla, Volkswagen, and Volvo. Over 140,000 miles of California streets and highways were navigated by a fleet of self-driving cars, including Toyota Priis and Audi TTs.

Cars with Auto Pilot Features

- Tesla (Model 3, Y, S and X)
- GM (Cadillac CT6, CadillacEscalade, Chevy Bolt)
- Audi (A6, A8)
- BMW (X5, 3 Series)
- Ford / Lincoln (Mustang Mach-E)
- Kia / Hyundai (Telluride, Palisade, Sonata)
- Mercedes Benz (E-Class, S-Class)
- Volvo (XC90, XC60, XC40)

II. HOW IT WORKS

A. BASIC REQUIREMENTS TO DESIGN A CAR

The technology and other components necessary for the development of this protocol are identified after a thorough study of autonomous vehicles. Using the information from sensor data, this paper aims to develop a protocol that will enable autonomous cars to share sensor data, thereby increasing safety and optimizing traffic. Using a simulated environment, the protocol will be tested. This block diagram provides an overview of the project to be developed.

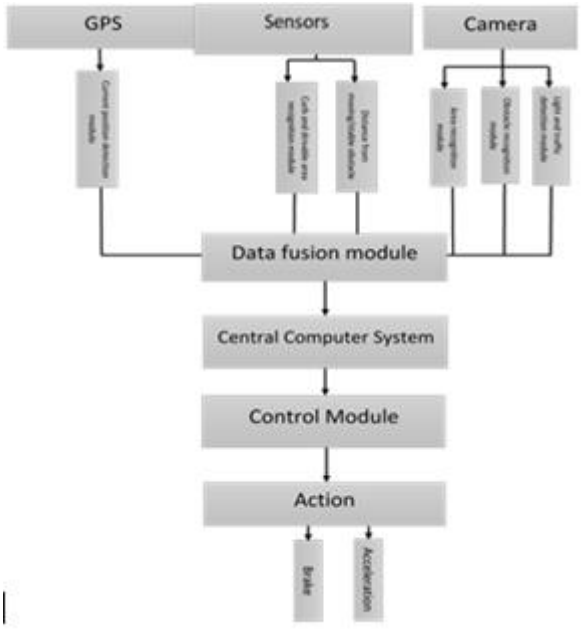


Fig. 1. Block diagram of Autonomous Car.

Figure 1 can be explained as follows

- We will design this system so that it begins from position A and reaches its destination, position B, by traversing through the path destined for it and further by examining various other conditions.
- To determine the correct route to reach the destination, pi-camera, sensors, and GPS data are used.
- Integrating all the data collected from individual sources is accomplished using the data fusion module.

- A Raspberry Pi and an Arduino UNO are used as the central computer system, which can exchange data with sensors and calculate millions of data points per second. Control is provided by a few gear motors and those motors can be controlled by Arduino UNO.
- Control modules transform the processed information so that the bot understands it.

B. METHODOLOGY

A brief about levels:

Level 1: A driver still controls most functions, but with some exceptions (such as steering or accelerating), the car can do some of them automatically.

Level 2: As part of level 2, at least one driver assistance system, such as cruise control or lane centering, is automated using information about the driving environment. Consequently, the driver is removing his or her hands from the steering wheel and foot from the pedal at the same time, disengaging from physically operating the vehicle. Although the driver still must be vigilant in this condition and be ready to take control of the vehicle, the driver should remain vigilant.

Level 3: Level 3 cars still require human drivers, but they can completely alter the safety-critical functions of the vehicle under certain traffic and environmental conditions. It means the driving force continues to be present and can intervene, if necessary, but isn't required to observe true within the same way it does for the previous levels.

Level 4: Level 4 is what's meant by "fully autonomous." Level 4 vehicles are "designed to perform all safety-critical driving functions and monitor roadway conditions for the whole trip." However, again this can be limited to the Operational design domain (ODD) of the vehicle—meaning it doesn't cover every driving scenario.

Level 5: As a fully autonomous vehicle, the vehicle should be capable of performing as well as a human driver, regardless of the driving situation, even in extreme environments like dirt roads, which will be difficult for driverless vehicles to travel on in the near future.

C. The sensory system can be classified into three different parts:

Navigation and Guidance: Instruments and techniques such as the compass, sextant, LORAN radiolocation, and dead reckoning have been used to determine - where you are, how you want to get there, and how to get there.

Driving and Safety: Driving an autonomous vehicle means directing the vehicle so that it acts appropriately under all circumstances, following the rules of the road, and seeing what is ahead of it and to the side. It is also necessary to see what is behind the car. A 360-degree view is imperative, which would require an array of video cameras and a camera to sense objects or markers.

Performance: Car's internal system management makes up a significant part of the design of an autonomous vehicle. To ensure autonomous operation, several application-specific circuit boards and subsystems are added to a conventional vehicle. A great deal of the system-level operation involves controlling power and measuring power requirements, and overall consumption, and thermal dissipation.

Sensors in AV's.:

1. Ultrasonic Sensor

Figure below shows Ultrasonic sensors. It measures distance by emitting an ultrasonic wave and receiving a reflector wave back from a target.

2. LDR Sensor

The figure below shows a LDR sensor, which functions on the principle of photoconductivity.

3. GPS

The global positioning system is a 24-satellite navigation system in which multiple satellite signals are used to determine the receiver's position on earth. A GPS navigation system is a GPS receiver that is designed for a specific purpose, such as a car or a handheld device.

- Gyroscope

A device used for measuring or maintaining orientation and angular velocity

III. FIVE CHALLENGES OF DRIVING SELF-DRIVE CARS

As a result of continuous research and development over the past fifty years, we can now see autonomous cars becoming a reality. However, there are still challenging aspects of designing an entirely autonomous system for the driverless cars.

1. Road conditions

Conditions of the roads may vary from one place to another, with some having marked, smooth highways and others with highly deteriorated roads with no lane markings. Moreover, lane markings are absent, potholes are present, the mountainous and tunnel roads have unclear signs for directions, and so forth

2. Weather conditions

The weather conditions play another spoilsport, whether sunny and clear or rainy and stormy. Autonomous cars should function in all kinds of weather conditions, with no possibility of failure or downtime.

3. Traffic conditions

Having autonomous cars on the road would require them to drive in all kinds of traffic conditions. There would be a lot of people on the road as well as a lot of autonomous cars. Anywhere there are humans involved, there are a lot of emotions involved. There may be a high degree of self-regulation and moderated traffic. However, there will always be situations where people break the law. An object may appear in unexpected circumstances. Even a few cms of movement per minute can mean a lot when traffic is dense. One cannot wait endlessly for traffic to automatically clear and have some precondition for movement to start. It is possible that if more of these cars are waiting for traffic to clear, it will eventually lead to a traffic jam.

4. Accident Liability

Accident liability is an important issue to address with autonomous cars. Who is at fault if the car is involved in an accident caused by a self-driving car? In the case of autonomous cars, the software will be the key component that drives the car and determines it's behaviours .Google's newer designs do not include a dashboard or steering wheel, but instead feature a person sitting behind the wheel .Where the car is designed in such a way that there are no controls such as a steering wheel, brakes, or accelerator pedal, how is the driver supposed to manage the situation? Furthermore, since autonomous vehicles tend to be in a relaxed state, occupants may not be paying close attention to traffic conditions when it is needed. By the time they act, it may be too late to avoid the situation.

5. Radar Interference

The sensors on an autonomous vehicle are mounted on the body, while lasers on the roof detect the reflections of radio waves from objects. The principle of radar works by detecting reflections of radio waves from objects around it. In a car on the road, radio frequency waves will constantly be emitted, and these waves will be reflected from the surrounding cars and other objects nearby. The time it takes for the reflection to occur is used to calculate the distance between the car and the object. The radar works by detecting the reflection of radio waves from surrounding objects. When on the road, a car continuously emits radio frequency waves, which get reflected from cars and other objects near the road. In order to determine the distance between the car and the object, the reflection time is measured. According to the radar reading, an appropriate action is then taken. How would a car be able to distinguish its own (reflected) signal from that of other vehicles on the road if this technology were applied to hundreds of vehicles on the road? There is a reasonable chance that this range of frequencies can accommodate all the vehicles manufactured, even if multiple radio frequencies are available for radar.

IV. HOW AUTONOMOUS CARS WILL AFFECT OUR LIVES

Cleaner Air

Ohio University has found that when self-driving cars are adopted, they will also reduce harmful emissions by up to 60 percent. Most emissions come from vehicles idling in traffic. As a result, we will have cleaner air to breathe in our cities, which will also help to protect our environment.

Less Congestion, Faster Travel

Every day, billions of hours are lost by commuters and travellers due to traffic congestion. It is estimated that when autonomous vehicles come in, travel time could be cut by as much as 40 percent. This time saved will help boost economies where driverless cars will be in use. If all they will be needed, traffic law enforcers will also have an easier time maintaining sanity on the roads.

Human drivers are known to be notorious for creating stop-and-go traffic situations, which lead to traffic congestion. This is not to forget distractions such as merges, lane changes, and bottlenecks. Self-driving cars could be a cure for traffic congestion, and people will have less to worry about getting stuck for hours in traffic jams.

More Money In Our Pockets

Human-driven cars can be expensive to maintain. When it comes to driverless cars, these costs will be reduced from insurance premiums to servicing and parking. In addition, driverless vehicles may help solve the last mile problem. When commuters use public transportation, they struggle with the final mile between their homes and the drop-off point.

Considering that autonomous cars can easily find a parking spot by themselves, these cars will make public transportation more convenient. The Ohio University study predicts that they will improve fuel economy by as much as 10 percent.

Reduced Deaths from Car Crashes

Furthermore, autonomous cars will make roads much safer. As Florida car accident attorneys point out, most fatal accidents are caused by driver error. By adopting these autonomous machines, 90 percent of traffic deaths could be prevented.

The benefits of driverless cars are numerous. These cars will simplify and enhance our lives in many ways. Here are a few of the many ways autonomous cars will improve our lives.

V. RESULT

With the advent of driverless cars, the way people travel will be disrupted and revolutionized. Despite a net positive outcome for society, such as increased mobility for older Americans and the disabled or a reduction in fossil fuel use, there will also be unintended consequences to consider. Negative effects include the loss of millions of driving jobs to the collapse of the traditional auto industry. As it seems clear that the development of self-driving vehicles will continue to gain momentum, it is important to prepare for these, and any other, unintended negative consequences that may arise from this disruptive technology.

VI. ACKNOWLEDGMENT

We would like to thanks our guide, Deepali Sonawane, Assistant Professor for guiding us in this research paper. We would also like to our University MIT-WPU for giving us this opportunity.

VII. REFERENCES

[1]. www.roboticsandautomationnews.com
[2]. www.synopsys.com
[3]. www.investopedia.com
[4]. www.iiot-world.com
[5]. www.wired.com
[6]. www.researchgate.net
[7]. https://www.maxbotix.com
[8]. https://www.elprocus.com
[9]. https://www.udacity.com
[10].https://spectrum.ieee.org

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Impact of ICT on Engineering Students Education: A Case Study on Pune Region Engineering Colleges

Nimish Godbole[1], Shantanu Kanade[2]
[1]Student, SOCS, MIT WPU, Pune, Maharashtra, India
[2]Assistant Professor, SOCS, MIT WPU, Pune, Maharashtra, India

ABSTRACT

Inthecurrentscientificandtechnologicalage, since the conventional teaching techniques are not adequate to arouse enthusiasm among the students and don't get together to the erudite person, psychological and emotional requirements of the students in the new thousand years, the strategies for teaching arithmetic should be changed. The integration of technology into teaching and learning of science has additionally not gotten away from the attention of educators. As a teaching,arithmetictoisespeciallyimpactedbythefast improvement of Information and Communication Technology (ICT) and mathematics educators have been taking a gander at approaches to incorporate ICT into the educational programs in the course of the most recentdecade.

The key advantages advance more prominent joint effort among students and support communication and the sharing of knowledge. ICT gives quick and precise feedback to students and this contributes towards positive inspiration. It likewise enables them to center around techniques and translations, answers asopposed to investing energy in dull computational estimations Late advancements in technology have changed the world outside and in addition inside the classroom; making it very attractive and intriguing for the students to know and to learn. Advancements in the application and spread of knowledge and data technology have had to change requests on education. The infusion of data and communication technology (ICT) into teachingand learning and so far as that is concerned into the realand virtual classroom has created much enthusiasm for educationalresearchasoflate.ICThasthecapabilityof demonstrating an option and more compelling teaching and learning apparatus in training. Confirmation radiatingfrominquiringaboutwritingrecommendsthat ICT has a ground-breaking and huge effect on training both as far as understudy's emotional andpsychological results in learning any subject of their decision. It has tended to make learning euphoric and enduring in a lot ofways.

KEYWORDS: Information and Confirmation Technology, eye-catching, Education.

I. INTRODUCTION

Computer Now days, majority of educational institutions are professional and hence based on ICT (information and communication technology) models. ICT regularly utilized conversely with IT (Information Technology), incorporates ways and methods for robotized data dealing with and recovery, including PCs,

telecommunications, and office frameworks [4]. The business information is not just held, discussions, still pictures, video, and interactive media. Data technology division will potentially keep on enhance into other professions and basically attack the operations of library and information services. The application of information and communication technology to library tasks have made practicality for electronic inventorying and online reference administrations, alongside other library activities, for example, computerized data, online access and document exchange, systems administration and sharingofdataassets.ICTshavebeenactualizedindata taking care of and preparing due to the development workloadconvolutedinadaptingtodataburst.Dataand communication technology makes it feasible for a personal to access information quickly and simply crosswise over the local, national and global borders in buy into broad changes that incorporate the scholastic library.Alladvancesforthecontrolandcommunication of information includes in Information and CommunicationTechnology[4].ThetermsInformation and Communication Technology recount the utilization of PC root technology and the web to make data and communication administrations accessible to an extensive variety of the clients. The expression is utilized broadly to address a scope of advancements, joining phones and rising technology gadgets and the key to these is web, which supplies the system for transporting information in various organizations consolidating content, pictures, sound, andvideo.

Information can be accessed from home, office,oranyworkstationconnectedtotheinternetsuch digitization of library resources which converts print resources into electronic form [5] [6]. The ICTs have transformed most of the educational institutions that moved from early stage of automating the educational operations to the stage of almost all spheres of educational services and routines. This growth or development impose that a broad section of the librarian's responsibility in the present era involves working not only with computers but also with other Communication and Technological tools which led to additional skills demand. The conventional academic skills, librarians are needed information and communication technology knowledge[16]. The advancement of any nation relies on the nature of instruction offered and practices. Indian instruction was notable for its Gurukul Arrangement of Training in the Vedic age. Education in India has experienceddifferentstagesandphasesofimprovement beginningintheVedicagetothePost-freeperiod.Inall phasesofadvancement,therewasaworryaboutgetting quality education considering the viable perspectives in education. Teaching and learning in the 21st century ought to be especially not the same as prior occasions, as to teaching and learning are currently happening in an inexorably online world. Generally, learning situations were limited to face– to confront conveyance or where remove instruction was embraced, the conveyance was to a great extent described by the posting of printed assets and communication were regularlyslowandcumbersome.ICTsoffergreatpower and benefit in improving students' learning, among others. In the first place, data and communication advancesofferaconstructivistwaytodealwithlearning through the arrangement of intuitive learning encounters. Second, learning through ICTs is more viable as they give chances to utilizing different advances (Video, PC, Telecommunication, and so forth.), in this way giving representation helps in the internationalization and comprehension of troublesome ideas and procedures. This gives open doors for giving connections amongst theory and practice. Third, ICTs give chances to students to increase profitable PC aptitudes which are fitting in the present occupation market. ICTs likewise give students with the repertoire ofassetstoupgradelearning.Studentsapproachcurrent and up-to-minute data; easily students can reconsider and refresh learning assets accessible to them. The utilization of ICT in education can enhance memory maintenance, increment inspiration and for the most part, extend understanding. Selinger (2004) guaranteed thatICTcanenhancethenatureofeducationsincesight and sound substance help to represent and

clarify troublesome ideas in ways that were beforehand blocked off through customary teaching assets and methodologies. There are number of advantages of using the current technologies for educational institutions like engineering colleges for different courses in order to make them professional but in resentment of that there are many challenges such as poor funding of ICT infrastructures frequent change in software and hardware, erratic power supply, poor bandwidth,copyrightsmanagementandmostimportant is lack of technical information by students, teachers or management staffs[7].

The literature study claims that the ICT promotes more collaboration between students and supports communication and sharing of learning. ICT gives fast and precise feedback to students and this contributes towards positive inspiration. It likewise enables them to focus around methodologies and interpretations of answers instead of invest energy in drearycomputationalestimations.ICTlikewisebolsters constructivist pedagogy method, wherein students utilize technology to investigate and achieve a comprehension of most of complex engineering concepts. For engineering students, there are number of computation based subjects such as mathematics, statistics, physics etc. which are becomes tough and inaccessible to many engineering students. This fact is not only accepted globally, but it is, consciously or unconsciously, being passed on from one generation to another. However, the use of appropriate ICT tools and standards by teachers and students from engineering colleges may boost their performance. There are lack studies to show the impact of using ICT in engineering colleges based on extensive survey over large number of samples. Additionally there are engineering colleges from Pune region are suffering from the undressed problems in the new technologies and ICT standards. These challenges bear most significantly on the traditional educational tasks.

