ISSN : 2456-3307

NEW HORIZON
COLLEGE OF ENGINEERING

National Conference on Research Challenges & Opportunities in Digital and Cyber Forensics NCCPS-2020

Organised by

Research Center of Department of Information Science and Engineering , New Horizon College of Engineering, Ring Road, Bellandur Post, Bengaluru, Karnataka, India

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

Volume 4, Issue 11, September-2020

Email: editor@ijsrcseit.com

NEW HORIZON
COLLEGE OF ENGINEERING

IJSRCSEIT

National Conference on Research Challenges & Opportunities in Digital and Cyber Forensics

NCCPS2020

September 30.09.2020

In Association with

and

International Journal of Scientific Research in Computer Science,
Engineering and Information Technology
ISSN : 2456-3307
Volume 4, Issue 11, September-2020
International Peer Reviewed, Open Access Journal

Organised by:

Research Center of Department of Information Science and
Engineering, New Horizon College of Engineering, Ring Road,
Bellandur Post, Near Marathalli, Bengaluru, Karnataka, India

Published By
Technoscience Academy

(The International Open Access Publisher)

Email: info@technoscienceacademy.com
Website: www.technoscienceacademy.com

CHIEF PATRON

Dr. Mohan Manghnani,
Chairman, New Horizon Educational Institution, Bengaluru

PATRON

Dr. Manjunatha,
Principal, New Horizon College of Engineering, Bengaluru

CO PATRON

Dr. M. S. Ganesha Prasad,
Dean & HOD Mech, NHCE

Dr. K. GopalaKrishnan,
Dean, Research and Development, NHCE

Conference Chair

Dr. R. J. Anandhi,
Prof & Head-ISE, NHCE

Conference Coordinators

Dr. Arvind Shivappa Kapse, Professor, ISE, NHCE
Dr. P. Mangayarkarasi, Associate Professor, ISE, NHCE
Dr. Supriya, Sr. Assistant professor, ISE, NHCE

ABOUT COLLEGE

New Horizon College of Engineering is an Autonomous college affiliated to Visvesvaraya Technological University (VTU), approved by the All India Council for Technical Education (AICTE) & University Grants Commission (UGC). It is accredited by NAAC with 'A' grade & National Board of Accreditation (NBA). It is one of the top engineering colleges in India as per NIRF rankings – 2018 and an ISO 9001:2008 certified institution. New Horizon College of Engineering is located in the heart of the IT capital of India, Bangalore. The college campus is situated in the IT corridor of Bangalore surrounded by MNCs and IT giants such as Intel, Accenture, Capegemini, ARM, Symphony, Wipro, Nokia, JP Morgan and Cisco to name a few.

NHCE has a scenic and serene campus that provides an environment which is conducive for personal and intellectual growth. The infrastructure acts as a facilitator for the effective delivery of the curriculum. NHCE boasts of state -of-the -art facilities for its students. The students are given utmost encouragement in their areas of interest by providing hi-tech facilities backed by faculty support. The institute places highest priority on innovative programs of instructions that include both traditional class room theory and professional skills training. There is a strong impetus on overall personality development of the students with emphasis on soft skills. Students are supported through mentoring and counseling systems. The management offers scholarships to meritorious students. At NHCE, from the moment a student walks into the campus, he/she is well guided to know his/her strengths and choose an area of functional specialization. This enables students to concentrate their efforts and energies to gain the competitive edge. NHCE has an unique distinction of achieving 100% admissions in all its courses year after year. NHCE has Centre of Excellence with reputed industries like Adobe, HPE, Vmware, Schnieder Electric, SAP, Quest Global, CISCO.

ABOUT DEPARTMENT

Dept. of Information Science and Engineering at NHCE was established in the year of 2001 and offers B. E., M. Tech and Ph. D. programs and Accredited by National Board of Accreditation (NBA).

B.E. Information Science and Engineering

The four year B.E degree equip the students to meet day- to- day Technological advancements of the ever dynamic IT field through adept training on various subjects of curriculum of Information Science and Engineering and beyond. The department offers B.E program through autonomous scheme from the year 2015. The department has a total intake of 180 every year students with a very good team of highly qualified and talented faculty members including Professors, Associate Professors and Assistant Professors.

M. Tech

The department of Information Science and Engineering also offers 2 year M. Tech program in Cyber-Forensics and Information Security.

ABOUT THE CONFERENCE

The National Conference on "***Research Challenges & Opportunities in Digital and Cyber Forensics***" (NCCPS-2020) provides a common forum for deliberations, sharing of recent trends, advancements and research of Digital Cyber Forensics in the areas of Science, Technology and Engineering. This conference will be a very good platform for academia, researchers, industry practitioners and technologists from all over the world to discuss and present recent advances and research outcomes in their respective fields. We are in the process of finalizing the eminent persons.

Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil courts. Criminal cases involve the alleged breaking of laws that are defined by legislation and that are enforced by the police and prosecuted by the state, such as murder, theft and assault against the person. Civil cases on the other hand deal with protecting the rights and property of individuals (often associated with family disputes) but may also be concerned with contractual disputes between commercial entities where a form of digital forensics referred to as electronic discovery (ediscovery) may be involved.

NCCPS aims to provide an environment where the authors and participants can establish research relations and collaborations with various eminent academicians, research fellows, scientists from India and abroad.

CALL FOR PAPERS

Conference Contents:-

- Digital Forensics
- Digital Evidence
- Seizure of Digital Evidence
- Imaging of Digital Evidence
- Computer Forensics tools and Toolkits
- Analysis of Digital Evidence
- Cyber Security

SUBMISSION GUIDELINES

- All papers should be original, unpublished, not submitted to any other journal/conferences, in pdf format as per the guide lines and IEEE format given in the conference website.
- www.newhorizonindia.edu/nhengineering/nccps2020
- Please mail your original manuscript mentioning your name, contact details and e-mail id to
  nccps2020@gmail.com
- All submitted papers will be checked for plagiarism and papers which are not satisfying the criteria will be summarily rejected
- Notification of acceptance will be through email
- All reviewed papers will be published in UGC approved journals
- Registration fee will be Rs 500.
- Registration form is available in the conference website
- Registration fee includes publication charges, E-Certificate and Publication.

PARTICIPANTS:-

1. Ph. D. Scholar
2. Academician
3. PG Scholar
4. Industry

CONTENTS

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Detection of Glaucoma by Optic Disc and Optic Cup Segmentation

Aswini S*[1], Gnanasekaran T[2]

*[1,2]Department of Electronics and Instrumentation, R.M.K Engineering College, Chennai, Tamil Nadu, India

ABSTRACT

Unique—Glaucoma is viewed as one of the perilous ongoing eye pathologies which lead to vision misfortune much of the time far and wide. The appropriate finding is needed at the perfect time bombing that will prompt irreversible harm for the optic nerve accordingly causing visual impairment. By the assessment of the optic nerve in an optic cup (OC) and optic plate (OD) proportion, there are more opportunities to discover glaucoma. The manual division is finished by looking at the size, shape, and structure of the optics cup just like a plate. Be that as it may, it is a dreary and time taking cycle. Henceforth an easy to use mechanized framework for the optic plate and optic cup extraction is proposed in this paper for the recognition of glaucoma. This paper clarifies a novel and more basic completely computerized confinement just as division of OD and OC by utilizing the Modified Fuzzy C implies calculation.

Keywords : Glaucoma, Optic Disc, Optic Cup, automated localization

I. INTRODUCTION

There are a few eye pathologies on the planet. Glaucoma is one such eye pathology that is ordered utilizing raised intraocular pressure, slow vision misfortune that outcomes in vision misfortune forever making a record to second replenishing explanation behind visual deficiency in the works[1]. Glaucoma is an ongoing neurodegenerative non-reversible eye illness where the neuroretinal nerve which associates the cerebrum and eye is harmed continuously. Early identification of glaucoma is extremely fundamental for sparing a patient's vision. PC helped calculations are commonly utilized for the recognition of glaucoma by figuring the cup to plate proportion for the shaded fundus retinal pictures. Cup to Disk (CDR) is shifted with patients having great eyes and patients with unusual eyes (Glaucoma influenced eye). Generally, the patient with Glaucoma has the cup to circle proportion high and it continues expanding. RGB fundus pictures are gotten utilizing both Fundus cameras just as Optical Coherence Tomography (OCT). Fig .1 shows the vision of an individual with Glaucoma and typical vision. This work principally centers around robotized divided screening glaucoma utilizing Cup to Disk Ratio (CDR) from the retinal fundus pictures.

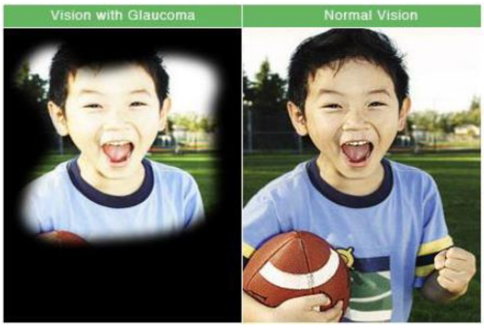


Fig.1 Glaucoma vision and normal vision

II. RELATED WORKS

In the previous, not many years, various investigations have talked about the issue of the division of optic plates. A technique for optic circle confinement, non straight sifting, and vigilant edge discovery with Hough change was proposed by Chrastek et al. [2]. Welfer et al. [3] gave a procedure which depends on versatile morphological preparation. Mendels et al. [3] recommended dynamic forms driven methodology by a creative outer determined field called inclination vector stream. Pixel grouping approach is given by Muramatsu et al [5] sections optic circle by bunching and arranging picture pixels as an optic plate or, in all likelihood foundation pixels. Later Fuzzy c implies and fake neural organizations are utilized for playing out the extraction. Joshi et al[6] proposed district-based dynamic form models by utilizing measurable data recovered from the foundation and closer view areas for limiting energy work. A Hough change-based round layout is proposed by Lowell et al [7]. Numerous goals sliding window band channel (SBF) is applied for OD division [8]. Our principal point is to outline a mechanized framework for fragmenting optic plate and optic cup and to compute CDR for the recognition of Glaucoma.

III. PROPOSED METHOD

The block diagram of the proposed method is illustrated in the fig .2

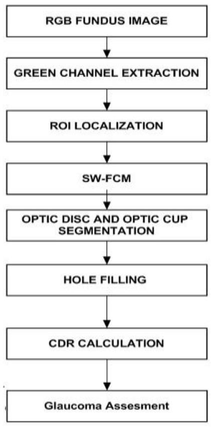


Fig.2 Flow diagram of proposed method

B. Green Channel Extraction

Fundus image consists of Red , Green and Blue components. Of the three shades, the green channel components display the highest vessel backdrop contrast in retinal images of the RGB representation. Red channel will be saturated easily whereas blue channel offers very poor dynamic range as illustrated in figure 3.