Now days, the teachers should be outfitted not just with subject expertise and viable teaching techniques however with the ability to help students to take care of demand of the developing information- based society with new types of ICT and need the capacitytoutilizethattechnologytoimprovethenature of learning particularly in designing universities. The scan for approaches to incorporate technology into engineering education is affected by two principal factors.Firstistheblastoftechnologiesthatisaffecting allpartsoflifeandtheimprovementofthehumanasset. Information based laborers should be technology mindful and additionally be having basic and inventive reasoning aptitudes. Second is the engineering education change that is currently stressing the advancement of engineering procedures. With the accentuation on designing procedure, the extent of the utilization of technology in the engineering classroom has, truth be told, extended. With technology, tedious calculationsareeffectivelyplayedout,differentcasesof geometric figures easilycreated.

Coupled with distinctive visuals, technology consequently gives an approach of acknowledging classrooms exercises that energize engineering reasoning. The utilization of technology can, indeed, encouragethenewchangeofengineering,didacticsthat attention on engineering procedures as it offers snappy and precise calculations and additionally powerful visuals as those found in geometry and charts. This at that point enables students and educators more opportunity to focus on the engineering forms in the classroom. Students can create and exhibit further comprehension of designing ideas and can manage further developed engineering substance than in 'traditional' teachingsurroundings.

Since from last few decades, there are number of researchers conducted the study to claim the important role of teachers for the achievement of student's performance in terms of computational based engineering subjects furthermore, technology integration in the mix with information about research resultswouldadequatelygetreadyteachersforasimple and successful joining of ICT standard into their classrooms. Therefore, the scope and significanceof this research work is to conduct the study ICT impact on the

engineering student's performance with special reference to Pune region engineering colleges. In this paper we define the literature survey in section II. In section III we presented the proposed approach framework and design. In section VI it presents the mathematical module and section V describes the results of recommender system. The last section VI it presents the conclusion.

II. LITERATURE SURVEY

In this section we presenting the all recent techniques and presents its features, works advantages, disadvantage.
Niyaz Ahmad (1) in his paper " Viable Educational Management: A Use of ICT inAssociation of Cutting edge training Establishments"communicates that the use of ICT in the enlightening organizationwill benefit from separating the data quickly and precisely speedy, basic leadership, gives the ability to the Overseers for effective administration of training and establishment, lessens the weight of Instructors, accessible at least aggregate cost of proprietorship, gives data at the entryway and reduces the Benefit to Information Applications. He says that "the council is directly more stressed over the adjustment in viewpoint in education framework. Presently there is an in trendy articulationof„Quality'ofinstructionallovertheplace. Be that as it may, we can't redo the education system without making the organization of establishments powerfulandproficient.Also,thismustbefinishedwith the use of technology i.e. ICT in the educational administration".
J. Meenakumari and Dr. R. Krishnaveni in their study (2) in "Transforming Higher educational establishment association through ICT" have recognizedabroadarrangementofutilitariandistrictsof e-organization. The examination disclosed that statistic factors don't significantly influence e-organization in cutting edge education establishments. It is in like manner clear from this examination that joining of ICT into data association for the teaching-learning methodology is more in the relationship with Research Strategy.
IdisemiApulu(3) disclosed that the usage of Information and communication technology (ICT) to gather focused advantage has transformed into a key indispensable issue among relationship in the brisk globalizing surrounding as ICT assumes a key part in the administration of associations.
Lin and Lin (4) among others uncover that there is a developing help for the positive connection amongst ICT and its advantages. Along these lines, it suggests that ICT achieves the organizational benefit. This paper has featured on the usage and viable utilization of ICT in associations that are valuable in upperhand.Heinfersthat"theutilizationofICTgreatly affects organizational execution as it gives a stage to developmentinnumerousorganizations.Alltogether words, ICT is known to enhance organizational activities, development, and aggressiveness".
Dr. T. O. Adeyemi (5) studied the impact of ICTonthestrongorganizationofcollegesinsouth-west Nigeria.HestudiedtheimpactofICTin11universities in 6 states of Nigeria. Thinking the disclosures of this examination, it was contemplated that information dialog and technology have the essential impact on the intense organization of universities in south west Nigeria.
Hossein Zainally poor (6) in his paper "Association of Faculties by Information and Communication Technology and Its Obstacles" analyzed the convincing utility of ICT for the association by 20 senior individuals from picked assets of legislative universities in Iran. His investigation disclosures exhibit that head of assets uses the technology for organizing. It was used by them in Information gathering, basic leadership, operational arranging, spending arranging and classroom programming. It was used to the sweeping degree in

scholarly endeavours, understudy affairs; investigate affairslegitimateandbudgetaryaffairs.ICTwasusedat unusual state in supervision and evaluation of understudy affairs, investigate affairs and scholastic undertakings, money-related affairs, and administrative affairs.

Savita Desai, Prashant Shah (7) in theirinvestigation inspects on "The piece of ICT inOrganization, Teaching, Learning, Evaluation, andInvestigation in Advanced education" perceivedunmistakable activities where ICT can be utilized in theassociation of schools. The regions perceived by themare online insistences, One window-one momentadvantage, Recording of understudy interest, Issuing ofbooks by the library, Marshals for the non-teachingstaff, Security of the grounds, Criticism from students,Recordkeeping, Circulars and GRs, Alumni affiliation.Susan Mathew K.(8) in her examination "

Effect of Information Communication Technology (ICT) on capable progression and enlightening needsof libraryspecialistsintheUniversitiesofKerala"disclose that an expansive bit of the library specialists has a positive approach towards the use of ICT based organizationsinlibraries.Thespecialistsdon'tappearto becontentwiththeopendoorsintheirworkplacedueto the absence of sufficient ICT foundation in University Libraries inKerala.

TheMajorityofthespecialistspayinglittleheedtotheir age, comprehension or abilities suggested the necessity for more IT organized topics in the educational programs. To fight in a mechanically impelled world, the University managers and Library affiliations must offer opportunities to make aptitudes in ICT applications, library organization, and sensitive capacities. Library science schools and teaching divisions the nation over the need to find a way to modify library science educational modules, and consolidate noteworthy changes to achievethe solicitations and challenges of library science profession.

Matovu Moses (9) studied the levels of availability of ICT for examination organization in Makerere University and assumed that ICT offices, for example,PCsAdministrationDataFrameworkandweb were the most by and large used for examination organization. Such workplaces for examination organizationwereforthemostpartassociatedindealing with examination results, following students' scholastic progress, reviewing of students as indicated by their execution, communication amongst speakers and heads of division, communication to students by means of emails.

Justus ArihoTwinomujuni(10) in his examination of "Issues in ICT utilization in picked Associations of Higher Learning in Kabale Locale " perceivedfactorsascostofICTgettingreadymaterials, aptitudes improvement in ICT and definitive help in associationwithICTexecution.Hefoundthatthatthere is a quantifiably unimportant association between the cost of ICT getting ready materials and ICT execution factors. Cost of ICT getting ready materials negatively affected ICT execution. As to abilities improvement in ICT and ICT use, he found that there was a genuinely hugeassociationbetweenthetwocomponents.Abilities improvement in ICT positively affected ICTexecution.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

A. Problem Definition

Thestatementofthepresentstudyisentitledas“Use of ICT in e-governance of higher education with specialreferencetocollegesandinstitutionsofPune – A Critical Study”. It is believed that the studywill give an insight about what extent the latest technologies of ICT are being used by the colleges/institutions and what are the impressions and impact of ICT on administration ofcolleges.

IV. HARDWARE ANDSOFTWARE USED

- Software Requirements

FrontEnd : Java 1.7, 1.8
Back End : Mysql 5.5, 5.6
ToolsUsed : NetBeans 7.2, 8.0
Operating System : WindowsXP/7/8/10

- Hardware Requirements

Processor : pentiumiv 2.6 ghz
RAM :512 mbddram
Monitor :15" color
Hard disk : 40gb
Keyboard : standard 102 keys
Mouse : 3buttons

V. RESULT

The aim of this research is to find out and critically evaluate the use of ICT for e-governance of the colleges/institutes affiliated to university of Pune. The study also intends to compare the extent of utility of ICT tools and evaluate the awareness of ICT in the colleges. The data is collected from total 15 colleges including professional and traditional colleges out of this we analysed data from 6 collages. The respondents from the colleges include non-teaching staff, teaching staff and director or principal of college. The following table shows the number of sample taken for research categorized according to university and type of college. The colleges offering traditional courses include Arts, commerce and Science colleges of the respective universitiesandtheprofessionalcollegesincludethe institutes providing professional courses like MBA, MCA, MCM, MPM, BBA, BBM, BCA etc.and
engineering colleges.

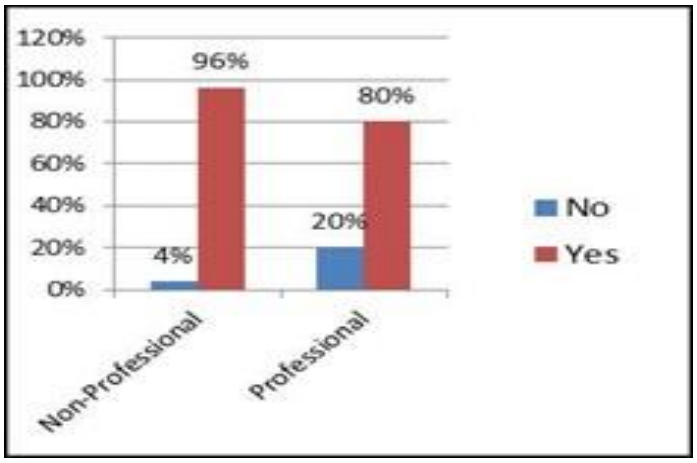


Figure Use of ICT in student process for NMU Colleges

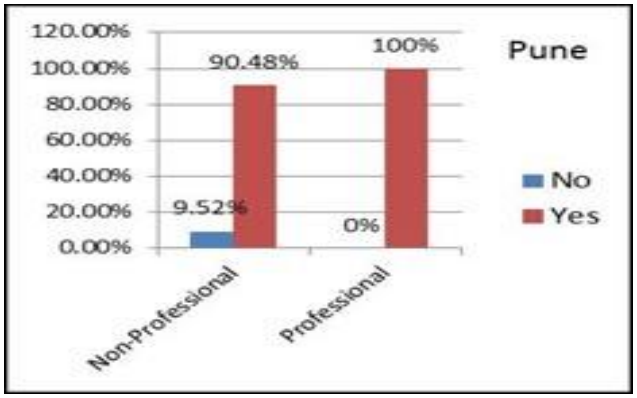


Figure Use of ICT in student process for PU colleges

The above graphs represent the use ICT for the student admission system in professional and traditional (non-professional) colleges. Using this technology it leads to fast, efficient and transparent administration. Few traditional colleges (4% in institutions and 9.25% in colleges) are still using manual system for student admission process.

The use of ICT in different processes of student admission in the HEIs of colleges the different processes involved in student admission system need ICT for their effective work. The tools generally used by the colleges are MS-Office, Custom Software, and ERP. If the system is not using information system then the whole process is done manually. It is seen that MS-Office is used maximum. For storing the enquiry details 51.43% use MS-Office and 51.43% use it for admission details.54.29%collegesmanuallygeneratediscount notification. 60% HEIs prefer manual checking of thetestimonialsand55.88%forclearanceofstudent after completion.

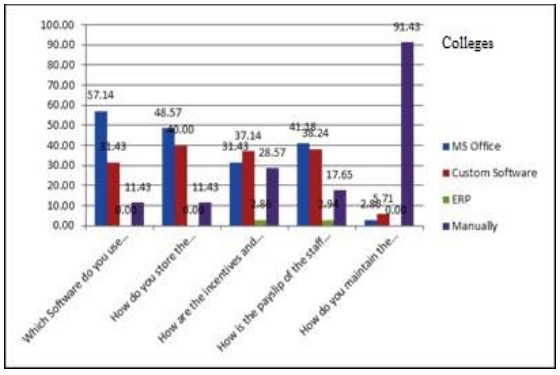


Figure ICT tools used in HEIs of colleges for Personnel Management

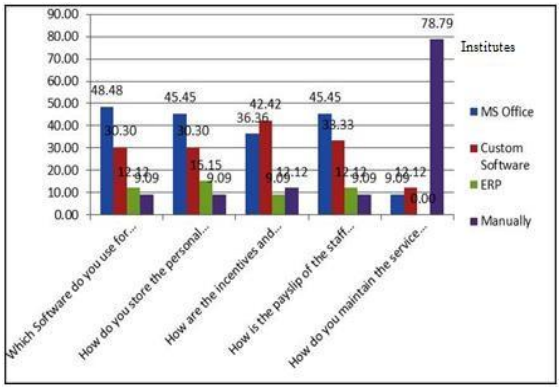


Figure ICT tools used in HEIs of PU forPersonnel Management

Useoftechnologyusedtolinkattendanceofthestaff with the payroll system ICT plays a vital role for effective functioning and linking of processes. The following figure shows the percentage of linking of staff attendance and payroll system in colleges and institutions with the help of technology (54.29%). The extent of linking is exactly same in the institutions of both theuniversities.

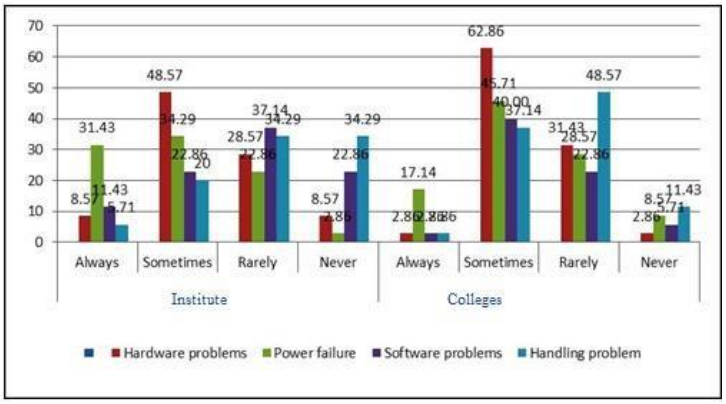


Figure Frequency of breakdown of system by using the technology in HEIs

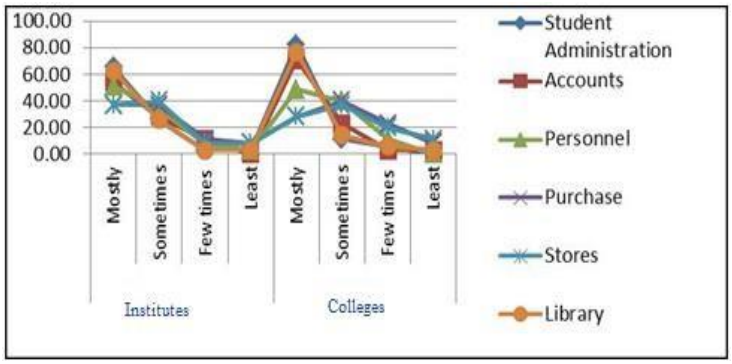


Figure Extent of use of ICT in different functional areas in HEIs of NMU and PU

VI. CONCLUSION AND FUTUREWORK

Managementofdatageneratedposesabigchallenge for the institutions using ICT for their day to day operations. Some of the commonly used tools for these include MS Office, emails and telephones. Tools such as Wikis, blogs and video messagingare used to lesser extent and customised software are used by very few institutions. In general it can be concluded that all the HEIs accept the importance and utility value of ICT. A very heartening aspectis that the awareness levels are at its peak, with regard to ICT. The factor which differentiates between successful implementation and failure of the system depends on the appropriate training to all the stakeholders with respect to their roles and responsibilities in the usage of various ICT tools. Committed efforts in this direction shall also leadto effective contribution of individuals to the society and the country. Efficiency and effectiveness in the administration of HEIs can be improved by the model suggested by the researcher. Some of the prime areas where usage of ICT tools as identified inmystudyincludestudentadmissionmanagement, human resource management, accounts management, purchase and inventory management, library management, exam management and for the interaction between the university andHEI‟s.

Nowadays technology is being implemented in all the rural and urban areas. Of course, there are certain limitations and problems in rural area such as load shedding, power failure, low internet connectivity, experts to use the system, dependency on a single person etc. But these limitations are overcome by alternative

solutions likepowergenerators,providingtrainingtodecrease dependency on individual. Sometimes it takes time to switch over to the alternatives and work is delayed. But these problems are temporary innature andcanbesolved.Lookingatthebenefitsoftheuse of technology these problems are negligible and couldbeovercome.Thepurposeofthisresearchwas to find out whether technology is actually used effectively for e-governance in higher educational institutions. The study reveals that there are many direct and indirect benefits using the integrated system for the e-governance of theinstitutions.

VII. REFERENCES

[1]. Natesan, N. (2001). Teaching Concepts in Mathematics through Video Cassette – An Experiment. Journal of EducationalResearch and Extension, 38, (1).

[2]. Subbaiah, S. (2005). Application of ICT in English Language Teacher Education. Ph.D., Education, Alagappa University,Karaikkudi.