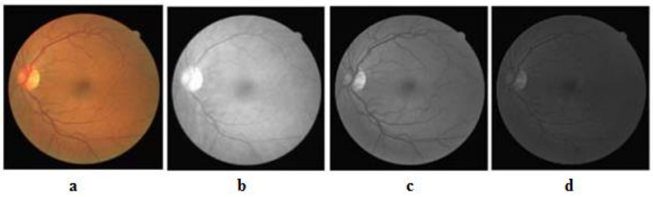


Fig .3 a) Original retinal image, b) red channel, c) green channel, d) blue channel

C.ROI localization

Image localization is done by selecting the region of interest by cropping the image strategically. Here the images are cropped taking OD and OC mask into consideration and masks are obtained as mentioned in [10]. The algorithm considers 15 pixels in addition from the original image surrounded by mask.

D. Spatially weighted Fuzzy C means Clustering (SW-FCM)

The customary Fuzzy C infers that the spatial information on pixels won't be assessed by the grouping calculation and the yield is influenced as an outcome. Consequently, a spatially weighted Fuzzy c implies bunching calculation (SW-FCM). The significant trait of a picture is that pixels in neighbors are profoundly related in the SW-FCM approach. A suitable locale of intrigue (ROI) of measure 255*255 pixels are picked around the greatest point in the green channel of the fundus picture as portrayed before. Since the ROI picture contains the optic circle and optic cup as well as veins. Henceforth veins are taken out so as to acquire better optic division in the fitting locales. Morphological shutting activity utilizing a wavelet change is acquired for lessening the differentiation of the veins. The got aftereffect of SW-FCM will have groups comparing to optic cup and optic circle and foundation. A circular fitting is useful for the plate locale since the state of the circle mostly round and additionally vertically it is considered as oval plate.

E. CDR Ratio

Once optic disc and optic cup is obtained , a variety of features can be computed. Here we followed clinical caucus to compute the cup to disc ratio (CDR) . A high CDR indicates a high risk of glaucoma. Fig. 4 illustrates the important features of the optic regions.

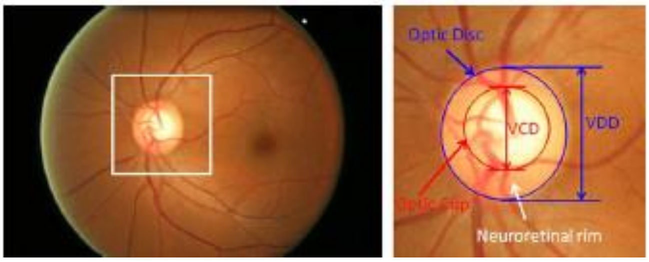


Fig.4 Major structure of optic disc and optic cup (Blue circle is optic disc and red circle is optic cup and region between red and blue is called neuroretinal rim)

Cup to Disc (CDR) ratio is obtained as the ratio between Vertical Cup Diameter (VCD) and the vertical disc diameter(VDD) . The measurement of CDR depends on the segmentation of optic region.

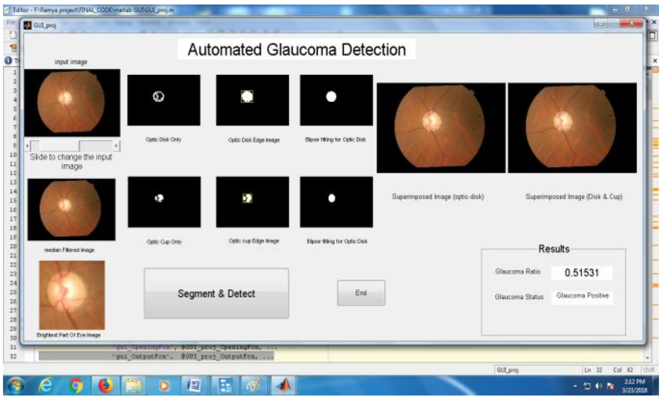
Considering the figure 4

$$CDR = \frac{VCD}{VDD} ....(1)$$

The calculated CDR is generally used for the detection of glaucoma. When CDR is greater than the threshold (here it is considered as 4) it is considered as glaucomatous else healthy.

IV. EXPERIMENTAL RESULTS

The proposed approach is tested using MATLAB7 . Fig 5 shows the a graphical user interface [12] developed for the assessment of glaucoma.Fig. 6 shows output of the the proposed method. Initially the RGB fundus image from database is selected. Image resizing is carried out as a second step of the algorithm. Later Localization is performed by the selection of region of interest. SW-FCM is applied for the segmentation. Optic disc and optic cup segmentation is done using the SW-FCM procedure. Morphological operations are applied for post processing . CDR is calculated as per equation.1 .With the given threshold value glaucoma is diagnosed.


Editor - F:\Ramya project\FINAL_CODE\matlab GUI\GUI_proj.m

GUI_proj

Automated Glaucoma Detection

Results

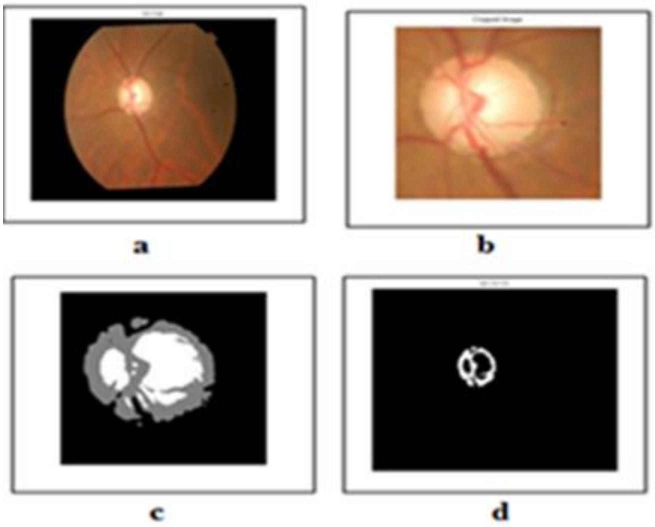
Glaucoma Ratio: 0.51531

Glaucoma Status: Glaucoma Positive

```
'gui_OpeningFcn', @GUI_proj_OpeningFcn, ...
'gui_OutputFcn',  @GUI_proj_OutputFcn, ...
```

input image
Slide to change the input image
Optic Disk Only
Optic Disk Edge Image
Ellipse fitting for Optic Disk
Superimposed Image (optic-disk)
Superimposed Image (Disk & Cup)
median Filtered Image
Optic Cup Only
Optic cup Edge Image
Ellipse fitting for Optic Disk
Brightest Part Of Eye Image
Segment & Detect
End
GUI_proj
Ln 32
Col 62
OVR
2:12 PM
3/23/2018

Fig. 6 Graphical User Interface of our proposed method



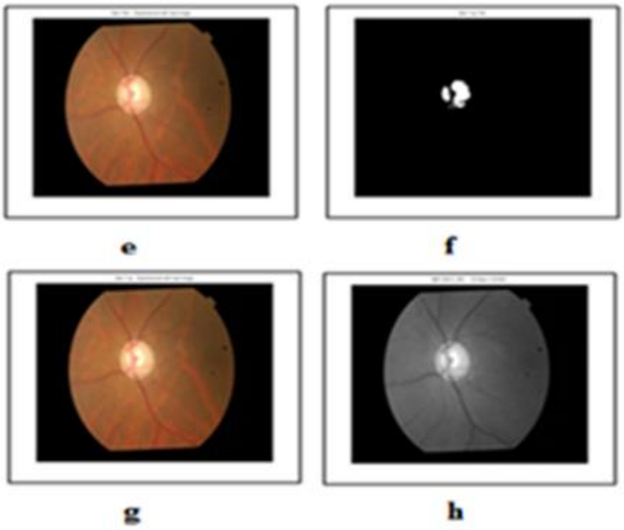


Fig .5 Output by proposed method a. Input Image, b.ROI Selection, c.SW-FCM Applied ,d. Segmented optic disc, e. Optic disc on original image, f. Segmented optic cup, g. Optic disc and optic cup superimposed , h. CDR calculated and Glaucoma detected

V. CONCLUSION

In this work, we built up a robotized framework for the division of optic circle and optic cup for the location of Glaucoma by computing the cup to plate (CDR) proportion. Additionally, our graphical UI is an easy to understand interface so any individual who is intrigued to distinguish glaucoma can without much of a stretch utilize our framework. As a continuation of this work, we are in the cycle of assessing the proposed technique on different information bases and improve the strategy.

VI. REFERENCES

1. Septiarini and A. Harjoko, "Automatic Glaucoma detection based on the type of Features used: a review," Journal of theoretical & Applied information technology, vol. 72, 2015.
2. R. Chrastek, M. Wolf, K. Donath, G. Michelson, and H. Niemann, “Optic disc segmentation in retinal images,” Bildverarbeitung f¨ur die Medizin, pp. 263–266, 2002.
3. D. Welfer, J. Scharcanski, C. M. Kitamura, M. M. D. Pizzol, L. W. Ludwig, and D. R. Marinho, “Segmentation of the optic disk in color eye fundus images using an adaptive morphological approach,” Computers in Biology and Medicine, Elsevier, vol. 40, no. 2, pp. 124–137,2010.
4. F. Mendels, C. Heneghan, and J. P. Thiran, “Identification of the optic disc boundary in retinal images using active contours,” Proceedings of the Irish Machine Vision and Image Processing Conference, pp. 103–115, 1999.

A. Muramatsu, T. Nakagawa, A. Sawada, Y. Hatanaka, T. Hara, T. Yamamoto, and H. Fujita, “Automated segmentation of optic disc region on retinal fundus photographs: Comparison of contour modeling and pixel classification methods,” Computer Methods and Programs in Biomedicine, Elsevier, vol. 101, pp. 23–32,2011.

5. G. D. Joshi, J. Sivaswamy, and S. Krishnadas, “Optic Disk and cup segmentation of monocular color retinal images for Glaucoma assessment,” IEEE Transactions on Medical Imaging, vol. 30(6), pp.1192–1205, 2011.
6. J. Lowell, A. Hunter, D. Steel, A. Basu, R. Ryder, E. Fletcher, and L. Kennedy, “Optic nerve head segmentation,” IEEE Transactions on Medical Imaging, vol. 23(2), pp. 256–264, 2004.
7. Dashtbozorg Behdad, Ana Maria Mendonc¸ a, Aurélio Campilho, Optic discsegmentation using the sliding band filter, Comput. Biol. Med. 56 (2015)1–12.
8. X.Zhang, G.Thibault, E.Decenciere,G.Quellec, G.Cazuguel ,A.Erginay, P.Massin and A.Chabouis, “ Spatial normalization of eye fundus images,” in ISBI 2012: 9th IEEE International symposium on biomedical imaging ,2012
9. S.Morales,V.Naranjo, J.Angulo , and M.Alcaniz, “Automatic detection of optic disc based on PCA and mathematical morphology,IEEE Transactions on Medical Imaging,Vol 32,No.4,pp 786-796,April 2013.
10. Chuang KS, Tzeng HL, Chen S, Wu J, Chen TJ. Fuzzy c-means clustering with spatial information for image segmentation. Comput Med Imaging Graph 2006;30(1):9-15.
11. https://in.mathworks.com/discovery/matlab-gui.html

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

User Feedback and Service Security in Android Application Platform

Dr. Avinash S. Kapse*[1], Pravinkumar M. Ghaywat[2]
*[1]Ph.D.(CSE),M.E.(CSE),B.E.(CSE), Diploma (CT) , Associate Professor & Head of Department,
Information Technology, Anuradha Engineering College, Chikhli, India
[2]Student, Department of Computer Science & Engineering, Anuradha Engineering College, Chikhli, India

ABSTRACT

Moreover some technology are benefits to the society whereas some are very hard to accept the drastic change. The best example in all this facts are Android devise which definitely helps to generate various features in coming technological word and helps to fulfil the demand of the clock. But as far as demand is concerned the security features are also became the major part for considering the fact and its mechanism off course became the major part of concerned .This paper will determine how we can make it is feasible to make control the security feature of the any Android devices by making a mechanism by which we can improve its performance and reduce the security related issue.