[3]. Kumar Rajender(2007). Comparative study of the effectiveness of three Instructional Systems for teaching Information Technology to Secondary School students ,Indian Educational Review,.43(2).

[4]. Raja Roa, S. (2008).Access, Awarness and Use of Media Support Services:Strategies to make them popular with the Learners. Indian Journal of Open Learning, 2008, 17(2),163-173

[5]. Li, L. L. (2009), Emerging technologies for academic librarians in the digital age. London: ChandosPublishing.

[6]. Mutula,S.M.,&Wamukoya,J.M.(2007).Web information management: A cross disciplinary approach. London: ChandosPublishing.

[7]. Majumdhar, R. P., & Roy, S. (2008), Application of blog in library and information services. IASLIC Bulletin, 53 (4),241-246.

[8]. Reinking, D. (2005), Multimedia learning of reading. In R. E. Mayer (Ed.), The Cambridge handbook of multimedia learning, 355-376. New York: Cambridge UniversityPress.

[9]. Singh, N. (2001), Internet: Importance and Usage for Library andInformation professionals. DESIDOC Bulletin of Information Technology, 21 (3), 17-28.

[10]. Abdelrahman, O. H. (2009). The State of ICT Implementation and Training at the University of Khartoum Library System (UKLIS). Paper presented at International on academic libraries (ICAL2009).

[11]. Adeyoyin, S. (2005) information and communication technology (ICT) literacy among the staff of Nigerian universitylibraries, Library Review, 54(4),257-266.

[12]. Afrodite, Malliari., Stella, Korobili., and Sofia, Zapounidou.(2011). Exploring the information seeking behaviour of Greek graduate students: AcasestudysetintheUniversityofMacedonia. The International Information and Library Review.43, 79-91.

[13]. Ahmad, N., & Fatima, N. (2009). Usage ofICT products and services for research in social sciences at Aligarh Muslim University. DESIDOC Journal of Library & Information Technology, 29(2),25-30.

[14]. Ajidahun, C. O. (2007). The training, development and education of library manpower in information technology in university libraries in Nigeria. World Libraries, 17(1),12-17.

[15]. UchennaAgu, S., Onyishi, I. E., &Okwo, I. M. (2012). Information and communication technology(ICT) and Administrative processes in Universities in Sout-Eastern Nigeria. International Journal of Computer Applications, 57(11),34.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Comparative Analysis of Different Shortest-Path Algorithms

Sanika Kendhe[1], Abhishek Nishad[1], Vikas Magar[1]
[1]School of Computer Science, Dr. Vishwanath Karad MIT World Peace University, Kothrud, Pune, Maharashtra, India
[2]Assistant Professor, School of Computer Science, Dr. Vishwanath Karad MIT World Peace University, Kothrud, Pune, Maharashtra, India

ABSTRACT
A shortest-path algorithm is an algorithm that comprises of finding the shortest path between the given vertex and all other vertices in a graph. This paper presents a comparison of different shortest-path algorithms used for different objectives. This paper will provide a short and crisp idea of all the shortest path algorithms. The explanation of these algorithms is represented by the different examples of each type with its complexity.
Keywords— Shortest-Path Algorithms, Dijkstra's Algorithms, Bellman-Ford Algorithm, Floyd-Warshall Algorithm

I. INTRODUCTION

There is always the necessity for the shortest path algorithms in computer science. That is why it is the most considered topic in this field. The idle shortest path is the one that has minimum lengths from the start node to the end node. As per the requirement, there are different shortest path algorithms based on graph theory [1][2]. Graph theory is mostly popular for AI-based application development like google map, driverless cars. Graph theory has several real-life applications like ola, uber, Zomato and too much organization's work based on graph theories shorted path algorithm strategy.
The graph is a non-linear data structure consisting of nodes and edges. A graph consists of a finite set of vertices (or nodes) and a set of edges that connect a pair of nodes.

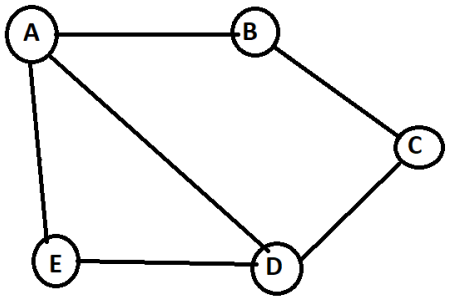


Fig.1. Graph Structure

The Graphs can be broadly divided into different categories. They are as follows: -

A. Weighted graph
B. Unweighted graph
C. Directed graph
D. Undirected graph

A. Weighted graph: These graphs are defined as the graphs whose edges have values. Edges can represent any value like cost, length, distance.

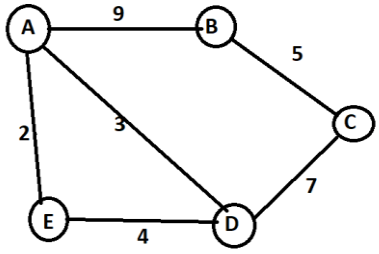


Fig.2. Weighted Graph Structure

B. Unweighted graph: In these graphs, there is no value is associated with edges by default.

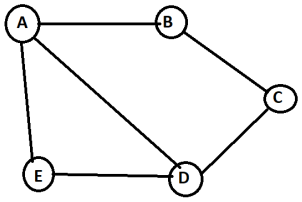


Fig.3. Unweighted Graph Structure

C. Directed graph: These graphs define the directions from one node to another node.

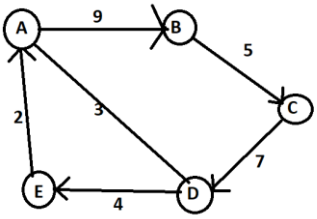


Fig.4. Directed Graph Structure

D. Undirected graph: These graphs are defined as graphs where a set of objects are connected, and all edges are bidirectional.

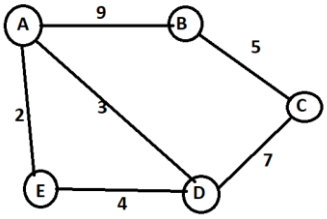


Fig.5. Undirected weighted Graph Structure

II. RELATED WORK

It clarifies that the shortest-path algorithm finds a path comprising the minimal cost between two vertices in a graph [3][4]. This paper presents a survey of different shortest-path algorithms used for different problems. The paper also recommends designing the shortest path routing algorithm using Particle Swarm Optimization for Wireless Sensor Network on which if we send the data packets it will take less time, less energy so that the battery consumption will be minimalized.

These days, in computer networks, the routing is based on the shortest path problem [5]. This will support in minimalizing the overall costs of setting up computer networks. New technologies such as map-related organizations are also applying the shortest path problem. This paper's main objective is to estimate the Dijkstra's Algorithm, Floyd-Warshall Algorithm, Bellman-Ford Algorithm, and Genetic Algorithm (GA) in solving the shortest path problem [6][7]. A short evaluation is achieved on the various types of shortest path algorithms. Further explanations and applications of the algorithms are illustrated in graphical forms to show how each of the algorithms works.

III. PROBLEM STATEMENT

While studying diverse algorithms it is tough to find the appropriate algorithm for a given challenge. It was problematic to map a proper algorithm with the given problem.

IV. ALGORITHMS

A. Dijkstra's Algorithm

Dijkstra's algorithm is a single-source shortest path algorithm. Here single source means that only one source is given, and we must find the shortest paths from source to all nodes.

Example:

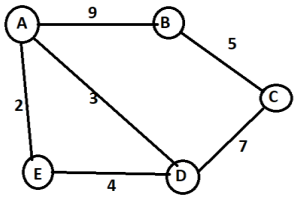


Fig.6. Weighted Graph

- **Advantages**

1. The algorithm is having low complexity.

- **Disadvantages**

1. The algorithm cannot be used for negative weights.
2. This algorithm cannot be used for dense graphs.
3. It does a blind search and thereby consumes a lot of time and wastes resources.

Complexities

Time Complexity: O(v2)

B. Bellman-Ford

Bellman-Ford is an algorithm that computes the shortest path from a single source vertex to all the other vertices in a weighted graph. It is slower than the Dijkstra algorithm but more versatile as it is capable of handling graphs with some of the edges being negative numbers.

Example: -

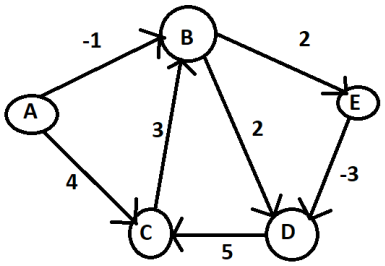


Fig.7. Negative Cycle Weighted Graph

- **Advantages**

1. Negative weights are found in various applications of graphs
2. Works better than Dijkstra's for distributed systems.
3. In these edges are considered one by one.

- **Disadvantages**

1. Does not work with undirected graphs with negative edges as it is declared a negative cycle

Complexities

Time Complexity: O(n3)

C. Floyd-Warshall Algorithm

The algorithm of discovering the shortest path between all the pairs of vertices in a weighted graph. The algorithm works for both directed and undirected weighted graphs.

Example: -

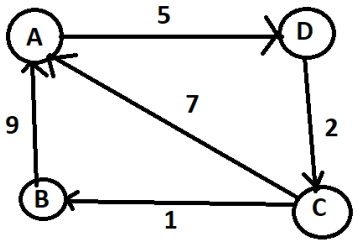


Fig.8. Positive weight cycle Graph Structure

Advantages

It helps you to find the shortest path in both negative and positive weighted graphs.

A single execution is more than enough to find the length of the shortest path between all the pairs of vertices.

Disadvantages

It works slower than other algorithms.

Complexities

1. Time Complexity: O(n3)

V. COMPARATIVE ANALYSIS

As discussed above following comparisons are found into the different shortest path algorithms. Every algorithm has some advantages as well as disadvantages.

TABLE I. COMPARATIVE ANALYSIS OF ALGORITHM

Algorithm	**Dijkstra**	**Bellman-Ford**	**Floyd-Warshall**
Negative edges	Does not work	Work	Work
Time Complexity	$O(N^2)$	O(MN)	$O(N^3)$
Space Complexity	O(M)	O(M)	$O(N^2)$
Source algorithm	Single	Single	All sources
Work with Undirected Cycles	Yes	Yes	No

Where,
M= number of edges
N=number of Nodes

VI. CONCLUSION AND FUTURE WORK

Table I gives the time complexity for each of the Dijkstra's, Floyd-Warshall and Bellman-Ford algorithms display that these algorithms are adequate in terms of their overall performance in resolving the shortest path problem. All these algorithms generate only one solution. It will be extended and enhanced in finding the shortest path or distance between two places in a map that signifies any type of network. In addition, other artificial intelligence techniques such as fuzzy logic and neural networks can also be employed in refining existing shortest path algorithms to make them more intellectual and more efficient.

VII. REFERENCES

[1]. Huijuan Wang, Langfang, China, "Application of Dijkstra algorithm in robot path-planning", Second international Conference on mechanic automation and control engineerig, 15-17 July,2011.

[2]. Yi-zhou ChenShi-fei ShenTao ChenRui Yang, "Path Optimization Study for Vehicles Evacuation Based on Dijkstra algorithm", ScienceDirect Procedia Engineering 71 (2014) 159 – 165.

[3]. Athanasios K. Ziliaskopoulos And Hani S. Mahmassani, "Time-Dependent, Shortest-Path Algorithm for Real-Time Intelligent Vehicle Highway System Applications", Transportation Research Record pp. 94-100

[4]. D. E. Kaufman and R. L. Smith. Minimum Travel Time Paths in Dynamic Networks with Application to Intelligent Vehicle/ Highway Systems. !VHS Journal, in press.

[5]. Q.P. Gu, T. Takaoka, A sharper analysis of a parallel algorithm for the all-pairs shortest path problem, Parallel Comput. 16 (1) (1990) 61–67.

[6]. T. Hagerup, Improved shortest paths on the word RAM, in: 27th Colloquium on Automata, Languages and Programming (ICALP), in: Lecture Notes in Comput. Sci., Vol. 1853, Springer-Verlag, 2000, pp. 61–72.

[7]. Y. Han, V. Pan, J. Reif, Efficient parallel algorithms for computing all pair shortest paths in directed graphs, Algorithmica 17 (4) (1997) 399–415. [51] T. Harris, The Theory of Branching Processes, Springer-Verlag, 1963

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Identification of Traffic Police Requirements Based On Traffic Concentration Along With Traffic Police Detection

Sneh Thorat, Kushagra Suryawanshi, Kshitija Supekar, Indraneel Tilloo
TY B. Tech, Department of Computer Science and Engineering, MIT World Peace University, Pune, Maharashtra, India

ABSTRACT
Traffic Detection System plays a vital function in the smart city platform in the current environment. The automated traffic management system's fundamental component is automatic moving vehicle detection from video sequences. In a millisecond, humans can detect and recognize things in complex surroundings. However, in order to transfer that mental process to a machine, we must first master the skill of object detection using computer vision techniques. This article addresses traffic concerns by determining the need for traffic cops depending on traffic density. YOLO v5 and computer vision are used to detect traffic cops. The findings of the investigation suggest that the proposed system can give useful data for traffic surveillance.

I. INTRODUCTION

Amajorproblemisseenineverydaylifeaspeoplearealwaysinahurrytoreachtheiroffices,schools etc. The population, as well as the number ofvehicles on the road, is increasing day by day. Imaginebeing late to the office one fine morning only to reach ata junction where the signal has malfunctioned. All thevehicles you see are congested in the middle of the roadwith no way for any vehicle to get out. That's when werealise the importance of traffic police. But unfortunatelymanytimestheyaren'tpresentthere.

Hence we came up with a solution of developingasoftwaretoavoidmajortrafficjamsandvehiclecongestions at rush hours using image recognition anddeeplearningalgorithms.

Thissoftwareaimstoprovidesolutionstoeveryday traffic problems by a simple way of alertingtraffic policemen of increasing vehicles at a particularsignal in a given span of time. Busy roads of India withreckless drivers and untimely signal malfunctions createshavoc due to which accidents and delays are prone tohappen. Our software will immediately notify the trafficinchargeofthatparticulararearegardingthesignalsmalfunction or increase in vehicle activity by installing abasiccameraandmajorroadjunctions. This will helprun traffic police activities smoothly and make peoplefollowtrafficlawsobediently.

Related Works:

Over8Literaturesurveypaperswereviewedand researched. It was found out that most of them usedYOLOv5anddeeplearningalgorithmstodetectvehiclesusingadatasetofimages.Allpaperswerepublishedafterori n2020.

A model is trained in [1] which uses alargenumber of preprocessing techniques that gives a higheraccuracy rate. Post-processing is also used to eliminatethenoiseregionsandproduceamoresmoothshapeboundary.

Thesystem in [2] is a simple real-time videoanalyzer. It has the potential to check whether peoplewearmasksornotandthushelpsustodefeatthewidespreadCOVID-19virus.

Modelstrainedin[3]have a higher accuracyrateindetectingthespeedandvehiclesaswell.It outperformsotherstate-of-the-artdetectionmethods.Thismodeliscompactandtakesuplessstoragespace.

Amulti-sensormulti-levelenhancedconvolutionalnetworkarchitecture is proposed in [4].Combining this technique withLiDAR captured imagesnot only ensures. Reliable and accurate vehicle detectionbutalsodetectsvehiclesindifferentlightingconditions.

[5]presentsanadvancedDLframeworkformotorway traffic flow prediction, by chaining togetherdataprofilingandoutlieridentification,spatialandtemporalfeaturegeneration,andvariousDLmodeldevelop ment.

Themodelproposedin[6]wasabletodetectnotonlyterrestrial-capturedvehicleimagesbutalsoimagescapturedfromaUAVthathaspoorquality.

A model which helps in detecting modules of asatellite using video clips as a dataset was proposed in[7].

The strongest advantage of YOLO as comparedtosimilarmethodsisthespeedof45framespersecondisproposedin[8].OthersimilaralgorithmssuchasR-CNNandDPMhaveamuchlowerFPS.

II. DATASET AND FEATURES

Thedatasetcomprises200imagesthatwerecollected through net scraping from various resources.Various data augmentation and preprocessing techniqueswere used on the dataset. Data augmentation is a set oftechniquesforproducingadditionaldatapointsfromcurrent data in order to artificially increase the amount ofdata available. The examination and editing of digitisedimages, particularly in order to increase their quality, isknownasimagepre-processing.

The image preprocessing techniques used in thispaperare:

1. Auto-orientation
2. Resize-416x416

The following are the dataaugmentationapproachesemployedinthispaper:

1. Shear:+-25degreesHorizontal,+-25Degreesvertical
2. HorizontalFlip
3. Grayscale
4. Brightness:Between-25%to+25%
5. Blur:Upto2px
6. Noise:Upto3%ofpixels

By using this our dataset was expanded to 600images.Thedatasetconsistsofpolicemanimagesclicked from different angles for the better training of themodel.ThedatasetimageswereannotatedusingtheLabelImgtool.

III. METHODOLOGY AND ALGORITHMS

Thefollowingmethodscanbeusedtoprocess images:

1. Imagesegmentation
2. Detectionofobjects.

Object detection is the technique utilised in thispaper.Objectdetectionisacomputervisionapproachfordetecting entities in images or videos. Object detectionalgorithmsoftenusemachinelearningordeeplearningto generate meaningful results. We can recognize andidentify objects of interest in photos or video in a matterofsecondswhenwelook at them. Object detection'spurposeistouseacomputertoimitatethisintelligence.

Image segmentation is a technique for breakingdownadigitalimageintosubgroupscalledImagesegments.Thisreducestheimage'scomplexity,makingiteasier tohandleoranalyse.Segmentationmeansassigninglabelstopixels.

In this paper, we have used two object detectionalgorithmsnamely

I. YOLOv5

II. Detectron2

I. YOLOv5

TheobjectdetectionalgorithmYOLO("YouOnly Look Once"), divides images into a grid system.Eachgridcellisinchargeof detecting items withinitself.Becauseofitsspeedandaccuracy,YOLOisoneofthemostwell-knownobjectdetectionalgorithms.

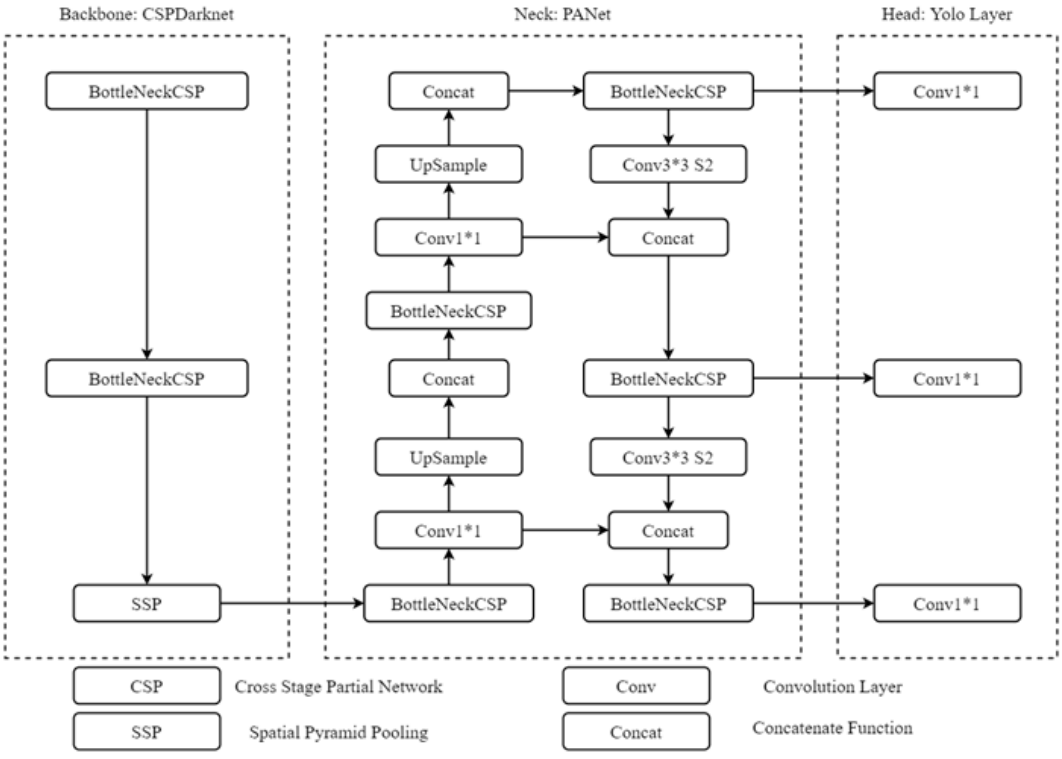


Fig 1.1 YOLOv5 Architecture

Glenn Jocher introduced YOLOv5 utilising the PytorchframeworkshortlyaftertherelеaseofYOLOv4.
On GitHub, you can find the open-source code. The IoUscoreindicateshownearthepredictedboxisto the actual box. It has a range of 0.0 to 1.0, with 1.0 beingthe best result. The box is characterised as Positive sinceit surrounds an object when the IoU is larger than thethreshold.
'mAP'isaprominentassessmentmetricincomputervision(i.e.localizationandclassification).Localizationestablishes whereaninstanceis(e.g.,boundingboxcoordinates),whilecategorizationdescribeswhatitis(e.g.adogorcat).
The mean Average Precision, or mAP score, iscalculatedbyaveragingthe AP over all classes and/orthetotalIoUthresholds,dependingonthedetectionchallengesavailable.
The mean Average Precision, or mAP score, iscalculatedbyaveragingtheAPoverallclassesand/or thetotalIoUthresholds,dependingonthedetectingproblems.
Yolov5'snetworkarchitectureisdividedintothreesections:
(1) CSPDarknetisthebackbone,
(2) PANetistheneck,
(3) YoloLayeristhehead.
ThedataisfirstsuppliedintoCSPDarknet,whichextractsfeatures,andthenintoPANet,whichfuses them. Finally, Yolo Layer gives you the results ofyourdetection(class,score,location,size).
Yolov5'sBenefitsandDrawbacks:
It'saboutathirdofthesizeofYOLOv4(27vs244MegaBytes). It's around 180 percent faster thanYOLOv4.Ontheidenticalassignment,it'saboutasaccurateasYOLOv4(withaslightdifferenceof0.003mAP). The fundamental issue is that, unlike prior YOLOversions,thereisnoofficialpaperforYOLOv5.

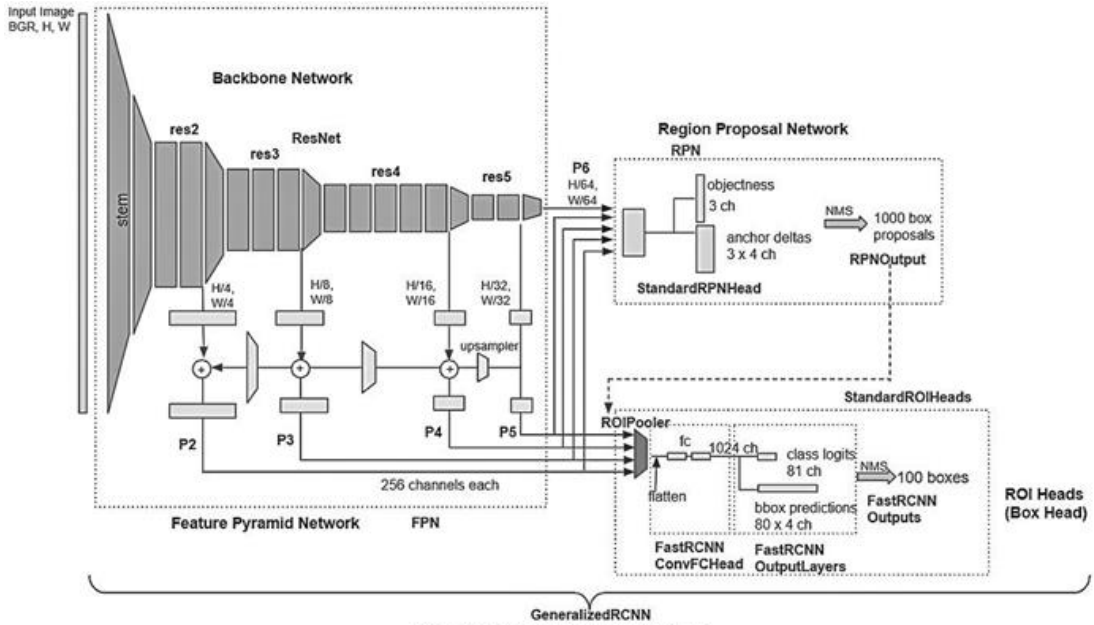


Fig 1.2 Detectron2 Architecture

II. Detectron2

Detectron2 is a complete rebuild of Detectron,which was first released in 2018. Caffe2, a deep learningframework funded by Facebook, was used to create theprecursor. Caffe2 and Detectron are no longer supported.Caffe2 is now included in PyTorch, and its successor,Detectron2,isbuiltentirelyinPyTorch.

Detectron2 aims to promote machine learning byproviding quick training and tackling the challenges thatbusinesses experience when transitioning from researchtoproduction.Ifweneedtoquicklytrainanobjectdetectionmodelwithaspecificdataset,Detectron2comes to the rescue. The COCO dataset is used to trainallofthemodelsinDetectron2.Onthepre-trainedmodel,we only need to fine-tune our custom dataset.The Detectron2 has a variety of Object Detection modelstochoosefrom.InstanceDetectionisoneofthese.

The classification and localization of an objectwith a bounding box around it are referred to as instancedetection. The Faster RCNN model from Detectron2'smodel zoo will be used to determine the language of textfromphotosinthisarticle.Objectdetectioncanbeconductedonanycustomdatasetusing Detectron2.

IV. RESULTS

To evaluate custom YOLOv5 detector performance,wehavetakenthehelpofTensorBoard'sScalarDashboard. The model has been trained on 400 epochsfortheYOLOv5method.

The metric mAP (mean Average Precision) is widelyused to evaluate the accuracy of object detectors such asthe Faster R-CNN, SSD, and many others. Precision is ameasurethatassessestheaccuracyofyourpredictions.In other words, the percentage of your predictions thatare correct is high. Recall assesses your ability to find allofthepositives.Thealgorithm'sabilitytodetectanobject'scentreandhoweffectivelytheprojectedbounding box encompasses an object that is measured inboxloss.

The probability of finding an object in a proposedzone of interest is measured by objectness. The imagewindow is likely to contain an object if the objectivity ishigh.Theclassificationlossindicateshowwellthealgorithmcanpredictanobject'sexactclass.

The model's precision and mean average precisionimproved significantly before levelling out after roughly100epochs.ThehighestpossiblemAPscorewas0.791.

Around50epochs,boxlossstartstodeclineabruptly.Lossesinclassificationstayconstant.

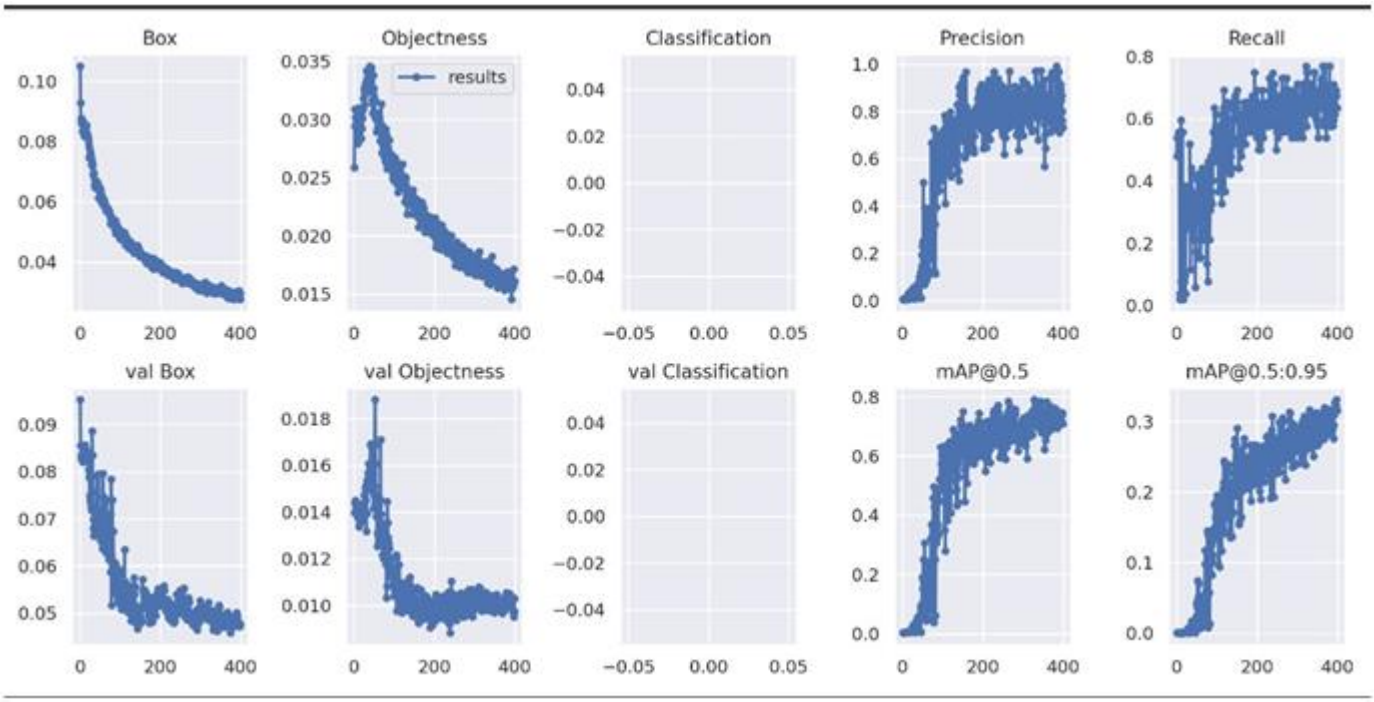


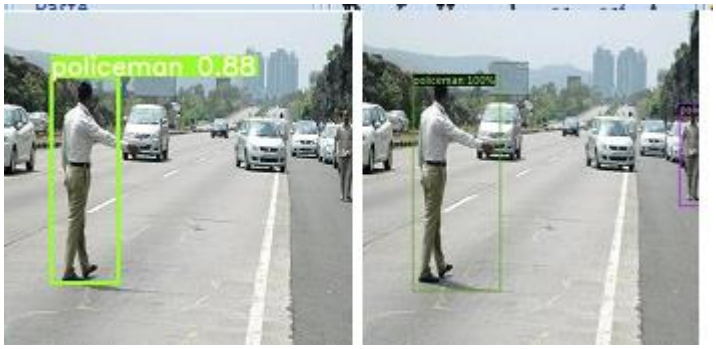
Fig 2.1 YOLOv5 Results

After50epochs,objectlosseslikewiseexhibitasignificantreduction.

Detectron2:

WhendeterminingmAP, the Intersection over Union(IoU) score is used. It's a value between 0 and 1 whichindicateshowmuchtheexpectedandgroundtruthbounding boxes overlap. An IoU score of 0 indicates thattheboxesdonot overlap. An IoU score of 1 indicatesthat the boxes' union is equal to their overlap, indicatingthattheyareperfectlyoverlapping.Thismodelwastrained on 1500 epochs with the Detectron2 algorithm.This model has a precision score of 0.505 and a recallscoreof0.491ontheIoUscale.

Also,wenoticedthatinthetwomodelsthatwe have trained, the Detectron2 is not able to distinguishbetweenapedestrianwearingwhiteclothesandatrafficpoliceman. In some cases, there were false positivesdetected by Detectron2. But in the case of the YOLOv5algorithm, it was able to distinguish between thepedestrianandthepoliceman.Differenceasfollows:



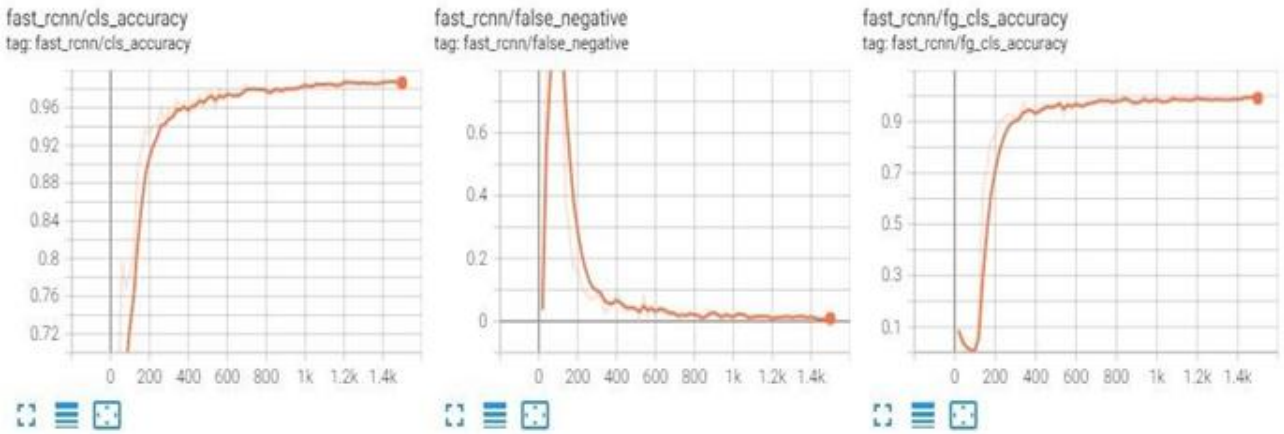


Fig 2.2 Detectron2 Results

V. CONCLUSION AND FUTUREWORK

In this paper we introduced Object Detection forIndian Traffic Policeman Detection. The YoloV5 andDetectron2 Algorithms are used in this study. The modelwas detecting a policeman from features like his WhiteshirtandKhakicolourpants.Themodelwassuccessfullyableto distinguish a police officer and anormal pedestrian wearing a white shirt. As PolicemanDetectionhasn'tbeenimplementedyet,wecannotcomparetheseresults with any other research papers.Based on the work presented in the study, The IoU scorefor the Detectron2 algorithm is 0.505 and the mAP scorefor the YOLOv5 algorithm is 0.791. The lack of datasetswas a limitation; however, by expanding the dataset, thestudycouldbeimproved.Inthefuture,ifneweralgorithms are discovered to yield better results, they canbeusedtoimprovePolicemandetection.