Keywords : Android OS, Smartphone's, Malwares, Cloud Services, Applications Security.

I. INTRODUCTION

Recently, the use of Android OS smartphones has increased rapidly, so that better security policy has become the most important area of research. Because smartphone devices are used rapidly by companies, and various government agencies also in the military, security plays an important role, because many users use these devices to store their precious sensitive data, attackers can use this sensitive information with the wrong intent. Some key security issues are related to communication issues or network handling issues. Some viruses are vulnerable to Android phones that cause a lot of damage to the device's memory in terms of both software and hardware damage, so to prevent this problem, it is necessary to design a system that protects the security process.

Anti-virus research is recently ongoing process for identifying and analyzing new and unknown malware for extracting possible detection scheme that can be used within some anti-virus software. There exits some virus and malware detector software that can scan and block viruses, Trojans that are infecting Android applications. Most malwares is being detected by scanning in signature database. For generating the reports and special signatures the infected application need to be analyzed and carefully observed so that we can collect some meaningful pattern about the specific malware.

II. RELATED WORK

The following are various studies related to this topic that have been conducted previously, including:

A. Applying Behavioral Detection to Android Devices

Shabtai A. and Elovici Y. present a lightweight, behavior-based detection framework called Andromaly for Android smartphones that implements a host-based intrusion detection system (HIDS).

B. Crowdroid: a behavior-based malware detection system for Android Burguera et al. provide a framework for receiving and analyzing the actions of smartphone applications called Crowdroid.

C. Detection of Smartphone Malware

Schmidt A.-D.'s dissertation provides a detailed overview of the evolution and current status of smartphone malware.

D. Cloud-based intrusion detection and response system for mobile phones

Houmansadr et al. proposes cloud-based intrusion detection and response architecture. Its objectives are transparent operation for the user, use of light resources, and real-time and accurate intrusion detection and response.

E. Paranoid Android: versatile protection for Smartphones

Portocalist et al. presents a prototype called Paranoid Android for Android Smartphone security checks on a remote server hosting an exact replica of the phone.

F. Smartphone Monitoring for Anomaly Detection

Schmidt et al. demonstrated how a smartphone running Symbian OS can be monitored to extract features for anomaly detection.

G. Virtual In-Cloud Security Service for Mobile Devices

Oberheide et al. introduced a model for moving anti virus functionality to off-device network services that use multiple malware detection engines.

H. XMan Droid: New Android Evolution to Reduce Privilege Escalation Attacks

Bugiel et al. proposes a security framework called XManDroid to detect and prevent application-level privilege escalation attacks at runtime.

I. Security as a Service in Cloud for Smartphones

Lakshmi S. proposed a generic architecture for a security service for smartphones and use cases how the service can be used.

System Implementation & Working

Using manifest.xml file we fetch all the user data whenever the user downloads any application from the net. Proposed system mainly consists of three modules which are listed below also following figure 1 shows the system architecture.

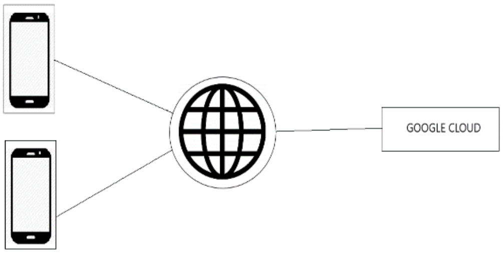


Figure 1: system architecture

i. Performing Signature Analysis.

Module actually decompiled the installed .apk files available on the system is performed. Android classified in various categories in which they bifurcated for security reason such as very light, light, medium, heavy, very heavy applications.

ii. Cloud Integration

All reviews of the applications are stored in firebase and are retrieved whenever required for any circumstances. When any feedback is reported the IMEI number the date of the report was activated from SIM 1 only and can be classified between 1 as good application and 0 s bad application

III. HOW SYSTEM WORKS

For this Android operation we use the Android Application Development Tool and in it we create one .apk file that needs to be run on the mobile phone together with the server (firebase) also needs to be started. When installed on the mobile phone, the application classifies the applications in light, heavy, etc. Then we will create a filter for the necessary permissions with the associated name, where we have to select some permissions for the program then we have to choose the filter color which then appears on the permissions for the program we can tell which filter the program has. Then select any application from the apylyzer application list, then several options will appear that select an online action and the user can choose any option to record their reaction to that option and the resulting feedback will be saved in Google Firebase.

4.1 Module

Since our main discussion area is the security of Android applications, we will try to address some of the shortcomings of various security policies at the moment. In this system, when the user actually downloads any application available in the application market, all services, permissions and signatures of that application are extracted using the manifest.xml file. The proposed system mainly consists of three units listed below

4.1.1 Extract of installed applications.

This module performs actual degradation of installed .apk files available on the system. The screen is also classified as very light, light, medium, heavy and very heavy depending on what signature, services, permissions and screen layout are available in a particular application.

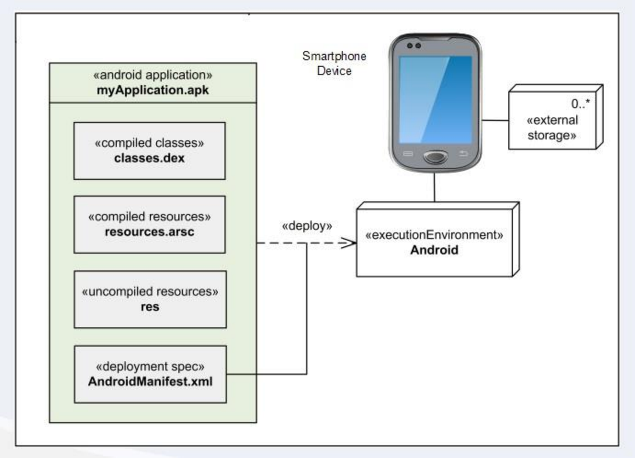


Figure 2: deployment diagram

4.1.2 Generating and Storing Reports.

All reports are stored in the cloud and are retrieved as per the need which was specify as good application and bad application in the algorithm.

4.1.3 User Feedback Detection.

Some filter application at last helps to set the permission in the system and generate the report as per the need and the user can uninstall the app which gets more threats score

IV. CONCLUSION

In this way we tried to remove the barrier of security concerned which required for any android devices and helps to modify the system in better manner. And able to determine how we can make it is feasible to make control the security feature of the any Android devices by making a mechanism by which we can improve its performance and reduce the security related issue.

V. REFERENCES

[1]. Byung-Gon Chun and Petros Maniatis., Augmented smartphone applications through clone cloud execution. In Proceedings of the 12th conference on Hot topics in operating systems, 2009.

[2]. Georgios Portokalidis, Philip Homburg, Kostas Anagnostakis, and Herbert Bos. Paranoid android: versatile protection for smartphones. In Proceedings of the 26th Annual Computer Security Applications Conference, 2010.

[3]. Asaf Shabtai and Yuval Elovici. Applying behavioral detection on android-based devices. In MOBILWARE, pages 235–249, 2010.

[4]. A D Schmidt. Detection of Smartphone Malware. PhD thesis, Technischen Universit¨at Berlin, 2011.

[5]. Amir Houmansadr, Saman A. Zonouz, and Robin Berthier. A cloud-based intrusion detection and response system for mobile phones. In Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and NetworksWorkshops, DSNW '11, pages 31–32,Washington, DC, USA, 2011. IEEE Computer Society.

[6]. Iker Burguera, Urko Zurutuza, and Simin N. Tehrani. Crowdroid: behavior-based malware detection system for Android. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, SPSM '11, pages 15–26, New York, NY, USA, October 2011. ACM.

[7]. Georgios Portokalidis, Philip Homburg, Kostas Anagnostakis, and Herbert Bos. Paranoid android: versatile protection for smartphones. In Proceedings of the 26th Annual Computer Security Applications Conference, 2010.

[8]. Aubrey-Derrick Schmidt, Frank Peters, Florian Lamour, and Sahin Albayrak. Monitoring smartphones for anomaly detection. In Proceedings of the 1st international conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications, MOBILWARE '08, pages 40:1–40:6, ICST, Brussels, Belgium, Belgium, 2007. ICST

[9]. Jon Oberheide, Kaushik Veeraraghavan, Evan Cooke, Jason Flinn, and Farnam Jahanian. Virtualized In-Cloud Security Services for Mobile Devices. In Workshop on Virtualization in Mobile Computing (MobiVirt '08), Breckenridge, Colorado, June 2008.

[10]. Philipp Stephanow Lakshmi Subramanian, Gerald Q. Maguire Jr. An architecture to provide cloud based security services for smartphones, 2011.

[11]. Sven Bugiel, Lucas Davi, Alexandra Dmitrienko, Thomas Fischer, and Ahmad-Reza Sadeghi. Xmandroid: A new android evolution to mitigate privilege escalation attacks. Technical report, Technische Universit¨at Darmstadt, 2011.

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

A Survey on Distributed Denial of Service Attacks in the Online Gaming Industry

Sanjana A, Medha Vinod
ISE Department, NHCE, Bangalore, Karnataka, India

ABSTRACT

In this digital era, threats in the cyber world has exponentially risen and has resulted in a huge number of cyber-attacks all over the world. One of the most notorious cyber-attacks is distributed denial of service (DDoS), which is a subclass of denial of service (DoS) attacks. DDoS attacks are a standard tactic used to make a service/server unavailable to its users. These attacks involve hackers sending large amounts of traffic to overwhelm and disable a targeted system with a flood of internet traffic. According to several reports, online gaming industry has become the biggest victim or target to DDoS attacks. This paper provides a systematic survey on the various DDoS attacks taking place in the gaming industry. This paper also provides an analysis of the trends of these attacks, counter measures and factors affecting it and vulnerabilities. Through this analysis, we can identify the prior vulnerabilities faced by online gaming and ensure a more successful defense against these threats in the future. Thereby it will help in providing a secure and efficient medium for online gaming.