Afutureupgradetotheprojectwillbeasmart signal. The signal will allow vehicles to pass on the basisoftrafficinthecurrentpath.Forexample,ifajunction of four roads is present in a heavily populated area, thesignals on the junction will use our algorithms to detectthe number of vehicles passing through each of the fourroads. The road having the highest number of vehicleswill be given the first priority and will be allowed to passwithanopeningof 30 seconds. The road with fewervehiclesthanthefirstwill be given less priority andhencewillbeopenforalessperiodoftimedependingon the number of vehicles. In this way, the wait time, aswellasthetrafficflow,willbecoordinatedwithease.

Fromthe given two images we can infer thatdetectron2 is not able to distinguish a normal pedestrianwearing a white shirt from a traffic policeman, which isnot the case for the YOLOv5 model. Also, in the case ofthe Detectron2 model, there were more false positivescompared to the YOLOv5 model. The time taken for theYOLOv5modelwasmuchlesscomparedtotheDetectron2 model. Based on the work presented in thestudy, it is plausible to conclude that the YOLOv5 modeloutperformstheDetectron2modelinaspectsofcomputationtimeandaccuracy.

VI. REFERENCES

[1]. J. J, B. R and A. Al-Heety, "Moving vehicle detectionfrom video sequences for Traffic Surveillance System",2022.

[2]. VSharma,"FaceMaskDetectionusingYOLOv5forCOVID-19",2020

[3]. W. Jia et al., "Real-time automatic helmet detectionof motorcyclists in urban traffic using improvedYOLOv5 detector", IET Image Processing, vol. 15, no.14,pp.3623-3637,2021.Available:10.1049/ipr2.12295 [Accessed17January2022].

[4]. J. Zhu, X. Li, P. Jin, Q. Xu, Z. Sun and X. Song,"MME-YOLO:Multi-SensorMulti-LevelEnhancedYOLO for Robust Vehicle Detection in TrafficSurveillance",Sensors,vol.21,no.1,p.27,2020. Available:10.3390/s21010027.

[5]. A. Mihaitaa, H. Lib and M. Rizoiua, "Trafficcongestionanomalydetectionandpredictionusingdeeplearning",2020.

[6]. S. Cepni, M. Atik and Z. Duran, "Vehicle DetectionUsing Different Deep Learning Algorithms from Image Sequence",BalticJournalofModernComputing,vol.8,no.2,2020.Available:10.22364/bjmc.2020.8.2.10.

[7]. T. Mahendrakar, R. White, M. Wilde, B. Kish,"Real-timeSatelliteComponentRecognitionwithYOLO-V5",2021.

[8]. A. Abdulkader, C. Vlahija, "Real-time vehicle andpedestrian detection, a data-driven recommendationfocusing on safety as a perception to autonomousvehicles",2020.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Alunite (Soil) Mineral Identification in Aurangabad District

Jaypalsing N. Kayte, Ratnadeep R. Deshmukh
Department of Computer Science & IT, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India

ABSTRACT
This paper us an analysis of hyperspectral image spectra (Hyperion EO-1) and field spectra (Fieldspec4) data to identify mineralization zone and mineral spectral behavior. Comparative analysis of field spectra and image spectra is very useful to identify mineralization zone and surrounding host rocks and soil. The chosen method entails collecting field spectra, processing them for noise, and spectral matching with USGS library end-members. A Hyperspectral remote sensing technique was applied with three progressive steps. First, the processing and interpretation of space-borne Hyperion (EO-1) data with a focus on the areas characterized by alteration and mineralized zones. Preliminary processing of Hyperion (EO-1) data involved removal of striping followed by atmospheric corrections. Additional processing stages include the Minimum Noise Fraction (MNF) transformation to minimize data dimensionality and the Pixel Purity Index (PPI) as a pure pixel locator. The Spectral Angle Mapper (SAM) categorization technique aids in the detection of end members. According to this study, the probability of alunite mineral is 0.85.

Keywords— PPI, SAM, EO-1, MNF, USGS, IMA, FLAASH, VNIR, SWIR, DN, CCD, PCA, NASA, BE, SFF

I. INTRODUCTION

Mineral deposits are geological entities found deep under the earth's crust that contain unusually high concentrations of certain elements with economic worth. The polarity of tectonic magmatic domains established by crustal evolutionary processes and produced by favorable surficial habitats and processes influence the homogeneity of concentrations in the earth's crust.Many developing countries rely on the mining of their natural resources to keep their economies afloat. Mineral exploration and exploitation, particularly of metalliferous deposits, is critical for many developing countries. Finding new mineral deposits, particularly metalliferous resources, will thus be beneficial to a country's economic development. In turn, reliable geo-information in the form of geological and mineral prospecting maps is critical for mineral resource exploration and development. However, geological and mineral exploration methods necessitate large sums of money, a long period, and a lot of human work, especially in difficult-to-reach places. When compared to multispectral remote sensing, hyperspectral (Hyperion EO-1) remote sensing has a greater number of bands. It is possible to apply the vast quantity of spectrum information to a variety of applications such as monitoring, agriculture,

pollution, landuse / landcover, soil and water quality monitoring, mineral identification, food quality monitoring, and so on. L. Zhang and B. Du (2012). A mineral is a natural substance with a chemical formula that is frequently solid, inorganic, and has a crystal structure. The International Mineralogical Association (IMA) has accepted 5,070 minerals out of 5,300 known minerals. Schneider, S., Murphy, R. J., and Melkumyan, A. (2014). Aluminium phosphates and sulphates of the alunite super group (APS minerals) are found in a variety of formation settings including metamorphic, igneous, and sedimentary worlds. Alunite is a mineral that forms when acidic, typically ore-bearing, solutions modify orthoclase feldspar-rich rocks. H. G. Dill (2001). However, even if geology or ground truth information is inadequate, mineral discovery or research is achievable with the aid of remote sensing. As a result, it would be a strong instrument for cost-effective mineral examination, which would substantially aid in the improvement of the country's economy. Geologists and others must prospect for mineral resources in remote places. R. Gore, A. Mishra, and R. Deshmukh (2020). Figure 1 depicts the mineral alunite and its field spectrum. To process the hyperspectral data, the following steps are taken: elimination of poor bands, removal of vertical strips in pictures, radiometric calibration, FLAASH atmospheric adjustment, minimal noise percentage, and pixel quality index. Finally, the EO Hyperion data was classified using the Spectral Angle Mapper (SAM) classification method.

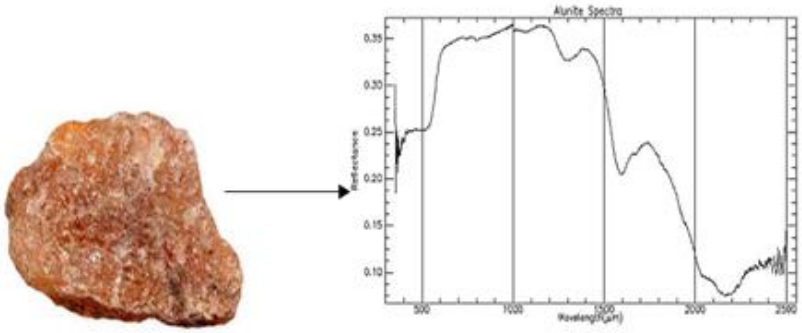


FIGURE. 1. THE SPECTRAL PATTERN OF ALUNITE MINERAL

II. STUDY AREA

Aurangabad District is one of the 36 districts of the state of Maharashtra in western India. In Aurangabad district mineral mapping report is not mentioned as government contribute mineral mapping report in India in general The most significant metallic and non-metallic minerals found in the Aurangabad district, such as Alunite, iron ore, and clay, are used in a variety of industries.

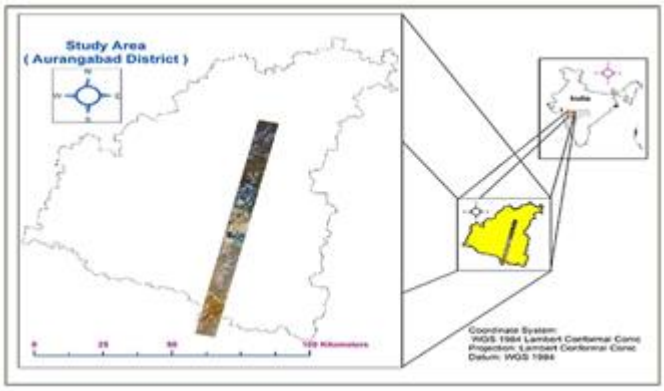


FIGURE. 2. THE RESEARCH STUDY AREA GEOLOGICAL POSITION.

A. Geological Information

The Aurangabad District, which is located on the Deccan plateau, is surrounded by the Deccan Traps, which formed during the Late Cretaceous and Lower Eocene periods. Thin alluvial deposits above the Deccan Traps run parallel to the main rivers. The basaltic lava flows of the Deccan Traps are the district's sole significant geological formation. The lava flows are horizontal, with each flow consisting of two layers. The top layer is made up of vesicular and amygdule zeolitic basalt, whereas the lower layer is made up of massive basalt Mahoney, J. J. (1988).

B. Hyperion (EO-1)

Data is utilised to identify the Alunite mineral in the present research Hyperion (EO-1). Hyperion (EO-1) is a US spacecraft with 242 spectral bands ranging from 0.4 to 2.5m, calibrated at 10nm intervals, and calibrated in 16-bit radiometric resolution. The width of the swath is 7.2km, and the height is 705km. It has a spatial resolution of 30m and a revisit period of 16 days. E. M. Middleton et al (2013). Imagery from the Hyperion (EO-1) scanner requires suitable preprocessing processes such as poor band removal, ertical strip removal, converting DN data to radiance values, atmospheric adjustment such as FLAASH, QUAC, and so on. M. Vigneshkumar and K. Yarakkula (2017). The metadata information for the hyperspectral data is shown in Table 1. The Hyperion (EO-1) visible and VNIR area (0.4 – 1.2m) from band 1 to band 70, which is mostly utilised for vegetation mapping. Hyperion (EO-1) SWIR (1.2-2.5m) from band 71 to band 224. Due to the lack of illumination and sensor overlap, only 198 of the 242 bands have been calibrated Upadhyay, M. R. (2013). The geological position of the research region is depicted in Figure 2.

TABLE I. DOWNDOADED HYPERION (EO-I) DATA METAFILE INFORMATION

Data Set Attribute	Attribute Value
Entity ID	EO1H1460462015358110Kv
Acquisition Data	2015-12-24
Reference_Datum	WGS84
Scene Start Time	2015 358 03:42:21
Scene Stop Time	2015 358 03:46:40
SUN_AZIMUTH	130.250063
Satellite Inclination	26.048956
SENSOR_LOOK_ANGLE	7.8141
IMAGE_UL_CORNER_LAT	20.311958
IMAGE_UL_CORNER_LON	75.405204
IMAGE_UR_CORNER_LAT	20.298772
IMAGE_UR_CORNER_LON	75.475783
IMAGE_LL_CORNER_LAT	19.393001
IMAGE_LL_CORNER_LON	75.193376
IMAGE_LR_CORNER_LAT	19.379903
IMAGE_LR_CORNER_LON	75.263570
PRODUCT_UL_CORNER_LAT	20.315440
PRODUCT_UL_CORNER_LON	75.190621

PRODUCT_UR_CORNER_LAT	20.314891
PRODUCT_UR_CORNER_LON	75.477985
PRODUCT_LL_CORNER_LAT	19.377421
PRODUCT_LL_CORNER_LON	75.189505
PRODUCT_LR_CORNER_LAT	19.376899
PRODUCT_LR_CORNER_LON	75.475186

III. METHODOLOGY

Several preprocessing procedures are necessary to categorise the hyperspectral data. Figure 3 depicts the detailed methods used to analyse the Hyperion (EO-1) data.

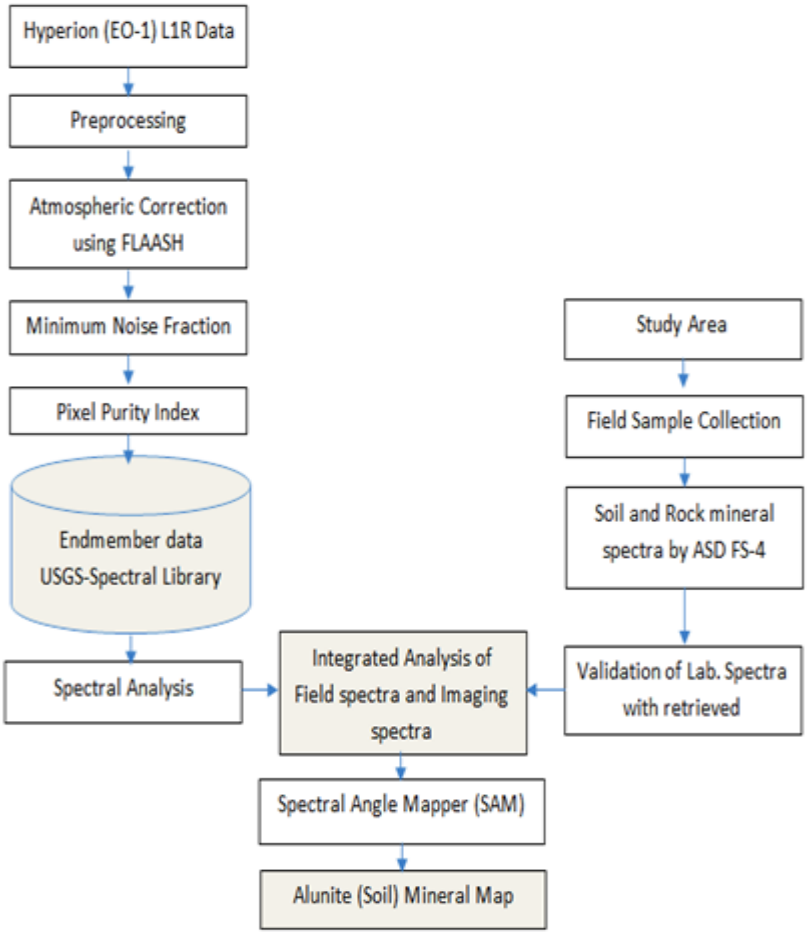


FIGURE. 3. ALUNITE SOIL MINERAL MAPPING METHODOLOGY

A. Remove the zero bands and bad bands

The Hyperion (EO-1) image comprises pixels with no information, which are referred to as zero bands. They may be found in bands 1-7, 58-76, and 225-242. M. R. Upadhyay (2013). In the spectral area, bad bands have a lot of noise and water vapour. It varies depending on the location and scanning time for each image. F. Van Der Meer (2004).

B. Remove the vertical stripe in the imagery

The number of vertical strips in a push-broom scanner's column. The raw image has numerous dark and bright columns due to a change in calibration or the failure of some detectors in the CCD display at the time of imprisoning the image. Check for column dropout or band issues before applying atmospheric adjustments. The terrible columns are substituted by averaging the preceding and next columns. M. K. Pal and A. Porwal (2015). To remove the strips in this study, a local destriping method is utilised.

$$\sum_{j=1}^{n} \frac{(x_{i-1,j,k}) + (x_{j+1,j,k})}{2n} \qquad 1$$

The equation 1 shows the local destriping algorithm.

C. Radiometric Calibration

The amount of light energy measured by the sensor from the item being viewed is referred to as radiance. C. Arellano, C. Wyatt (2012). When distributing remote sensing data, radiometric calibration is employed. It comprises adjustments for the distant sensor's sensitivity, topography and sun angle, as well as air scattering and absorption. It is most often used to transform a digital number to a radiance value for each pixel. It is available in three different formats: BIL, BSQ, and BIP.

D. Fast Line of sight Atmospheric Analysis of Hypercube (FLAASH)

FLAASH corrects wavelengths in the VNIR and SWIR ranges up to 3m. FLAASH has features such as adjacency correction to calculate a scene-average visibility, cirrus and opaque cloud map, and modifiable spectral shine for artefact suppression. H. G. Solutions (2017).

E. Minimum noise fraction (MNF)

To minimise the complexity of hyperspectral data, MNF was developed as an alternative to principle component analysis. It is distinguished by a two-pace cascaded PCA. The first stage is to use a probable noise covariance matrix to decorrelate and rescale the data noise; it has item discrepancy and no band-to-band correlations. In the second pace, a standard PCA of noise-whitened data is employedIt splits the data space into two sections: big Eigen Values and rational Eigen pictures, and small Eigen Values and noise-conquered images. In further processing, the noise is removed from the data by employing just the logical sections, therefore humanising the spectrum processing effects. B. Datt (2003).

F. Pixel Purity Index (PPI)

Vigneshkumar, M., and Yarakkula, K. manipulate the pixel purity index algorithm for each pixel in the picture cube by randomly generating appearance in the N-dimensional, a distributed scheme of the MNF converted information (2017). Total points in the space are now divided into lines, and those that go down at the lines' extremities are computed. Individual pixels that count above a certain threshold are labelled "pure" after repeated projections to different lines.