Keywords : DoS, DDoS Attacks, Online Gaming Industry, Safer Medium, vulnerabilities

I. INTRODUCTION

DoS (Denial of Service) attack is a cyber- attack with spiteful user aimed to render a host computer or other device unavailable to its authorized users by disturbing the device's normal operation. DoS attacks is usually practice of overwhelming or a targeted machine with requests until normal traffic is not able to be processed, resulting in denial-of-service for the users. A DoS attack uses a single computer to launch the attack. A DDoS (distributed denial-of-service) attack is a malicious attempt that tries to disrupt the regular traffic of a targeted server, service or network by overwhelming the target or its contiguous infrastructure with an overflow of Internet traffic. DDoS attacks are more complex as compared to DoS attacks as they involve a large range of devices, increasing the intensity of the attack. Being attacked by one computer is not the same as being attacked by a botnet of a large number of devices. One of the fields affected by DDoS is the gaming industry.

There are different ways by which these attacks affect users. The first is providing the access to lager multiplayer games where there can be only limited which then waits until the developer agrees to the demands of the attacker. On the other side, the game may harm the reputation of the company with limiting player access Similar kind of attacks are initiated by rival businesses or even by overly addicted fans looking to boost their game by harming each other. These can be commenced by the passionate community members observing to punish a developer or publisher for wrong business practices. However, some engage in these attacks to signify their lashing out towards content changes in an online game or even due to the fact that the individual player has been debarred from a game for a certain reason.

II. DDOS ATTACKS IN ONLINEGAMING INDUSTRY

Online gaming industry has been a victim to Distributed denial of service (DDoS) attacks for so many years. Based on several reports from the industry and present trends, the prevalence of DDoS attacks is multiplying exponentially and online gaming servers are the number one target for DDoS assaults [1]. According to [2], this cyber-attack keeps happening on a daily basis for several online gaming websites and servers. These attacks spike prominently during holiday seasons, the summer and spring seasons. A recent report published by Akamai [3], It was observed that 3,072 distinct DDoS attacks in the gaming industry was published in the report present by Akamai [3], between the time span of July 2019 and June 2020.

A. *Infamous DDoS Attack Incidents in Online Gaming*

The most common type of DDoS attack for video games or online games is the network layer attack in which the defenders target your network infrastructure itself. Two popular hacktivist collectives "Lizard Squad" and "Poodle corp." are infamously known for their DDoS attacks on popular online video games like Nintendo, League of Legends, few games in Blizzard networks and also on PlayStation, Xbox.

Some of their attacks are :

1) *Christmas 2014 attacks on PSN and Xbox Live :* Hacking group Lizard Squad threatened formerly to take gaming down the services on Christmas. And on 25th of December, 2014 (Christmas Day), Lizard Squad demanded to have DDoS attack on the Network PlayStation and Xbox Live. Later, distributed denial of service (DDoS) attack took credit on Xbox Live that left tens of thousands of users unable to connect to the service [4]. Their servers were down for several hours and had their cyber-security teams trying to bring them back up. Using a recently discovered malware variant, it was found that these hackers turned household routers into so-called "stresser" tools, which was used to flood the networks with bogus traffic, finally made the service unavailable for legitimate gamers [5].

1) League of Legends DDoS: Servers of the game League of Legends were taken offline with a DDoS attack on 18th August 2014, Later Lizard Squad claimed this to be their first attack [4].
2) Destiny DDoS: 23th November 2014, Lizard Squad claimed they attacked and took down Destiny servers with a DDoS attack [4].
3) Xbox Live DDoS: 1st December 2014, Xbox Live was apparently attacked by the infamous Lizard Squad. Numerous users attempting to connect to use the service would be given the 80151909 error code [4].
4) Sony's PlayStation Network DDoS: In 2011, the PlayStation Network was compromised by sony, which was not noticed by the security breaches of that user accounts, Qriocity and Sony Online Entertainment because distributed denial of service attacks was used as a distraction to make their services unavailable. It was later unveiled that the nearly 77 million users account information on the was been stolen by the hackers by PlayStation Network and Qriocity A week later, it was the acknowledged by the company that the Sony Online Entertainment gaming service had also been breached, affecting an additional 24.6 million users. More than 101 million legitimate user accounts have been compromised. The user names, addresses, email

addresses, dates of birth were included in the data stolen [6]. Lizard Squad claimed the responsibility of the PlayStation Network disrupted via a DDoS attack, 24th August 2014 and again reclaimed 8th December 2014[4].

5) Battlefield 1: Online gamers of a new beta of the video game Battlefield 1 saw their activity disrupted after an alleged distributed denial of service (DDoS) attack knockout the servers of games company Electronic Arts (EA). In 2016, Poodle Corp launched repeated attacks against EA, Blizzard and Riot Games. These hacktivist collectives sold DDoS attacks services and was in a form of advertisement that often partake in stunt hacking. They would also try to intentionally ruin launches of specific and often popular titles, like Battlefield 1 [7].
6) Blizzard: Blizzard Entertainment, an American Video game company which has released several video games like Call of Duty (CoD), Overwatch, World of Warcraft (WoW) has been a victim several times to DDoS attacks over the years. First in April 2016, Blizzard's World of Warcraft: Legion launch faced a cyber-attack. According to Blizzard Entertainment, a distributed denial of services (DDoS) assault caused high latency issues and disconnections during the launch of their new expansion. DDoS attack was a small scale assault, but still managed to take down all the servers of the game during the expansion launch of World of Warcraft: Warlords of Draenor. The hacker group Lizard Squad claimed responsibility for the attack at the time [8]. Later that same year their game servers "Battle.net" was taken down for a span of two hours with players not being able to connect to the game's servers. In August 2017, Over the years, Blizzard's server "Battle.net" has become a victim to several DDoS attacks. The most recent attacks were on June 2020. One of their popular online game "Call Of Duty: Modern Warfare and Warzone" was attacked and the servers were down [10].
7) Final Fantasy XIV : Popular online game Final Fantasy XIV has been dealing with an advanced and persistent DDoS attack. A recent DDoS attacks had flooded the Square Enix's networks, which resulted in an intermittent service degradation and disconnection for over a month [11].
8) Ubisoft : Ubisoft was faced with a series of DoS and DDoS attacks that resulted in service degradation and disconnection that had impacted several major online titles including Rainbow Six Siege and Ghost Recon. Ubisoft issued a statement regarding those attacks stating, DDoS assaults is a common threat for almost all online video games and their service providers. In addition to the outages at Ubisoft, NCSoft released Master X Master, a Multiplayer Online Battle Arena (MOBA) game. NCSoft suffered from several DoS attacks that resulted in users experiencing high level latency and dropped connections [11].
9) Pokémon GO: A group of hackers called "Poodle Corp." had claimed responsibility for a distributed denial of service (DDoS) attack that had down taken the servers of insanely popular augmented reality game Pokémon GO offline [12].
10) Under *application layer attack:* the Mirai botnet was one of the scariest DDoS attack in the history. The couple of Students originally created the Mirai botnet to disable Minecraft servers and later was manipulated to launch the largest-ever DDoS attack [13]. The Mirai botnet had compromised more than 600,000 devices at its peak, creating a DDoS tool magnitudes greater than anything the internet had seen before and was capable of crippling huge parts of it [14].

A. *TRENDS OF DDOS ATTACKS IN ONLINE GAMING*

Akamai has observed since July 2019 that 3,072 distinct DDoS attacks in the gaming industry, making it the largest target DDoS across the net [3].

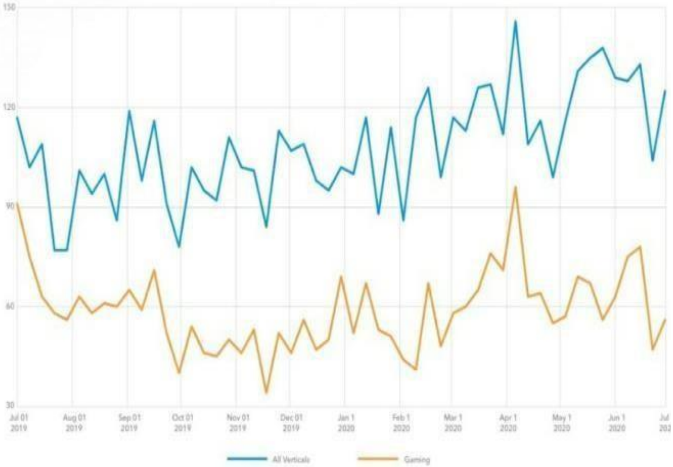


Fig.1 Weekly DDoS Attack Events [3]

DDoS attacks are consistent, occurring particularly in gaming. In 2016, Mirai botnet which was responsibility for a large number of DDoS attacks that created havoc on internet. Several countries like Russia, Turkey and Netherlands are notoriously known for their strong existences in underground forums for DDoS services which is used for targeting mainly gaming.

DDoS Attacks Events by mitigation Outcome are given below, Gaming vs. Rest of the services from July 2019 to June 2020[3].

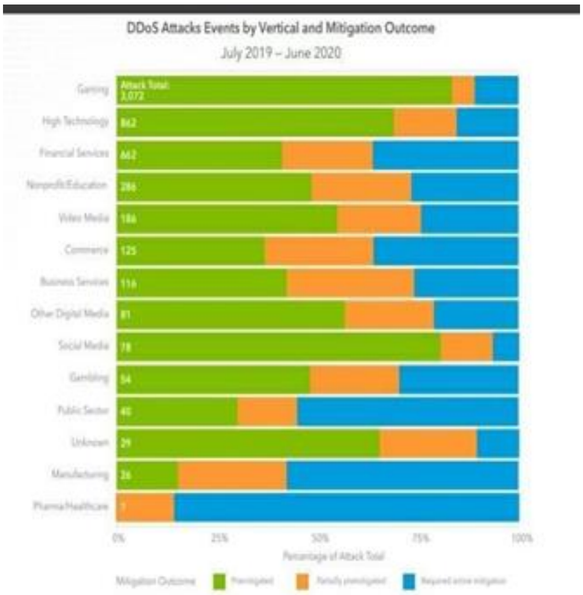


Fig.2 Vertical Outcome

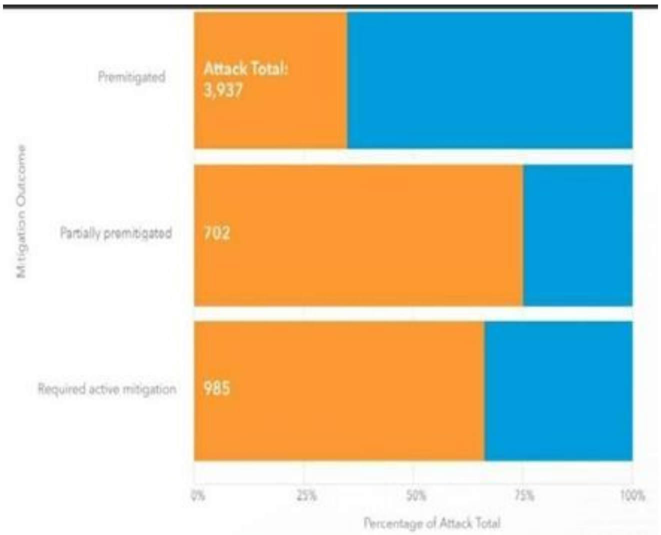


Fig.3 Mitigation Outcome

III. FACTORS CONTRIBUTING TODDOS ATTACKS IN ONLINEGAMING

There are reasons indicating that online gaming industries are targeted more than others, which are [15]:

A. Business Competition

In the world of competitive industries such as online gaming, an attack of DDoS can be used to take down a rival's servers or website.