G. Spectral Analysis

The categorization of materials based on their spectral distinctiveness is aided by spectral analysis. To rank the equivalent of an image spectrum to the minerals in a spectral library, the spectral analysis utilises a number of

approaches, including binary encoding, spectral angle mapping, and spectral feature fitting. M. Vigneshkumar and K. Yarakkula (2017).

H. Spectral Angle Mapper

SAM computes the angular distance in n dimensions between an image's reflection spectrum and the mineral spectral. The categorised picture gives the best SAM match at each pixel for each end member based on the angular distance in radians between the image spectrum and the reference spectrum. The spectral angles with fewer spectral angles are represented by darker pixels, and the spectra are parallel to the reference spectrum. By changing the thresholds used to choose the pixels in the SAM image, the rule images may be utilised for classification. M. R. Upadhyay (2013).

IV. RESULT AND DISCUSSION

A. Removing the bad bands from Hyperion (EO-1) data

The Hyperion (EO-1) data set has 242 bands, 120 of which are calibrated; the other bands are affected by noise, non-illuminated, and water vapour. The list of underused and poor bands of the Hyperion (EO-1) sensor is shown in Table 2. Figure 4 clearly depicts the overlap zone of zero bands. Figure 5 depicts the spectral profile plot after the zero bands and overlap region have been removed. Figures 5 and 5 demonstrate the effect of eliminating problematic bands from the spectral profile plot.

TABLE II. FOR SUBSET DATA THE PARAMETERS FOR FLAASH ARE:

Parameter	Characteristics	Remarks
Latitude		Central Latitude
Longitude		Central Longitude
Sensor Type	Hyperion (EO-1)	Hyper Spectral Sensor
Ground Elevation	0.38km / 380m	220m for the Subset Area
Pixel Size	30m	Spatial Resolution of Hyperion (EO-1) Sensor is 30M.
Flight Date	29/09/2015	Date of Acquisition
Flight Time	03:42:21	Average of the Start time and end time.
Atmospheric Model	Mid-Latitude Summer	Depending upon the latitude and the surface temperature of the area the atmospheric model is chosen. It is Mid-Latitude Summer for the Subset Data
Aerosol Model	Near to Urban	Since Subset is an urban + rural area
Water retrieval	Yes	This method is used for retrieving the water amount for each pixel
Water Absorption	1135m	In the Hyperion (EO-1) data of subset data the bandwidth of band 99 ranges from 1134-3796
Initial visibility	40	Because the data was captured in the month of nova and hence the data has naze
Aerosol Retrieval	None (Since the initial visibility is	This method is used for retrieving the aerosol amount and estimating a scene average visibility

	40)	
Spectral polishing	Yes	Spectral polishing done to get smooth reflectance curves.
Wavelength Calibration	No	This method is use for Identifying and correcting wavelength, miscallibaration hyperon sensor are automatically supported for wavelength recalibration.

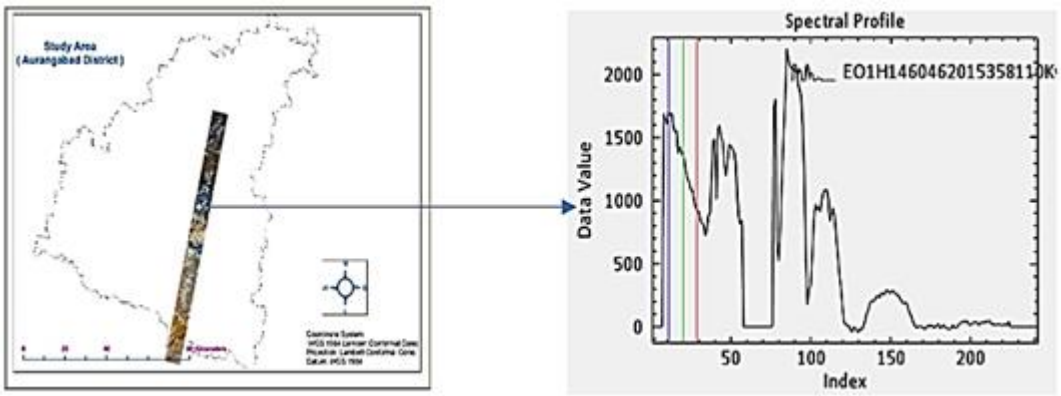


FIGURE. 4. PRIOR TO THE REMOVAL OF THE BAND BANDS AND THE SPECTRAL PLOT

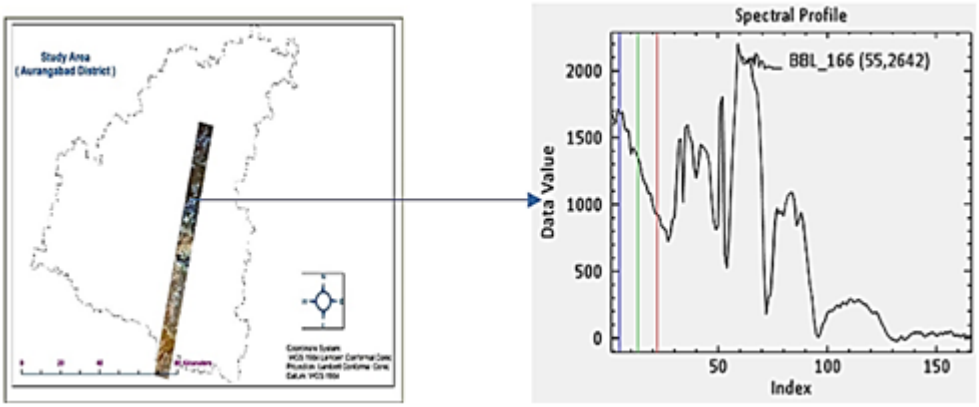


FIGURE. 5. AFTER REMOVING THE BAD BANDS AND ITS SPECTRAL PLOT

B. Destriping

Local destriping techniques are used to eliminate the vertical stripes. They are highly suggested for vertical stripe removal since they only affect the strip column layer. The vertical strips removed procedure improves the connection between reflection spectra and mineral spectra and aids in mineral classification formulation precision. Pour, A. B., and M. Hashim (2014). Table 3 displays the availability of vertical strips in the images column. Figure 6 depicts the spectral profile plot and visualisation variation after the vertical strips have been removed.

TABLE III. LIST OF VERTICAL STRIPS IN HYPERION (EO-1) IMAGERY

Sr. No.	Bands Number	Column Numbers	Sr. No.	Bands Number	Column Number
1	8,9	6,68,114,245	9	118	145

2	10,11	6,68,114	10	135	60
3	12	6	11	158	18
4	28,29	47	12	162	103
5	87,88	54	13	168	117
6	94	92	14	198	117
7	99	91	15	202	182
8	116	137	16	201	7

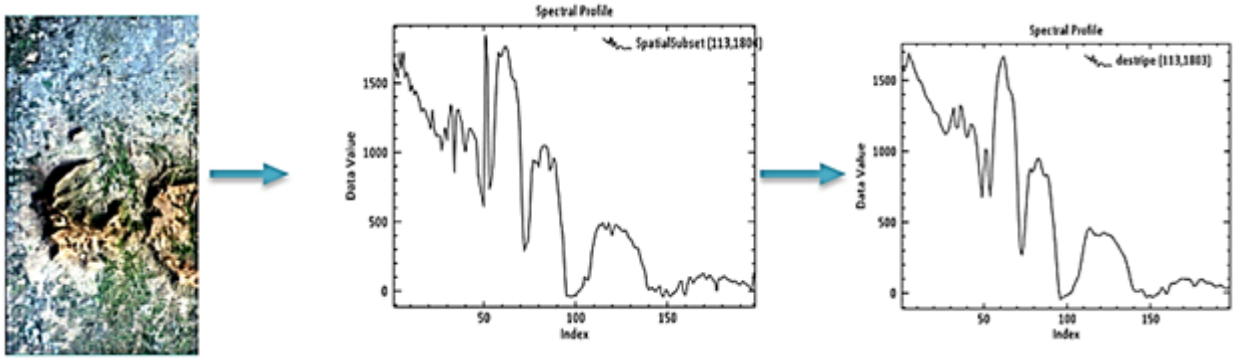


FIGURE. 6. EFFECT OF DESTRIPING IN VISUAL INTERPRETATION AND ITS SPECTRAL PLOT

C. Radiometric calibration

To determine the radiance value of the earth's surface, the radiometric calibration uses the DN value of Hyperion (EO-1) data. The output file format is BIL, with a scale factor of 0.1. (Pixel Interleaved Band) It converts digital numbers from the Hyperion (EO-1) CCD into radiance values. C. Zhang (2014). Figure 7 depicts the radiance value as well as its spectral profile plot.

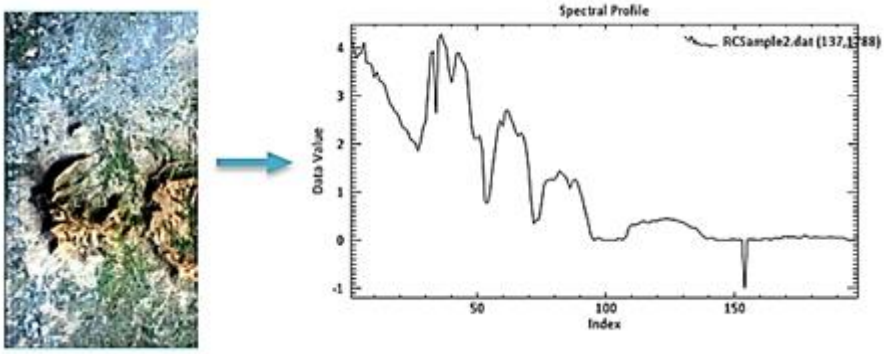


FIGURE. 7. RADIOMETRIC CALIBRATION AND ITS SPECTRAL PLOT

The FLAASH module is used to do atmospheric adjustment. FLAASH utilises sophisticated techniques to deal with the most difficult climatic circumstances, such as cloud cover. As an input image, FLAASH requires a radiometric calibrated radiance image in BIL format. Kumar, M. V., and K. Yarrakula's 4-byte signed numerals (2017). Figure 8 depicts the reflectance value and spectral profile plotted with the FLAASH module.

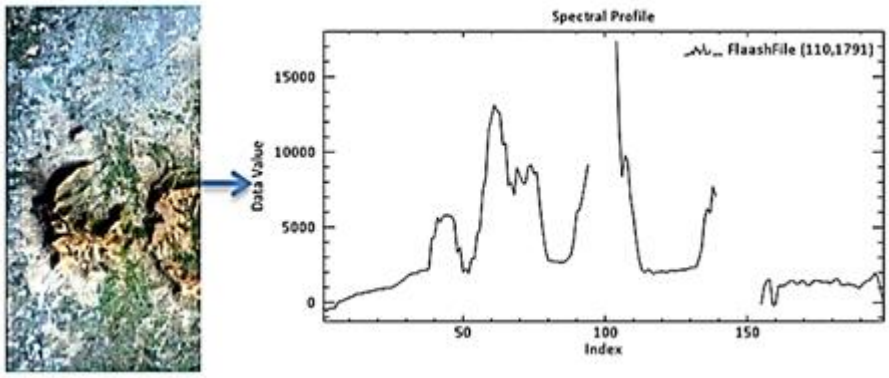


FIGURE. 8. FLAASH MODULE AND ITS SPECTRAL PLOT

D. Atmospheric correction module

The FLAASH module is used to do atmospheric adjustment. FLAASH utilises sophisticated techniques to deal with the most difficult climatic circumstances, such as cloud cover. As an input image, FLAASH requires a radiometric calibrated radiance image in BIL format. 4-byte signed numerals (2017). Figure 8 depicts the reflectance value and spectral profile plotted with the FLAASH module.

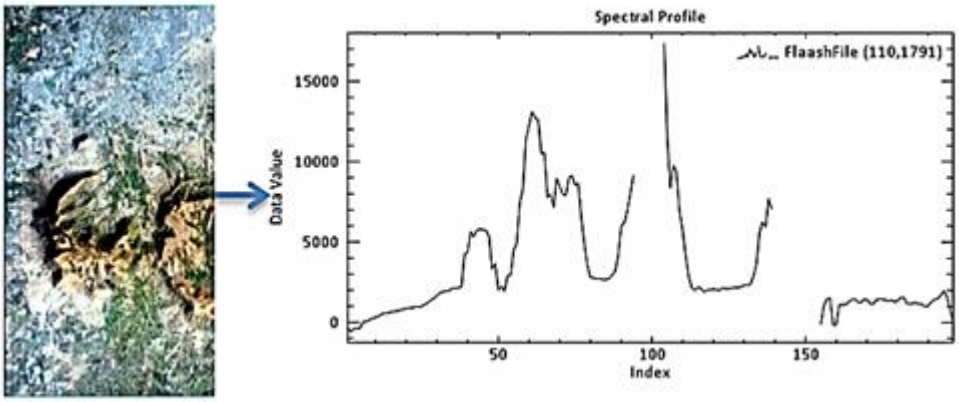
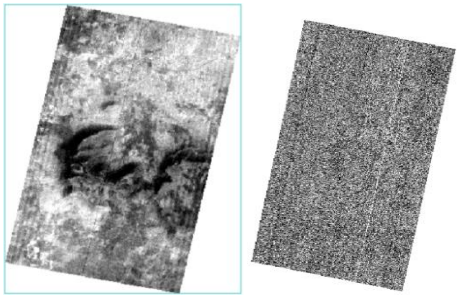


FIGURE. 9. FLAASH MODULE AND ITS SPECTRAL PLOT

E. Minimum Noise Fraction (MNF)

There is a lot of noise information in the reflectance bands of Hyperion (EO-1) imagery. The MNF transformation is a more advanced PCA algorithm. Depending on the amount of noise, MNF shortens the reflectance bands in ascending order. Kempeneers, P., et. al.(2004). Figure 9 clearly shows the large amount of noise present in the data and it affect the descending order bands. MNF takes only 9 bands in the region to process the Hyperion (EO-1) data.



Band 6 Band 15

F. Pixel Purity Index(PPI)

MNG's noiseless bands are used as the pixel purity index input. PPI processes the MNF bands in iterations ranging from 2.5 to 10000. In the PPI, impure and pure pixels are represented by black and white pixels, respectively, Upadhyay, M. R. (2013). Figure 10 depicts the image's pixel purity index.

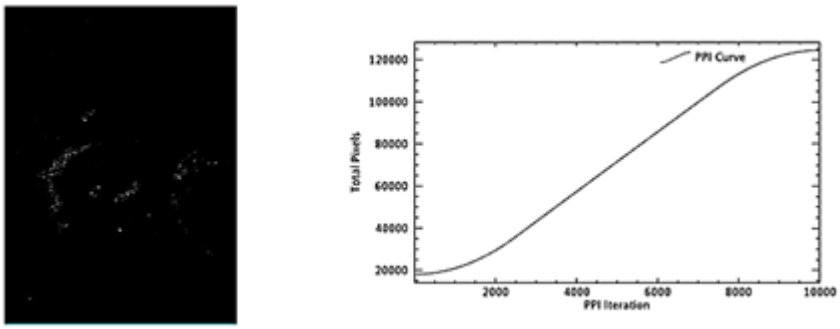


FIGURE. 10. PIXEL PURITY INDEX.

G. Spectral Analysis

The spectral libraries of the USGS and NASA were used to get the Alunite mineral spectra. These mineral spectra have a band interval of 2.5nm, whereas the Hyperion (EO-1) imaging spectra have a band interval of 10nm. Spectral Resembling techniques are used to transform library spectra data from 2.5nm to 10nm intervals. The spectral analyzer programme compares Alunite mineral spectra to picture spectra and provides probability estimates using methods such as SAM, SFF, and BE. In this study, Alunite mineral has a high probability of approximately 0.85 in the wavelength range between 2000nm and 2500nm.

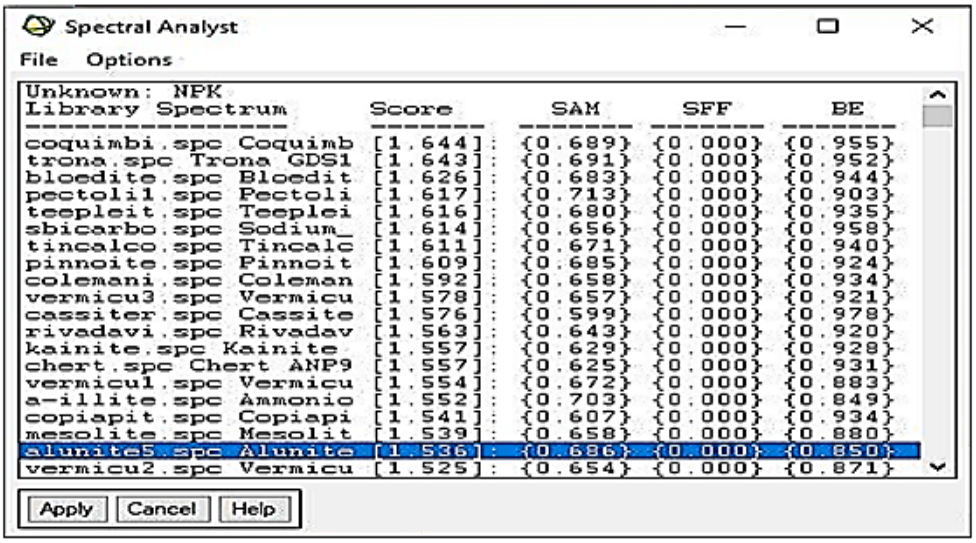


FIGURE. 11. ALUNITE MINERAL PROBABILITY

Figure 11 depicts the total likelihood score obtained when comparing picture spectra to mineral spectra. Figure 12 depicts the relationship between picture spectra and mineral spectra. The white line represents the mineral spectrum of the endmember. The picture spectra were represented by the red line.