B. Extortion

Industries like online video games and e- commerce websites are dependent on their online presence and become an easy prey for perpetrators exchange for keeping a specific website online. extorting money.

Hacktivism

Hacktivists commonly target websites related to media, politics or shared sites to protest their actions or ideologies.

C. Vandalism

Cyber vandals, typically random offenders, often attack gaming services or other high profile targets.

D. Nature of Gaming

An advantage is taken over DDoS attack perpetrators gaming and emotion that online gamers have a deep connection for a level or a connection to a specific character in the game. Any interruption in the game may lead to chaos and causing the attackers take advantage of this experience and emotion of these online gamers and twist on the worst to bring about an outbreak.

IV. LOOPHOLES AND VULNERABILITIES

In recent times, the gaming industry has taken DDoS attacks as a considerable margin [17-21].The Hypertext Transfer Protocol (HTTP) does not work neither support the attacks, thereby they are primarily designed or targeted at the network layer.

They explode the server with exponential requests which slows down the servers to the point where the connection ultimately breaks. After a DDoS attack, online gamers are unable to log in and save their data and also the entire storage is wiped lost. Some of loopholes and vulnerabilities are:

A. *Predictable rush hours*

The existing server and network resources are exhausted by DDoS attacks, they are most effective when the resources are already scarce, for instance when a network is being utilized by a large scale of users simultaneously. Sony and Microsoft sold a combined 11 million consoles just before Christmas in the year 2014, which made it easy to expect that their networks would be strapped to their respective limits. During a similar condition, when the reports are depreciation in service due to the sheer volume of regular requests and traffic, then disrupt server/service caused by is much easier for an attacker or hacker to saturation already struggling network infrastructure.

A. Don't have to take it offline

All gamer can conveys that we can't completely shut down a gaming server to bring it to a halt. Games, especially those featuring multiplayer competitive operations, are completely about instant feedback of users; every additional millisecond between "order given" and "action taken" can severely disrupt the experience of the game. An e-commerce website resulting an attack on a half-second latency might go unnoticed, but a DDoS assault on a Call of Duty server causing the same delay would completely stop all activities. This is not because the server is unavailable, but because it becomes unusable or unstable.

B. Proprietary Protocols

Gaming platforms are built on proprietary protocols rather than HTTP, which are custom network protocols built with highest precision in performance. For an application such as a game, it is not easy for it to distinguish between a player and a DDoS bot because there is very little information provided by the online gamers and taken by the game's developer to differentiate between them.

D. *Single points of failure*

Many applications and online games derived from cloud are managed from a central platforms. When these are taken down by hackers, this causes the entire service to go dark for their legitimate users. In some cases, a DDoS attempt can wreak havoc even if it doesn't succeed in taking the targeted servers completely offline. For instance, mere pressure resulting in slower or more inconsistent performance can ruin the day for an online gamer.

E. *UDP*

It is very popular among DDoS attackers because it's easy to spoof and is used in almost all DNS amplification attacks, which exploits the vulnerabilities and loopholes in domain name system (DNS) servers. Beyond UDP, several other common attack vectors are SYN Flood, DNS Response, TCP and NTP.

V. CONTROL MEASURES

Most online industry Game developers and the related companies remain the main target for DDoS attacks, which comprises of the large percent of all DoS and DDoS attempts. The Security Operations Command Centre (SOCC) Experts tailor the mitigation controls to detect these attacks and try to eradicate these attacks in the future by conducting live analysis of the internet traffic to determine further improvement . DDoS attack events are found out either by the SOCC or by the targeted organization itself. SOCC records major part of the attack mitigation data [1].

A. Anti-Malware Software

It is a rock solid anti-malware software that also monitors your internet connection. The software Anti-malware is used reports of existing malware and bot signatures to identify and block them from infecting your computer. This is only a fraction of the work done, as new kinds of malware will be made the next second and there can only be few people discovering and reporting their signature to the respective companies.

B. VPN

Virtual private network (VPN) use certain protocols to basically encrypt the data and send it through servers so the sender and receiver of the data will not be exposed. Several VPN providers like Nord VPN also have specific DDoS attack relief servers which uses a stability check systems to monitor all unusual amount of internet traffic going through the server. Finally distributes it and cover the data in order to minimize the negative effects on the legitimate users [22].

C. Generic Routing Encapsulation Tunnel

A generic routing encapsulation tunnel (GRE) is a vital component that ensures that the normal users are not affected by insufficient mitigation measures. A GRE tunnel reduces the network traffic and establishes a high-speed point-to-point connection between the network nodes that will bypass normal routing disturbances [1].

VI. CONCLUSION

Due to very fast advancement in technology, we experience a humungous amount of cybersecurity threats and challenges. The online gaming industry is one industry that has been threatened over the years. This survey paper focuses on DDoS attacks and how these attacks have been affecting the gaming industry over the years. The various loopholes that are used by the DDoS attackers have been discussed, along with the trends of these attacks over the years and the control measures taken to prevent such attacks. With time, there definitely will be an improvement in the research to generate methods that ensure DDoS can be handled effectively the safety of online gaming.

VII. REFERENCES

[1]. DDoS Mitigation,"It's Not a Game: The Ever-Growing Risk of DDoS Attacks on Online Games",Accessed on: September 23rd.[Online].Available: https://www.imperva.com/blog/ddos- attacks-on-online-gaming-servers/

[2]. CAMBRIDGE, Mass., State of the Internet / Security report, Gaming: You Can't Solo Security, Sept. 23, 2020 .Accessed on Sept. 24, 2020.

[3]. [Online].Available:https://www.akamai.com/uk/en/multimedia/do cuments/state-of-the-internet/soti-security-gaming-you-cant-solo- security-report-2020.pdf

[4]. Martin Mkeay,"Gaming, You can't solo Security",Accessed on: September 23rd. [Online]. Available: https://www.akamai.com/uk/en/multimedia/documents/state-of- the-internet/soti-security-gaming-you-cant-solo-security-report- 2020.pdf

[5]. Brian Feldmen ,"Three Minecraft Players Were Behind the Botnet That Took Down a Chunk of the

Internet Last Year",Accessed on: September 24rd. [Online]. Available:https://nymag.com/intelligencer/2017/12/three- minecraft-players-created-the-webs-scariest-botnet.html

[6]. Russell Brandom ,"Lizard Squad used hacked routers to take down Xbox Live and PlayStation Network",Accessed on: September 24rd. [Online]. Available:https://www.theverge.com/2015/1/9/7520415/lizard- squad-used-hacked-routers-to-take-

[7]. Fahmida Y. Rashid ,"Sony Data Breach Was Camouflaged by Anonymous DDoS Attack",Accessed on: September 24rd. [Online]. Available:https://www.eweek.com/security/sony-data- breach-was-camouflaged-by-anonymous-ddos-attack

[8]. "Recent DDoS Attacks on Game Providers Ubisoft and NCSoft",Accessed on: September 24rd. [Online]. Available:https://security.radware.com/ddos-threats-

[9]. attacks/threat-advisories-attack-reports/ddos-assaults-on-gaming- providers/

[10]. Paul Sawers ,"PlayStation Network and Xbox Live DDoS arrest:

[11]. U.K. authorities grab an 18-year-old man",Accessed on: September 24rd. [Online]. Available:https://venturebeat.com/2015/01/16/18-year-old- arrested-over-playstation-and-xbox-ddos-attacks/

[12]. Tom Spring ,"Blizzard Entertainment Hit With Weekend DDoS Attack",Accessed on: September 24rd. [Online]. Available:https://threatpost.com/blizzard-entertainment-hit-with- weekend-ddos-attack/127440/

[13]. Eric Kain"Hit By DDoS Attack — 'Call Of Duty' 'Overwatch' And 'World Of Warcraft' Experiencing Issues",Accessed on: September 24rd.[Online].

[14]. Available:https://www.forbes.com/sites/erikkain/2020/06/02/call- of-duty-modern-warfare-and-warzone-servers- down/#91fa6b77a908

[15]. "Recent DDoS Attacks on Game Providers Ubisoft and NCSoft",Accessed on: September 24rd. [Online]. Available: https://security.radware.com/ddos-threats-attacks/threat- advisories-attack-reports/ddos-assaults-on-gaming-providers/

[16]. Duncan Riley, Inc. ,"Pokemon GO goes down following DDoS attack from Poodle Corp",Accessed on: September 24rd. [Online]. Available: https://siliconangle.com/2016/07/17/pokemon-go-goes- down-following-ddos-attack-from-poodle-corp/

[17]. Akamai Technologies, Inc. ,"Akamai Report Reveals Broad, Persistent Cyber Attacks Targeting Video Game Players and Companies",Accessed on: September 24rd. [Online]. Available: https://www.prnewswire.com/news-releases/akamai-report- reveals-broad-persistent-cyber-attacks-targeting-video-game- players-and-companies-301136183.html

[18]. https://nymag.com/intelligencer/2017/12/three-minecraft-players- created-the-webs-scariest-botnet.html

[19]. Lance Whitney ,"Why certain companies are more heavily targeted by DDoS attacks",Accessed on: September 24rd. [Online]. Available: https://www.techrepublic.com/article/why-certain-companies-are-more-heavily-targeted-by-ddos-attacks/

[20]. Olawale Daniel ,"Online Gaming: Are DDoS Attacks The Biggest Nemesis For Online Gamers?",Accessed on: September 24rd. [Online]. Available: https://techatlast.com/ddos-attacks-online- gamers/

[21]. Olawale Daniel ,"Online Gaming: Are DDoS Attacks The Biggest Nemesis For Online Gamers?",Accessed on: September 24rd. [Online]. Available: https://techatlast.com/ddos-attacks-online- gamers/

[22]. Paul Sawers ,"PlayStation Network and Xbox Live DDoS arrest:

[23]. U.K. authorities grab an 18-year-old man",Accessed on: September 24rd. [Online]. Available:https://venturebeat.com/2015/01/16/18-year-old- arrested-over-playstation-and-xbox-ddos-attacks/

[24]. Olawale Daniel ,"Online Gaming: Are DDoS Attacks The Biggest Nemesis For Online Gamers?",Accessed on: September 24rd. [Online]. Available: https://techatlast.com/ddos-attacks-online- gamers/

[25]. Noah Gamer ,"Why DDoS attacks target gaming and software companies",Accessed on: September 24rd. [Online]. Available:

[26]. https://blog.trendmicro.com/why-ddos-attacks-target-gaming-and- software-companies/

[27]. Lance Whitney ,"Why certain companies are more heavily targeted by DDoS attacks",Accessed on: September 24rd. [Online].Available:https://www.techrepublic.com/article/why- certain-companies-are-more-heavily-targeted-by-ddos-attacks/

[28]. Hrvoje,"DDOS: THE ENEMY OF ONLINE GAMING AND HOW TO PROTECT YOURSELF",Accessed on: September 24rd. [Online]. Available: https://www.keengamer.com/

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Automatic Waste Segregator Using Image Classification

Sonali Preetha Nandagopalan, Silpa S, Prakriti Sharma K P

ISE Department, NHCE, Bangalore, Karnataka, India

ABSTRACT

Negligent and improper waste segregation has led to a lot of environmental issues like global warming and we and the upcoming generations are the victims to it. Improper segregation causes production of waste that cannot be reutilized which makes itself hazardous as the dumping of plastic. Hence Waste Segregation is of utmost necessity. A fully automated waste segregation system would be beneficial as it would enable us to implement a fully sealed garbage sorting space, so the chances of pollution of garbage reduces. As it is automated, the odour problem from waste can be handled. It would also mean that the workers' health in the waste management industry would be prone to lesser risks. Final products procured from the waste segregation process can be refined into useful resources or disposed without generation of any pollutant. This paper proposes an "Automatic Waste Segregator" (AWS) which can be used by organizations handling large number of people and hence dealing with a lot of day to day waste. The waste classifier is built using an Image Classification Algorithm, trained and tested on the Waste images dataset. The classifier segregates the waste into three categories namely, dry, wet and plastic waste. The classifier is then deployed on a Raspberry Pi board. The trash will be thrown into a dustbin which is internally divided into three bins. All three bins are covered by plates which form the common base where connected to it) will then detect the type of waste and the corresponding plate opens and the trash falls into the right bin. The AWS is connected to a network hence security is of utmost importance. We propose multi factor authentication to access any data or IOT device related to the AWS. In this paper we also deal with next generation firewall for protection of the network the project works on and also ensuring hardware outage doesn't result in insecure state of IOT device.

Keywords : Automatic waste segregator, Waste Management, Raspberry PI, Image Classification, Camera, IOT Security.

I. INTRODUCTION

Generating waste is as normal as breathing or bathing. It is a part of the drill. All the problems arise when this waste is not disposed or segregated properly. It can cause economic, environmental and health issues in multiple ways. Each kind of waste, after segregation is disposed in a different way. Waste can be recycled, used in landfills or even incinerated.

When waste is not segregated properly, it can contaminate soil and water bodies. When soil is contaminated: land fertility reduces, which leads to lesser produce and so more people go hungry to bed in the end. When water bodies get contaminated: the water quality reduces, marine/river life gets effected and as a result all the animals and human beings that sustain on food from the water bodies, suffer. Water contamination also leads to formation of pathogens like Cholera and Dysentery that were labelled as epidemic, once upon their time. When the wrong kind of waste is used in landfills or incinerated, more greenhouse gasses are produced which leads to atmospheric pollution.

People who live near such waste dumping yards, or work in waste management are deeply affected by it. They are prone to infections and blood diseases. Over the years, improper waste management has been the even cause death.

Moreover, recent studies prove that often governments have to spend a lot of money (definitely more than the amount spent on waste management) to counter the threat and effects of improper waste segregation.

This is why accurate waste segregation is very important. It saves nature on a whole from getting in harm's way. It also saves us humans from a lot of vulnerabilities and definitely gives us a prettier version of the earth, to live in.

Now, the waste segregation is at the individual's discretion. Every individual is supposed to segregate the waste into dry, wet and plastic; and dispose it on days assigned to that particular type of waste. This system of waste management has rules and fines to ensure its implementation. The large organizations are the ones who fall prey to this system. Nobody takes responsibility for that, causing utmost of financial loss to the organization. Even at an individual level, urgent engagements and practically any other activity holds more importance that segregating waste in our society. Since all has been tried and tested, with not much output, we intend to make the entire segregation process automatic and real time.

II. RELATED WORK

The works related to our projects are as stated below:

A. Automated Recycling System Using Computer Vision - Desi Tomaselli (ECE-498: Capstone Design Project) [4]:

The author has designed a segregation system which comprises of an IR proximity sensor, a motor, 4 containers (glass, metal, paper, plastic) and the classification system used is KNN (k- nearest neighbor) algorithm deployed on a Raspberry Pi 3 Model B. Once the object enters the system, the classifier system classifies the object held in the waiting compartment. The images taken from the camera, are fed into the model and are classified (into glass, paper, metal, plastic) based moves in a certain direction depending on the classification done and the object falls into the respective container.

B. Trash Classifier using Image Processing [20]:

The author has used a conveyer belt, magnets, bins, raspberry pi processor for the waste segregation process. Raw garbage is loaded on the conveyer belt. In the initial stage, the magnet grabs all the metallic scraps and puts them in a separate bin. Next the garbage is queued in order to restrict the amount of trash entering the image acquisition module. The Raspberry Pi processor gets the image captured by the camera in image processing and acquisition module. The image is then sent to the unit which trained using an algorithm. The classification data is then sent back to Raspberry Pi, which guides the conveyor flap to tilt and direct the garbage into the respective bins (organic wastes, papers, plastics, and non-magnetic metals).

C. Intelligent Garbage Classifier [2]:

The author has built a system that possibly can visually classify and segregate different types of waste in an effective manner using various latest technologies like computer vision, robot control and others.

D. Intelligent Waste Separator [3]:

The author has designed a system which can segregate inorganic and other kinds of waste. The topics of main significance are image processing, computer vision, machine learning, pattern recognition, embedded systems, and circuit design. Although this system doesn't resolve the trash issue, it gives a solution for simplifying the waste segregation process and also reinforcing environmental culture.

E. Classification of Trash for Waste Classification Data

The author devised a classification scheme where trash could be classified into various categories using machine learning and computer vision algorithms. The report showed that in order to create a more accurate system, there is a requirement for a large and continuously growing dataset.

III. METHODOLOGY

A. Proposed system:

The proposed solution is an Automatic Waste Segregator, “The Autowastagator”. The Automatic Waste Segregator will be built using an Image Classification model using the ResNet algorithm. The model will be built on a Waste Images Dataset procured from different resources in order to increase the accuracy and efficiency of the model. The following table comprises of the resources from which the data is collected and the three categories they are divided into:

Table 1: Dataset Collection

SL.NO.	CATEGORY	RESOURCES
1.	Wet	The train and test dataset of the Organic data of Kaggle Waste Classification Data, Google Images, other Images from the internet
2.	Dry	The train and test dataset of the Recyclable data of Kaggle Waste Classification Data (non-plastic component), train and test dataset of Gary Thung and Mindy Yang's waste dataset (cardboard, glass, metal, paper and trash components), Google Images, other Images from the internet
3.	Plastic	The train and test dataset of the Recyclable data of Kaggle (plastic component), train and test dataset of Gary Thung and Mindy Yang's waste dataset (plastic component), Google Images, other Images from the Internet

The data collected is then trained and tested and a model is created. The input to the model will be a video input where the video comprises of trash being thrown. As already mentioned as the target audience will be members of an organization, there is a high probability only one trash is thrown at a time which is then recorded by a webcam and then the waste category classification is done. At the end of the process a report is generated comprising of the details of the number of images (obtained from video stream) of each category of waste disposed.

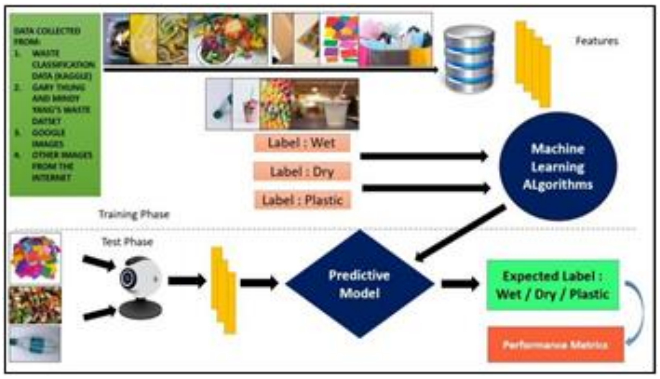

DATA COLLECTED FROM:
1. WASTE CLASSIFICATION DATA (KAGGLE)
2. GARY THUNG AND MINDY YANG'S WASTE DATSET
3. GOOGLE IMAGES
4. OTHER IMAGES FROM THE INTERNET
Features
Label : Wet
Label : Dry
Label : Plastic
Machine Learning ALgorithms
Training Phase
Test Phase
Predictive Model
Expected Label : Wet / Dry / Plastic
Performance Matrics

Figure 1: Architecture of Algorithm

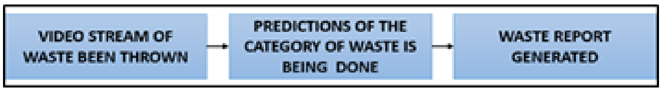

VIDEO STREAM OF WASTE BEEN THROWN
PREDICTIONS OF THE CATEGORY OF WASTE IS BEING DONE
WASTE REPORT GENERATED

Figure 2: Project Flow

Proposed System:

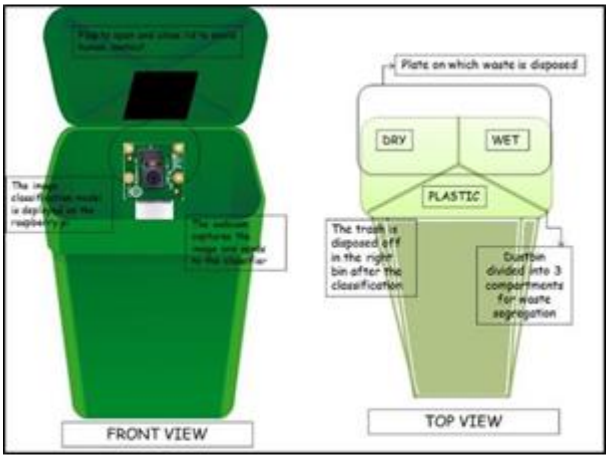


Plate on which waste is disposed
DRY
WET
PLASTIC
The trash is disposed off in the right bin after the classification
Dustbin divided into 3 compartments for waste segregation
FRONT VIEW
TOP VIEW

Figure 3: Proposed Design of Dustbin

The real-life implementation of the proposed system could include the classifier being deployed on a Raspberry Pi board. The dustbin is internally divided into three bins. All three bins are covered by plates which form the common base where the trash falls. The Raspberry Pi (with the camera connected to it) will then detect the category of waste thrown and the corresponding plate opens and the trash falls into the right bin

C. Multi Factor Authentication

Over the last few years Multi-factor authentication has gained a lot of traction. Other thanks the traditional password authentication there are six other different types of methods of application namely, retina scans, security tokens, fingerprint recognition, voice recognition, facial recognition and gesture-based authentication. This paper will also focus on how the combination of these authentication factors can be utilized to secure access to smart things.