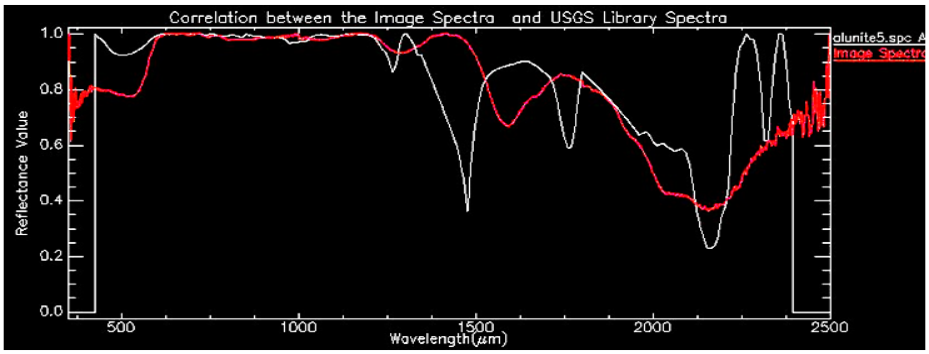


FIGURE. 12. IMAGE SPECTRA AND LIBRARY SPECTRA ARE CORRELATED.

H. Spectral Angle Mapper

In the spectral angle mapper technique, the image spectrum and Alunite spectra are compared. The bands in the SWIR area extend from 1900nm to 2400nm. The angle between the picture and the endmember mineral spectra is 0.25 degrees. The existence of the Alunite mineral in the earth's topography is shown by the red pixels in the SAM result. In Figure 13, the Alunite material is classified using SAM. The dark pixels represent other earth surface things that inhabit the region. In the Aurangabad district.

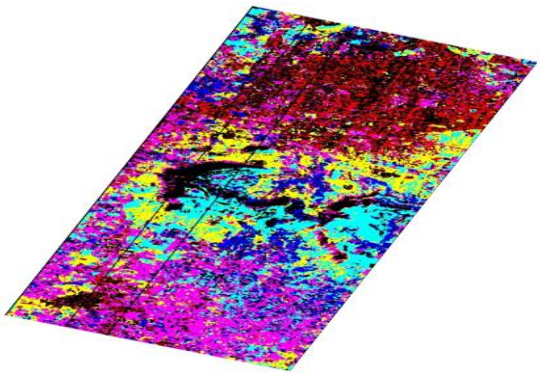


FIGURE. 13. ALUNITE MINERAL IDENTIFICATION USING THE SPECTRAL ANGLE MAPPER

V. CONCLUSION

The goal of this research was to see if Hyperion (EO-1) data could be used to quantify and map the mineral potential zone. It analyses hyperspectral data and compares the results to the research area's field spectra and geological map. It demonstrates how the Hyperion data can be used to map geological properties and detect mineral abundance.

Hyperion imaging, on the other hand, has its own set of restrictions, including a low signal-to-noise ratio, the appearance of apparent strips in multiple bands, and limited spectral special resolution.

Based on past information about the area, a logical method of Hyperspectral remote sensing was use. It was successful in emphasizing the value of the mineral Alunite. The Spectral Angle Mapper method was use to map these targeted minerals using Hyperion data.

The spectra were matched using the composite score of SAM, SFF, and BE in this investigation. SAM was used to classify the minerals that scored well (>1.5). It has a strong correlation with the data collected in the field. The position, strength, and shape of the absorption feature of spectral curves were use to identify individual

mineral species. Only the absorption characteristic in each spectrum is attempted to be match by the spectral curve matching approach. Fieldspec4 field sample is required for further verification.

VI. REFERENCES

[1]. Datt, B., McVicar, T. R., Van Niel, T. G., Jupp, D. L., & Pearlman, J. S. (2003). Preprocessing EO-1 Hyperion hyperspectral data to support the application of agricultural indexes. IEEE Transactions on Geoscience and Remote Sensing, 41(6), 1246-1259.

[2]. Dill, H. G. (2001). The geology of aluminium phosphates and sulphates of the alunite group minerals: a review. Earth-Science Reviews, 53(1-2), 35-93.

[3]. Gore, R., Mishra, A., & Deshmukh, R. (2020). Mineral Mapping at Lonar Crater Using Remote Sensing. Journal of Scientific Research, 64(2).

[4]. Kumar, M. V., & Yarrakula, K. (2017). Comparison of efficient techniques of hyper-spectral image preprocessing for mineralogy and vegetation studies.

[5]. Kempeneers, P., Deronde, B., Bertels, L., Debruyn, W., De Backer, S., & Scheunders, P. (2004, September). Classifying hyperspectral airborne imagery for vegetation survey along coastlines. In IGARSS 2004. 2004 IEEE International Geoscience and Remote Sensing Symposium (Vol. 2, pp. 1475-1478). IEEE.

[6]. Kokaly, R. F., Clark, R. N., Swayze, G. A., Livo, K. E., Hoefen, T. M., Pearson, N. C., ... & Klein, A. J. (2017). USGS spectral library version 7 (No. 1035). US Geological Survey.

[7]. Mahoney, J. J. (1988). Deccan traps. In Continental flood basalts (pp. 151-194). Springer, Dordrecht.

[8]. Middleton, E. M., Ungar, S. G., Mandl, D. J., Ong, L., Frye, S. W., Campbell, P. E., ... & Pollack, N. H. (2013). The earth observing one (EO-1) satellite mission: Over a decade in space. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 6(2), 243-256.

[9]. Pal, M. K., & Porwal, A. (2015, July). Destriping of Hyperion images using low-pass-filter and local-brightness-normalization. In 2015 IEEE International Geoscience and Remote Sensing Symposium (IGARSS) (pp. 3509-3512). IEEE.

[10]. Pour, A. B., & Hashim, M. (2014). ASTER, ALI and Hyperion sensors data for lithological mapping and ore minerals exploration. SpringerPlus, 3(1), 1-19.

[11]. Schneider, S., Murphy, R. J., & Melkumyan, A. (2014). Evaluating the performance of a new classifier–the GP-OAD: A comparison with existing methods for classifying rock type and mineralogy from hyperspectral imagery. ISPRS journal of photogrammetry and remote sensing, 98, 145-156.

[12]. Solutions, H. G. (2017). Fast line-of-sight atmospheric analysis of hypercubes (flaash). Accessed: Dec.

[13]. Upadhyay, M. R. (2013). Indian Space Research Organisation Department of Space Government of India Dehradun–248001 (Doctoral dissertation, Indian Institute of Remote Sensing).

[14]. Van Der Meer, F. (2004). Analysis of spectral absorption features in hyperspectral imagery. International journal of applied earth observation and geoinformation, 5(1), 55-68.

[15]. Vigneshkumar, M., & Yarakkula, K. (2017, November). Nontronite mineral identification in nilgiri hills of tamil nadu using hyperspectral remote sensing. In IOP Conference Series: Materials Science and Engineering (Vol. 263, No. 3, p. 032001). IOP Publishing.

[16]. Wyatt, C. (2012). Radiometric calibration: theory and methods. Elsevier.

[17]. Zhang, L., & Du, B. (2012). Recent advances in hyperspectral image processing. Geo-spatial Information Science, 15(3), 143-156.

[18]. Zhang, C. (2014). Combining hyperspectral and LiDAR data for vegetation mapping in the Florida Everglades. Photogrammetric Engineering & Remote Sensing, 80(8), 733-743.

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association withInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

A Survey of Webpage Template Detection Techniques

Tanveer I. Bagban[1], Dattatraya V. Kodavade[1], Prakash J. Kulkarni[2], Sandeep A. Thorat[2]
[1]Department of Computer Science and Engineering, D.K.T.E'S Textile and Engineering Institute, Ichalkaranji, Maharashtra, India
[2]Department of Computer Science and Engineering, Rajarambapu Institute of Technology, Islampur, Maharashtra, India

ABSTRACT
The World Wide Web has become a major source of knowledge in today's digital era. Web templates are increasingly being utilized to build visually appealing and properly formatted webpages. Web-based search engines are increasingly used by users to deliver accurate search results on a variety of topics of interest. Search engines, on the other hand, scan through the large online archive in search of data required for the given query. The inclusion of these templates, on the other hand, has the potential to skew search results and offer incorrect information to users. As a result, identifying and removing web templates from the webpages is critical to improving the accuracy and reliability of search results. Template detection and extraction can be applied across homogenous as well as heterogeneous web pages. The survey paper investigates various methodologies to detect and extract the templates from the webpages. The contribution of the paper is to present state of the art techniques in template detection and extraction and presents comparative analysis of various methods along different parameters.

Keywords—webpage, template, homogeneous, clustering, heterogeneous.

I. INTRODUCTION

The World Wide Web (WWW) has established itself as the major repository for publicly accessible information. Due to its ability to properly format and structurally represent the information, it is widely in use for information publishing on the web. A Significant number of web documents on the web are designed using Content Management Systems (CMS), and are generated using templates. A Template is a framework document which is filled with web data to create the final web document.

Web Templates are common contents or formats that appear in many web documents of a web site. Significant number of web pages on the web has template components to some extent. Some of the template components are navigation sidebar links on the left or right side of the page; corporate logos, background colors and styles; dropdown menus along the top having links to information about products, links to locations, and contact

information; link to advertisements; and copyright information. The usage of templates in web pages helps particularly in navigation, presentation, and branding.

There are multiple reasons for using templates in web documents. One is due to web site design software that enables a user to manage web sites, helping him to edit and apply templates to set of pages. Second, it is used to design personal home pages in which the owner can duplicate the same portion of HTML from page to the other to provide a similar look and feel. Other includes dynamically generated pages in which contents are wrapped into a template.

According to [1] template constitutes 40-50% portion of a typical web page and is further increasing. Over the past decade, the usage of template has doubled. Different types of web sites have different usage of templates. While media sites make heavy use of templates, catalog sites have 60% or more of their content as templates. Figure 1 and Figure 2 highlight two webpages from amazon website both sharing same template but their contents show two different headphones details. It is clearly visible that two webpages are generated from same template as they share same menu, right side frame and the format in which headphone details are presented.

Templates, though it is used in web design, they negatively impact in the information retrieval process. First, the template words affect relevant information by their irrelevant contents. Second, distribution of links in web documents is skewed by the presence of duplicated links in templates hence reducing precision. In web content mining, web templates need to be removed before unstructured web contents are extracted and mined. Cleaning of the web documents before web content mining becomes necessary for improving web mining results. This pre-processing step is called as web page cleaning. Hence template identification and removal improve web content mining results

The contribution of the paper is to present various state of the art methods available in the literature of template detection. The paper highlights comparative analysis of various methods along the parameters like scope of input, output generated, features used, techniques used and complexity of methods.

The paper is organized as follows: Section 2 gives classification account of various template detection techniques, Section 3 presents various states of the art methods available in template detection, Section 4 gives comparative analysis of various methods discussed in Section 3 and Section 5 focuses on conclusive remarks.

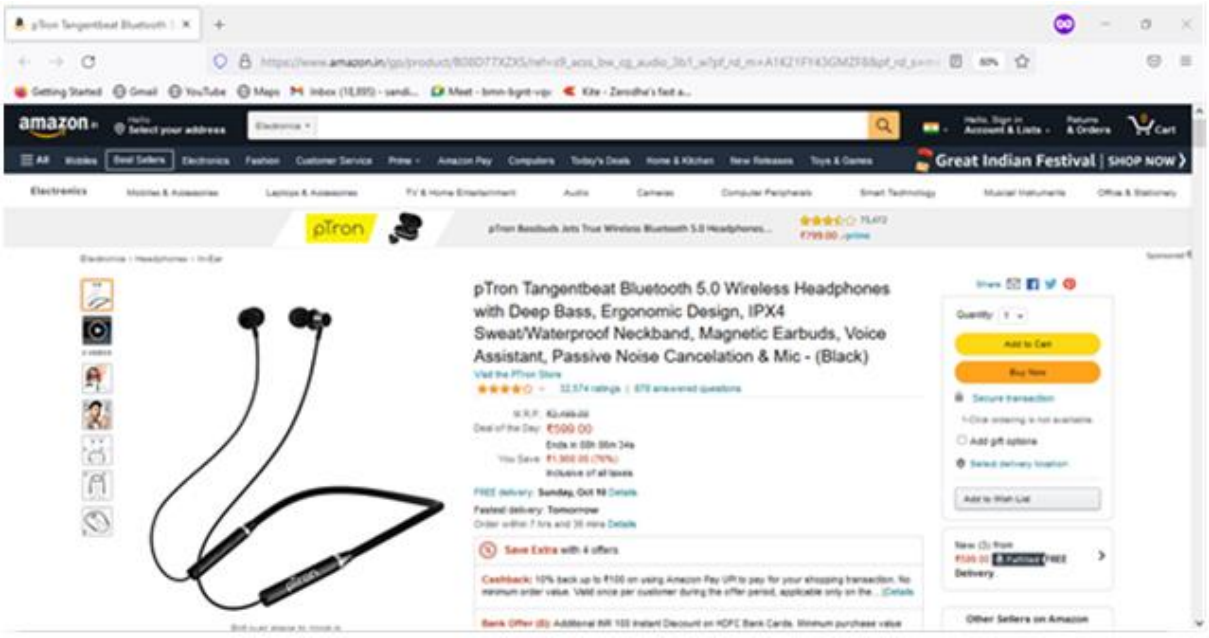


Fig. 1 Sample Template generated Web Page

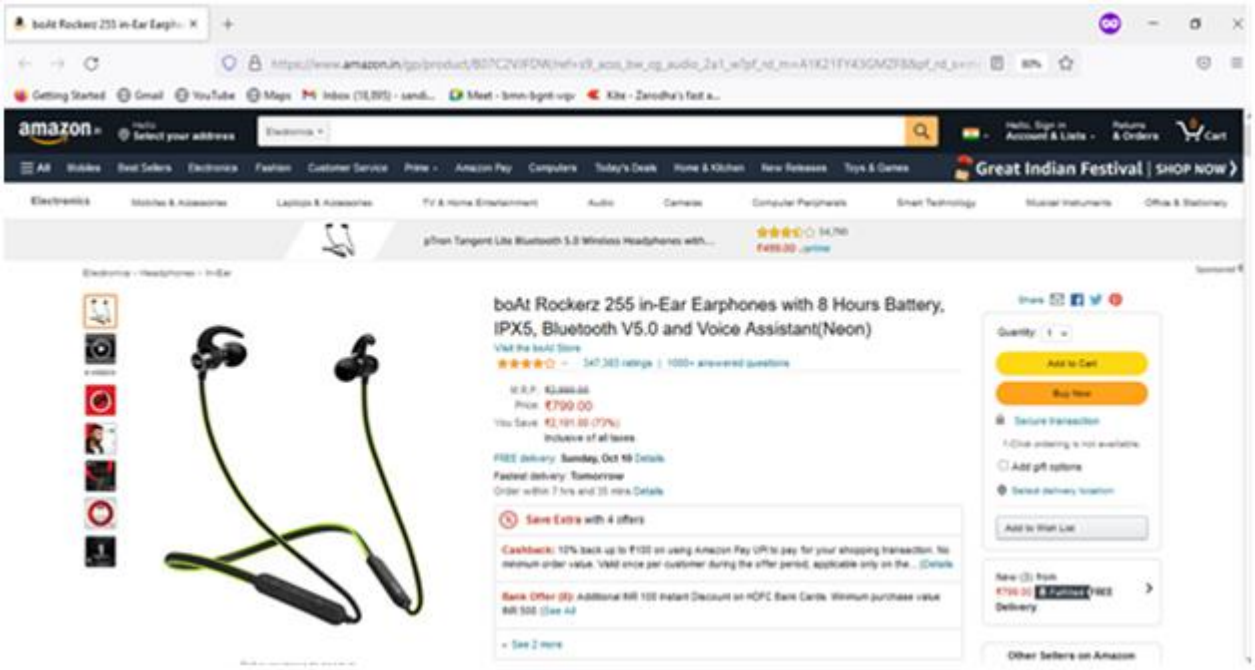


Fig. 2 Sample Template generated Web Page

II. CLASSIFICATION OF TEMPLATE DETECTION TECHNIQUES

This section presents classification of different template detection techniques. Template detection approaches are categorized into four types as follows:

A. Template Detection from Homogeneous Webpages

Homogeneous webpages are those that are generated from the same template. All approaches for detecting and extracting templates from homogenous webpages require that the set of input webpages be generated from the same template, i.e. they all share the same template. Large number of methods belongs to this category. The merit of these methods is that they are relatively less complex. They require relatively less number of features and require less number of sample webpages for training and testing. The demerit of these methods is that they are applicable to only those webpages which are generated from same templates hence they are not scalable and widely applicable to wide variety of webpages.