The table 1 provides an overall view of the various authentication mechanisms. It also includes usability which depends on four factors namely, Speed, efficiency, learnability and memorability. Each authentication factor will be categorized based on the four factors. From a user's perspective, the speed and efficiency of facial recognition is medium and the learnability and memorability is categorized as easy. These values are assigned considering that the fact that the user doesn't have to remember any text in order to authenticate himself but the facial recognition system takes time to recognize and sometimes falters owing to next factor, password or pin authentication, this authentication takes place faster as the system would recognize them faster as it is already present in the database but the user will have to remember the same. As there are a number of restrictions imposed on password creation memorability factor further aggravates due to inability of many users to remember them over a time period. Thus, in conclusion the speed is categorized as fast and efficiency is termed as good but learnability and memorability are categorized as medium.

Moving onto fingerprint recognition, this form of authentication is found to be leading in all the usability factors owing to the facts that the user doesn't have to remember anything as well as the system can easily recognize the user with utmost speed and efficiency. Let us now take into consideration gesture recognition. The efficiency of the authentication process will be on the higher end. Both the system has to be configured and the user will have to learn the gesture and remember it for a certain time period. Thus, fingerprint recognition and gesture recognition are categorized as medium. Location based authentication comprises of a combination of multiple forms of authentication, that is, fingerprint and facial recognition. This is because the user first needs to be provided authenticated access to enter and then further location details are accessed to verify the identity of the user. Thus, taking into consideration all factors location-based authentication is termed as medium. Thus, as we have arrived at some reasonable conclusion with respect to these authentication factors, utilizing the measurements of speed, efficiency, learnability and memorability we can combine different factors of authentication to secure the IoT network of the AWS.

Table 2: Analysis of Authentication Methods

D. Next Generation Firewall

The matching criteria is based on execution of regular expression against IP packet headers in the currently used firewalls. From the monitored traffic, the network IDS and IPS have capability to extract insights. With the utilization of next-generation firewall, the advance machine learning techniques can be used to analyse packets and build predictive models which can be used to predict abnormal behaviours of unforeseen traffic. This technology can be designed to be a plug-in IDS/IPS. Enhancement and dynamic updating of firewall rules can be done using this system.

IV. RESULTS

The accuracy of the classification system has been improved by addition of dataset. The proposed solution is expected to have an accuracy rate of above 93%. At the end of the process a waste classification report is generated comprising of the details of the images (obtained from video stream) of each category of waste disposed. The waste classification report provides information regarding the quantity of waste, percentage of contaminants found and so on which will help us figure out ways to reduce the production of such waste and how to dispose them in a safe manner. The IoT network security has been improved with the utilization of multi factor authentication and next generation firewall, making the data secure and safe to use by the users.

V. CONCLUSIONS

The Automatic Waste Segregator has an improved efficiency and better accuracy. The components multi-factor authentication and next generation firewall further improves the security features of the IoT network. It is evident that the waste segregation process is done with very less human effort, in an effective and eco-friendly way, thereby reducing risks of pollution or emission of hazardous pollutants.

VI. CONCLUSION

- The tensile test showed very good load bearing capacity for the 0/90 ° direction with a peak load 1600N.
- The peak load for +45°/-45° was around 2000N.
- The laminates showed good results in both the cases. Also, the strength of the fiber is higher in longitudinal direction than that of transverse.
- The results give scope for the application of these natural fibers in interior of automobiles.
- The addition of mango particles have given improved results in tensile strength compared to the results with only banana fibres.
- The work can be extended by increasing the number of layers and varying the percentage of fibres.

VII.REFERENCES

[1]. J Sanjai1, V Balaji2, K K Pranav3 B. Aravindan4, "AUTOMATED DOMESTIC WASTE SEGREGATOR USING IMAGE PROCESSING" International Research Journal of Engineering and Technology (IRJET)

[2]. Alvaro Salmador, Javier Pérez Cid, Ignacio Rodríguez , "Intelligent Garbage Classifier", International Journal of Interactive Multimedia and Artificial Intelligence,

[3]. Vol. 1, Nº 1, ISSN 1989-1660

[4]. Andres Torres-García, Oscar Rodea-Aragón, Omar Longoria-Gandara, Francisco Sánchez-García, Luis Enrique González-Jiménez ," Intelligent Waste Separator", Jesuit University of Guadalajara, Department of Electronics, Systems and IT (ITESO),

[5]. Mexico, ISSN 2007-9737

[6]. Desi Tomaselli ," Automated Recycling System Using Computer Vision", ECE-498 Capstone Design Project

[7]. Mindy Yang and Gary Thung, "Classification of Trash for Recyclability Status [online] Available: http://cs229.stanford.edu/proj2016/report/ThungYang ClassificationOfTrashForRecyclabilityStatus-report.pdf

[8]. Kaliappan S, Ramprabu J, B. Karunamoorthy, A. Ezhilarasi," Implementation of Embedded system based Raspberry Pi for Hi-Tech Green India", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-2S2 December, 2018

[9]. Uppugunduru Anil Kumar1, B. Renuka2, G. Kiranmai3,

[10]. G. Sowjanya4," AUTOMATIC WASTE SEGREGATOR USING RASPBERRY PI, International Conference on Emerging Trends in Engineering, Science and Management.

[11]. WasteBot - https://github.com/Harshulagarwal/WasteBot

[12]. "How to build an image classifier for waste sorting", https://towardsdatascience.com/how-to-build-an- image-classifier-for-waste-sorting-6d11d3c9c478

[13]. Waste Classification - https://medium.com/bbm406f19/week-1-waste- classification-dde0aaf12ccb

[14]. "Classify waste category from images" - https://www.kaggle.com/c/waste-classification

[15]. Kaggle dataset - https://www.kaggle.com/techsash/waste-classification- data

[16]. "Automatic Classification of solid waste using Deep learning" - https://link.springer.com/chapter/10.1007/978-3-030- 24051-6_83

[17]. "SmartWasteSegregation- https://github.com/AashiDutt/SmartWasteSegregation

[18]. "Watson waste sorter" - https://github.com/IBM/watson-waste-sorter : "Waste Management system using IoT–based machine learning in university" - https://www.hindawi.com/journals/wcmc/2020/613863 7/

[19]. Waste segregator - https://github.com/boudhayan-dev/Automatic-Waste-Segregator

[20]. "Waste classifier" - https://github.com/KhazanahAmericasInc/waste- classifier

[21]. Trashcam – https://github.com/yaoharry/Trashcam

[22]. Trash Classifier using Image Processing: https://veltech.edu.in/international/visai19/uploads/VIS AI19-PROPOSAL%20REPORT.pdf

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Lie Detection Using Facial Micro- Expresions (September 2020)

Ritom Tamuli, Srutibanta Samantara, Shubhodeep Sarkar, Sourav Adhikari

Information Science & Engineering, Bangalore, Karnataka, India

ABSTRACT

In many fields, such as airport management, criminal inquiries, counterterrorism, etc., identifying lies is key. We can't go to the people in this area requesting for a practical lie detection test as it takes a hard task which takes a lot of time. An evergreen and changing topic has been Lie detection. The most common and effective approach to date has been polygraph techniques. The biggest downside of the polygraph is that it is difficult to obtain successful outcomes without establishing physical interaction with the person under investigation. This physical touch will usually trigger additional attention in the subject. One way of identifying lies is to recognize facial micro- expressions, which are small, spontaneous expressions seen on the face of individuals as they attempt to hide or repress emotions. So, our goal is to use facial micro- expressions to build and improve a lie detection system. The system's primary goal is to target the slight changes that occur in the face when someone is tricky and deceptive.

Keywords :- Lie detection, micro expressions, Emotions, Expressions

I. INTRODUCTION

Lying is an act of disrespect and would have cost a lot in any aspect of life, whether in personal or professional life. So the evaluation of a verbal statement with the purpose of exposing a potential deliberate deception. Lie identification is commonly referred to as a polygraph. A polygraph is a mechanism that tests different factors, such as breathing, blood pressure, heartbeat and sweat, which are used as hints in the calculation of lies. The downside of the polygraph is that it causes false positives when the person under examination is nervous or emotionally excited. Lie Identification is of the utmost importance, particularly in areas such as security, crime, interpersonal relationships, and may result in highly disastrous outcomes if undetected. Manual estimation of lie detection is hard work, time consuming, and unreliable. So here we are going to use facial features to present a lie detector.

Emotions play a very influential and purposeful role in daily life. Emotions show the exact emotions of an individual at any given moment. Emotions play a crucial role in the process of identifying lies, are more accurate as emotions are common and do not change with caste, community, creed, faith and the region. At every given moment, the feeling felt by a human can only be normal, effected by the environment. Thus, in contrast to manual labor, the odds of identifying specific details are high.

The 80 muscular facial contractions of a person and their variations give birth to thousands of gestures. Seven fundamental emotions, such as rage, disgust, terror, satisfaction, surprise, sorrow and contempt, are grouped into a single class of expressions. Contempt is an emotion that has been added to the list of common emotions lately. As of now, six basic emotions (with neutral expression) are restricted to the analysis in hand, leaving behind distrust.

Present day lie detectors, such as polygraph examination, are very powerful thermal cameras that measure minute shifts in the face temperature of the person. This paper explores an accessible, cost- effective and minimally - intrusive model.