B. Template Detection from Heterogeneous Webpages

Heterogeneous webpages are those that are generated from different templates. When detecting and extracting template from heterogeneous webpages, it is necessary to use a collection of input web pages that are not all generated from the same template, which means that the templates on each page may be different. The methods falling under this category are less in numbers. Clustering techniques are mostly used to detect template in these methods. The merit of these methods is that they are applicable to wide variety of webpages within same website and also in other websites. Hence their scope of input webpages is more. The demerit of these methods is that they are complex in nature. They require good feature selection techniques to select optimum number of features from the large number of features. Their feature selection and clustering complexity is quadratic in nature.

C. Web-Site level Template Detection

This technique detects templates from only the webpages that belong to a single website, not from all webpages. The methods falling under this category are less in numbers. The merit of these methods is that they are having relatively less complexity as it may be domain specific. Due to their domain specific nature they require less number of features. Their demerit is that it is applicable to only webpages of the given website. They are domain specific e.g. Detection of templates in news webpages of given news website.

D. Web Scale level Template Detection

This technique detects templates on a given set of webpages belonging to any website. A very few methods belong to this category. These methods require input as the set of webpages belonging to different websites and may be having different templates. The merit of these webpages is that they are applicable to webpages which are from different websites and from different domains. The demerit of these methods is that they are complex in nature. They require good feature selection techniques to select optimum number of features from the large number of features. Their feature selection and clustering complexity is quadratic in nature.

III. TEMPLATE DETECTION METHODS

Bar-Yossef and Rajagopalan [2] presented ground-breaking work on the detection of the webpage's template portion. It is a method for finding templates at the web site level that focuses on detecting templates from a collection of homogeneous pages. They refer to pagelets as templates. A pagelet is a sub-section of a webpage that serves a specific purpose, such as displaying a menu, advertising, or a user comment. They visualize a webpage using a DOM tree. The strategy builds distinct segments of a webpage's DOM tree and then picks segments from the DOM tree; the frequently repeated segments are identified as pagelets. Segments are the characteristic features of this technique. It calculates the frequency of segments across webpages in order to classify it as a pagelet. The complexity associated with determining the pagelet is quadratic. This method proposes two distinct algorithms: the Local Template Detection Algorithm and the Global Template Detection Algorithm. The approach for detecting local templates works well with small input sets. The approach for detecting global templates is scalable to large input sets. Due to the fact that it requires segmenting and detecting pagelets within the DOM tree, its complexity is quadratic and thus not scalable.

Lin and Ho[3] developed, InfoDiscoverer, on the premise that content generated from templates appears more frequently, i.e. the frequency of information contained within the template is greater than the frequency of information contained inside the actual contents. This technique falls under the topic of web-site-level template detection and is therefore limited to homogeneous webpages. To find the most frequently used information, the webpages in a set of training web pages are separated into content blocks. The process begins by segmenting a page into various content blocks based on the HTML tags contained inside a Web page. It determines the entropy value of each feature (term) based on their occurrence in the set of pages. The entropy value of a content block is defined by the entropy value of each feature within the block. It presents a method for dynamically selecting the entropy threshold that divides blocks into informative or redundant blocks by examining the information measure. While informative information blocks are distinct components of the page, redundant content blocks are common components. Extraction of block features is quadratic in complexity in relation to the number of features on a webpage. The complexity of computing feature entropy and block

entropy is also given as quadratic in terms of the number of features on a webpage, suggesting that it is not scalable. Another shortcoming of the approach is that it is limited to the processing of the Table tag within an HTML document. This strategy assumes that all of a website's pages are generated from the same template, referred to as homogenous webpages. It is only applicable to websites with homogeneous webpages.

Debnath et al. [4] implemented the concept of redundant blocks in conjunction with words, text, and images. This technique falls under the category of web-site-level template detection and also limited to homogeneous webpages. The algorithms are designed to work with web pages that share a common underlying template structure. The method takes as input a collection of homogeneous web pages and outputs content blocks. The difference between content and non-content blocks is determined by a quantity called block document frequency, which is the frequency with which blocks appear in documents. If it occurs frequently, it is classified as a non-content block or template block. Based on heuristics, the algorithms divide the webpage into blocks. It does not just look for table tags; it looks at all tags on a page to detect the presence of a template. It requires no manual input. This technique separates relevant data from non-contents or templates and then extracts the contents. Without human interaction, the extraction is carried out automatically. The technique presents two algorithms for extracting content blocks, called ContentExtractor and FeatureExtractor. The ContentExtractor algorithm makes a distinction between content and non-content blocks based on the repetition of identical blocks across multiple pages. The Content Extractor retrieves content blocks using the Inverse Block Document Frequency idea. Because the complexity of ContentExtractor is quadratic in terms of the number of blocks and webpages, this solution is also not scalable at webscale. The FeatureExtractor algorithm extracts data from externally supplied features. It is invoked to find blocks that contain a specified set of required features among the set of chosen blocks, to rearrange the blocks according to their probability values, and to select the winner block as the content block.

Yi et al.[5] implemented a Site Style Tree-based approach but focused more on visual considerations. This technique falls under the topic of web-site-level template detection and also limited to homogeneous webpages. They identified a template as a noisy part of a webpage. The technique identifies noisy portions on webpages. The technique is based on the observation that blocks containing noisy data will share some data and presentation styles, whilst blocks having true data will have distinct data and presentation styles. The technique accepts a collection of webpages in order to create a structure known as a Site Style Tree (SST). It summarizes the presentation styles and contents of all of the webpages. The possibility of SST nodes being considered noisy nodes is governed by the range of presentation styles and their content. The SST is constructed by evaluating a collection of DOM trees and identifying nodes that are repeated. Thus, the SST serves as a compressed representation of the DOM Trees collection. The nodes that appear frequently on the webpages are more likely to be noisy and are eliminated. Their work is limited to homogenous webpages built using the same template, and the method is only applicable to the webpages of a single website. As a result, it is unsuitable with processing web pages created using a variety of various templates and websites. Additionally, the complexity of developing SST is quadratic, which explains why it is ineffective at the Web scale.

Crescenzi et al. [6] developed the technique on the premise that webpages created from same template share a common structure. This approach belongs to the category of web-site level template detection but supports heterogeneous webpages. The approach clusters webpages belonging to single website only. They proposed a model that considers structural features of webpages. It models webpages in the form of collections of tree links and clusters webpages with a similar link structure based on principle of the Minimum Descriptive Length

(MDL) and the webpages similarity is measured with respect to features of the links collection. While just crawling a small area of the web, the algorithm creates clusters of pages with a uniform structure. The algorithm begins with a single page in the first cluster, such as the main page, and then recursively explores the outbound links to form additional clusters. The technique takes advantage of link collections' features to reduce the number of pages it has to fetch. Pages that may be accessed by a similar set of links are referred to as being in a single cluster. The complexity to evaluate the model using MDL principle is quadratic. The disadvantage of this method is that it works for a specific website and cannot be applied across the website. The method doesn't deal with pages containing less structured data.

Reis et al. [7] developed a method for clustering based on tree edit distance. This technique falls under the domain of web-scale template detection and also works with heterogeneous webpages. The technique automatically extracts data from the web. The approach is primarily concerned with detecting and extracting data such as web news from various websites. Clustering is a technique for grouping webpages based on the Tree-edit distance between them. This concept is based on the similarity of the underlying structure of a collection of web pages for a particular website. Web pages having a similar structure are clustered together. The tree-edit distance is used to compare the structure of pages. The approach is primarily concerned with determining the least expensive mapping between the trees in question. This solution entails two primary tasks: collecting required pages using crawlers and extracting web news from the crawled webpages. The extraction method consists of four steps: (1) web page clustering (2) Pattern generation for extraction (3) Data matching (4) Data labeling. The first stage is to create clusters of pages using a technique called hierarchical clustering. Additionally, it employs a threshold value to determine whether or not two clusters can be merged. Finally, several clusters with webpages conforming to the same template structure will be generated. The following stage generates node extraction patterns, which are a special type of tree that accepts as input each page in the cluster. The following phase involves matching the node extraction patterns to the target pages and extracting their contents. The final step is to extract the required information, such as the title and body of the news, from the extracted contents in the previous phase. The method includes comparing the structure of pages to determine the distance between them, and then using agglomerative hierarchical clustering to merge the pages. The complexity of its page-to-page tree comparison and clustering approach is quadratic. This is not scalable for websites with a large number of pages. The disadvantage of the strategy is that it is domain-specific, meaning it is only applicable to news websites.

Kim and Shim [8] proposed template detection and extraction technique in which templates are detected and extracted from a set of heterogeneous web pages. This approach belongs to the category of web-scale level template detection and also supports heterogeneous webpages. Their main focus is on template extraction. They adopted clustering based approach to detect templates. In this technique the webpages are represented using DOM tree and DOM tree paths are extracted and modeled using Matrices. The DOM tree paths are said to be template paths if its frequency of occurrence is more within the webpage and across the webpages. Three different matrices are modeled before clustering. First is a template matrix which is a used to model template paths in each web document. Second is document matrix which is used to model documents in each cluster. Third is an essential path matrix which is used to model DOM tree paths which are likely to be the part of template in each web document in a given cluster. The approach is to extract all templates paths in the web documents of a cluster, the clusters of web documents are represented by product of template matrix and document matrix. Initial random data is assumed in template matrix and document matrix based on likelihood

of template paths in each document. The clusters obtained are evaluated using information theoretic based approach Minimum Descriptive Length (MDL).Different clustering models are obtained using template and document matrix. The evaluation of a clustering model is done by obtaining MDL value for each model. The clustering model is finalized whose MDL value is minimum. Since initial matrices such as template matrix and document matrix are generated based on random values, the time required to determine final cluster with a set of template paths in each of its document is quadratic to number of paths and number of documents hence it is not scalable at a web scale.

Grigalis and Cenys [9] approach is based on clustering of the webpages based on the information of URL links. This approach belongs to the category of web-scale level template detection and also supports heterogeneous webpages. All the web pages in a cluster obtained are supposed to be generated from a same template. In this the webpages are represented as DOM Tree. Their approach is based on the assumption that links from exactly the same location in a DOM Tree point to similar webpages i.e. Links on different webpages having same XPath location point to structurally similar webpages. After collecting the set of webpages to be clustered, a group of similar XPaths of a set of URL links in each of the web page are extracted and corresponding webpages are clustered. Further webpages in each cluster are refined based on their DOM tree paths similarity. This approach requires double clustering. Further second clustering is done by calculating the distance matrix is based on webpages DOM tree paths similarity whose complexity depends on number of DOM tree tags paths in each web page. The complexity is on order of number of paths for every web page hence it is not scalable at a web scale.

IV. COMPARISON OF TEMPLATE DETECTION METHODS

The following Table 1 compares many widely popular distinct template detection approaches that are available in the literature. The analysis is based on parameters such as the method's applicability as a Web-site-based or Web-scale-based technique, its support for homogeneous or heterogeneous webpages, the differences between the input and output, the features used as the basis for template detection, the major technique used, and the method's complexity. All of the approaches presented here have a precision and recall of greater than 90%. Their runtime complexity for feature preprocessing, as well as the techniques used to detect templates, is quadratic.

V. RESEARCH GAP IDENTIFICATION

A comprehensive review of the available literature in the domain of Template Detection from the given collection of webpages resulted in an understanding of the various approaches used for template detection in the given set of webpages. As a result of examining the methodologies, the following research gaps have been identified:

- The majority of approaches do not support sample input pages collected across the websites.
- The majority of approaches are effective when used with input pages that were generated using the same template.
- Some approaches necessitate building a model from training data set using a subset of a given website's sample pages, which can lead to an overfitting problem.

- The majority of approaches rely on threshold-based hierarchical clustering, which is quadratic in complexity, and hence is not scalable when the input is a huge collection of webpages.

VI. CONCLUSION AND FUTURE WORK

The survey paper has discussed various techniques for detecting templates from a given set of webpages. Some of the solutions described require inputs in the form of set webpages from the same website, while others accept inputs from different websites. Some strategies works on a homogeneous set of webpages, while others works on a heterogeneous set of webpages. Some methods generate extracted templates, while others produce clusters of webpages having the same templates. Still others produce data extracted from a given set of webpages. All of the techniques claim to have a high to extremely high level of accuracy when it comes to precision and recall, which is nearly 90% for a large set of webpages.

After analyzing the above- mentioned techniques, we conclude that the methods developed by Kim and Shim [8], Grigalis and Cenys [9] are superior for template detection because they support webpages at the web scale level, i.e. they are not limited to the same web-site, and they have the ability to process heterogeneous webpages.

Working on Template Detection in the future will open up the following research opportunities.

- Automated template removal for web content mining from a specified group of webpages.
- For comparative shopping, automate the integration of product details and prices from various E-Commerce webpages.
- Automated integration of genetic information and related data from many websites publishing genetic sequences in various formats.

VII. ACKNOWLEDGMENT

D.K.T.E'S Textile and Engineering Institute, Ichalkaranji supported the research for this study. We would like to give special thanks to the CSE Department of D.K.T.E'S Textile and Engineering Institute, Ichalkaranji for providing the necessary facilities for this research. We would like to acknowledge Prof. (Dr.) P. V. Kadole, Director of the institute for their assistance and support.

TABLE I COMPARISON OF TEMPLATE DETECTION METHODS

Method	Level	Support for Homogeneous / Heterogeneous webpages	Input	Output	Features	Technique	Complexity
Bar-Yossef &	Web -Site	Homogeneous	Webpages from same	Pagelets (Template	Webpage Segments	Segment Frequency	Quadratic

Rajagopalan, 2002			Web-site	section)			
Lin & Ho, 2002	Web-Site	Homogeneous	Webpages from same Web-site	Informative Block (Non Template part)	Table Tags of webpages	Feature Entropy and Block Entropy	Quadratic
Debnath et al., 2005	Web-Site	Homogeneous	Webpages from same Web-site	Content blocks (Non Template part)	All HTML Tags in a webpage	Inverse Block Document Frequency	Quadratic
Yi et al., 2003	Web-Site	Homogeneous	Single Webpage from a given Web-Site	Template removed Contents	Presentation styles in DOM Tree	Entropy based Noisy Nodes Determination	Quadratic
Crescenzi et al., 2005	Web-Site	Heterogeneous	Seed webpage in a Website	Cluster of Webpages with similar structure and Template	URLs in webpages	MDL Principle based Clustering	Quadratic
Reis et al., 2004	Web-Scale	Heterogeneous	Set of News webpages	News Data from News Webpages	DOM Tree paths	RTDM Threshold based agglomerative Hierarchical Clustering	Quadratic
Kim & Shim, 2011	Web-Scale	Heterogeneous	Set of heterogeneous webpages	Template paths from Webpages	DOM Tree paths	MDL Principle based Clustering	Quadratic

Grigalis & Cenys, 2014	Web - Scale	Heterogeneous	Set of heterogeneous webpages	Clusters of webpages	Set of DOM Tree paths of URLs in webpages	Similarity threshold based clustering	Quadratic

VIII. REFERENCES

[1]. D. Gibson, K. Punera, and A. Tomkins, "The volume and evolution of web page templates," in Special interest tracks and posters of the 14th international conference on World Wide Web - WWW '05, 2005.

[2]. Z. Bar-Yossef and S. Rajagopalan, "Template detection via data mining and its applications," in Proceedings of the eleventh international conference on World Wide Web - WWW '02, 2002.

[3]. S.-H. Lin and J.-M. Ho, "Discovering informative content blocks from Web documents," in Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining - KDD '02, 2002.

[4]. S. Debnath, P. Mitra, and C. L. Giles, "Automatic extraction of informative blocks from webpages," in Proceedings of the 2005 ACM symposium on Applied computing - SAC '05, 2005.

[5]. L. Yi, B. Liu, and X. Li, "Eliminating noisy information in Web pages for data mining," in Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining - KDD '03, 2003.

[6]. V. Crescenzi, P. Merialdo, and P. Missier, "Clustering Web pages based on their structure," Data Knowl. Eng., vol. 54, no. 3, pp. 279–299, 2005.

[7]. D. C. Reis, P. B. Golgher, A. S. Silva, and A. F. Laender, "Automatic web news extraction using tree edit distance," in Proceedings of the 13th conference on World Wide Web - WWW '04, 2004.

[8]. C. Kim and K. Shim, "TEXT: Automatic template extraction from heterogeneous web pages," IEEE Trans. Knowl. Data Eng., vol. 23, no. 4, pp. 612–626, 2011.

[9]. T. Grigalis and A. Cenys, "Using XPaths of inbound links to cluster template-generated web pages," Comput. Sci. Inf. Syst., vol. 11, no. 1, pp. 111–131, 2014.

TECHNO SCIENCE ACADEMY
The International Open Access Publisher

IJSRCSEIT

MIT-WPU
।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"

Organized by

School of Computer Science,
MIT-World Peace University (MIT-WPU), Kothrud,
Pune, Maharashtra, India

Publisher

Technoscience Academy

Website : www.technoscienceacademy.com
Email: info@technoscienceacademy.com

Email : editor@ijsrcseit.com, ijsrcseit@gmail.com