II. RELATED WORK

We give a short background of micro-expressions and a review of similar studies in the field of psychology. We also provide for a study of preceding studies on actuated micro-expressions. For a more detailed overview of the relevant studies on facial expressions, we direct the reader to Zeng et al. survey [19]. In the study of facial gestures, the primary objective has been on identifying six specific emotions and having facial action unit marking using FACS. Few efforts within computer vision exist to examine more complicated facial expressions. In social psychology, nevertheless, micro-expressions as a dynamic mode of facial expression have been extensively researched by Guttmann [8] and Ekman [4]. Ekman initially noticed the presence of facial micro-expressions when he looked at a recording of a mental patient attempting to mask a plot to commit suicide. By studying the video in slow motion, Ekman found a very brief gesture of deep anguish, which was eventually replaced by a grin. Since these gestures are very quick, they are undoubtedly overlooked through natural monitoring. Micro-expressions were later first-hand found in social studies [17] and preparation programmers for studying to observe them were developed [4]. Studies of micro- expressions in psychology clearly indicate that people are inherently poor to understand micro-expressions. Frank et al.[5] carried out a micro expression identification trial for real-life videos and discovered that U.S. undergraduates and coast guards had a precision of 32 per cent and 25 per cent without experience, and 40 per cent and 47 per cent without experience, respectively (with a chance of 20 per cent), with very poor perfect amounts of observation. Many facial expression experiments till date use a research body composed of people acting on facial expressions. They have been shown to vary greatly from the normal facial gestures that exist in daily life [1]. As anticipated, the emphasis is now turning towards the use of induced and inherent data for research [10]. These details are more complex to work with, as they require greater entitlement to communication and thus less authority over monitoring environments. Few computer vision research on the identification of facial micro-expressions have implemented acted data, but none of the research have made their results publicly accessible. Polikovsky et al. [13] obtained figures from 10 university students who conducted micro- expressions and implemented gradient orientation histogram descriptors. Likewise, Shreve et al. [14, 15] recorded 100 active facial micro-expressions from an undisclosed number of volunteers and used tension patterns for classification of the features. Example recordings with micro-expressions have been revealed and asked to imitate them. Micro-expressions, however, are spontaneous by psychological study [4] and cannot be extracted by behaving. Not unexpectedly, Shreve et al. [14] recorded chance validity (50 per cent) while trying to test their classifier on 24 random micro-expressions in the Canal-9 political debate corpus. While the weak outcome could be partially accredited to head man oeuvre and voice, it is obvious that a new approach and a greater unconstrained facial micro-expression compilation are required to obtain fair functional precision. In our article, we introduce both a considerably greater corpus of random facial micro-expressions and a process that triumphs in categorization. More diverging similar efforts incorporates Michael et al.[11], who suggested a system for automatic detection of deceit using body gestures. While the authors scantily discuss micro-expressions, no review of their frequency in the training data is mentioned. Numerous effective facial expression detection techniques till date have included the use of spatial-temporal local texture descriptors. An example of such a texture descriptor mentioned as LBPTOP, which freshly provided state-of-the-art findings in facial expression scrutiny [10,20].

III. METHODOLOGY

The proposed system is a lie detector using facial-micro-expression. It is quite difficult to catch micro-expressions by human eye while interrogating suspects. But using high tech camera and machine learning applications like face recognition system and iris movement system makes our work quiet easy. For this problem we have come up with a solution which is quiet easy and logical we have tried to neglect the use of graphs and complicated algorithms. First a high tech camera is used to detect the hotspots next we will find the coordinates of the hotspots and assign counters to those coordinates and keep some value for the counters when there is any kind of movement in those hotspots we decrease the counter by one, and another variable is introduced by allocating some value to it and then the sum of all the coordinates is calculated if the sum is less than the variable the most probably the suspect is lying.

• FACE RECOGNATION

A facial recognition device is a technology capable of recognizing or verifying a person using a digital image or a video image from a video source. There are several ways in which facial recognition systems operate, but they typically work by matching selected facial features from a given image with faces in a database.[23]
The Face Recognition technology is used for security purposes. The Face Recognition Device should be able to recognize a face in a picture automatically. This involves extracting the features and then remembering it, regardless of lighting, voice, illumination, ageing, transformation (translate, rotate and scale image) and posture, which is a difficult task.

A variety of considerations need to be taken into consideration in order to create a useful and usable facial recognition system.[23]
1. The average speed of the device from detection to detection should be appropriate.
2. The accuracy of this should be high

Face Recognition Methods

In the early 1970s, facial recognition was viewed as a 2D pattern recognition problem. Distances between important points were used to distinguish recognized faces, e.g. to measure distance between eyes or other important points, or to measure various angles of facial components. However, it is important for the face recognition systems to be fully automatic. Face recognition is such a daunting but fascinating topic that it has attracted researchers of diverse backgrounds: psychology, pattern recognition, neural networks, computer vision, and computer graphics. The following methods are used to face recognition.

1. Holistic Matching Methods
2. Feature-based (structural) Methods
3. Hybrid Methods

1.Holistic Matching Methods: In a holistic approach, the entire face area is taken into account as input data to the face catching process. One of the best examples of holistic approaches are Eigen faces (the most commonly used approach for facial recognition), Principal Component Analysis, Linear Discriminant Analysis and Independent Component Analysis, etc.[24]

I. 2.Feature-based (structural) Methods: Feature points such as eyes , nose and mouth are first extracted in this process and local statistics (geometric and/or appearance) are fed into a structural classifier. A major challenge for feature extraction methods is the "restore" feature, which is when the device attempts to recover features that are invisible due to broad variations, e.g. the Pose header when we match a front image with a profile image.[24]

Hybrid Methods: Hybrid facial recognition systems use a mix of both holistic and feature extraction approaches. In general, 3D images are used in hybrid approaches. The representation of a person's face is captured in 3D, allowing the device to observe the curves of the eye sockets, for example, or the shapes of the chin or forehead. Even a face in the profile will serve because the machine uses depth and a measuring axis, giving it enough details to create a complete face. The 3D method typically proceeds as follows: detection, position, measurement, representation and matching. Detection-Capture of a face either by scanning a photograph or by photographing a person's face in real time. Position-Determination of the position, size and angle of the head. Measurement- Assigning measurements to each curve of the face to create a prototype with a particular emphasis on the outside of the eye, the inside of the eye and the position of the nose.[24]

• LIES, EXPRESSIONS AND EMOTIONS

To recognize the language of the body and micro-expression. We first need to establish the baseline on how someone behaves when lying before going on to this initiative. Some of the approaches are from watching the body language, the sound of the voice of a person has an incredible impact when a person is untruthful that he sometimes becomes upset and his sound becomes strong. There are also ways to identify whether someone is untruthful [27]

It is not possible to decide what feelings are read from facial expressions, according to Paul Ekman.[28] According to Paul Ekman it is not enough to determine what emotions are read from facial expressions.it is also crucial to discover whether the interpretation of the observation are correct or not.. Facial gestures and thoughts are universal, and experiments and research have said that facial expressions can be interpreted correctly.[28] Basically, there are seven facial micro expressions of surprise, pleasure, disgust, sorrow, terror, and rage, and all these feelings display any change in expression, some of which are easy to observe while others are minute.[31]

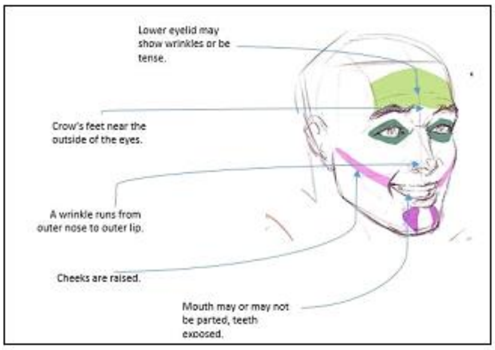

Lower eyelid may show wrinkles or be tense.
Crow's feet near the outside of the eyes.
A wrinkle runs from outer nose to outer lip.
Cheeks are raised.
Mouth may or may not be parted, teeth exposed.

Figure 1: Happiness Micro-expression

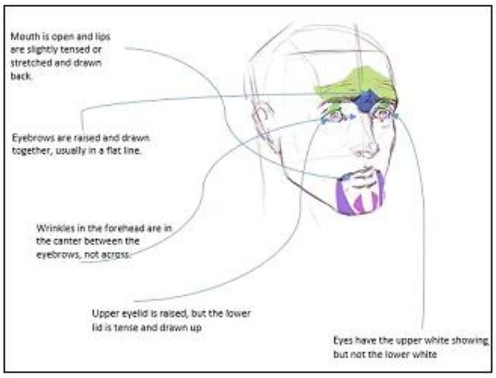

Mouth is open and lips are slightly tensed or stretched and drawn back.
Eyebrows are raised and drawn together, usually in a flat line.
Wrinkles in the forehead are in the canter between the eyebrows, not across.
Upper eyelid is raised, but the lower lid is tense and drawn up
Eyes have the upper white showing but not the lower white

Figure 2: Fear Micro-expression

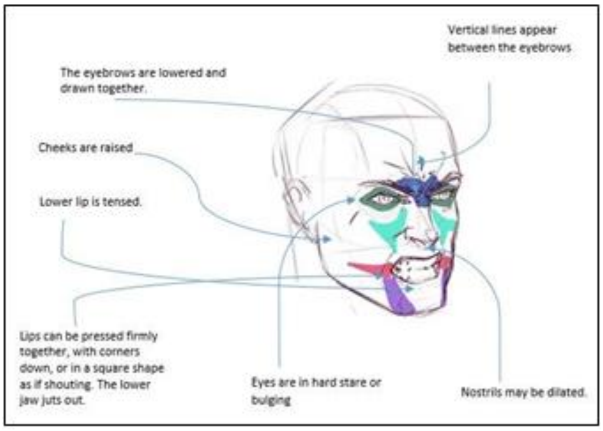

Vertical lines appear between the eyebrows
The eyebrows are lowered and drawn together.
Cheeks are raised
Lower lip is tensed.
Lips can be pressed firmly together, with corners down, or in a square shape as if shouting. The lower jaw juts out.
Eyes are in hard stare or bulging
Nostrils may be dilated.

Figure 3: Anger Micro-expression

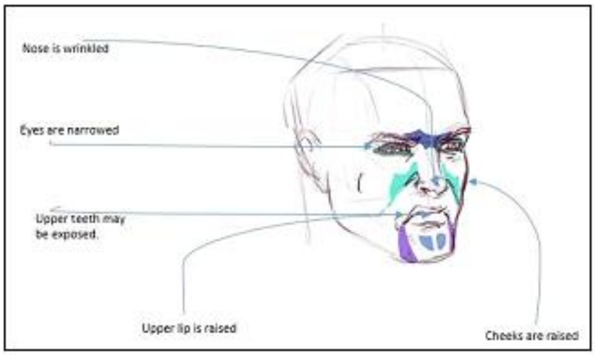


Figure 4: Disgust Micro-expression

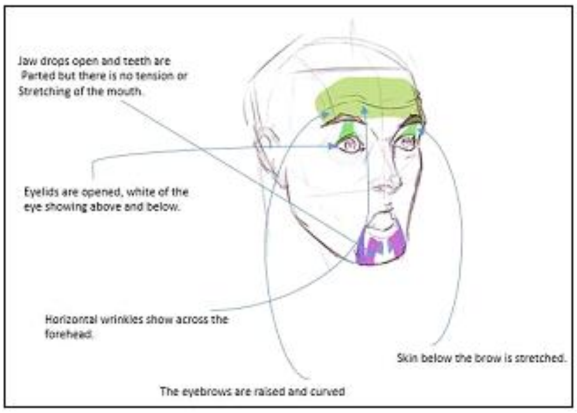

Jaw drops open and teeth are Parted but there is no tension or Stretching of the mouth.
Eyelids are opened, white of the eye showing above and below.
Horizontal wrinkles show across the forehead.
Skin below the brow is stretched.
The eyebrows are raised and curved

Figure 5: Surprise Micro-expression

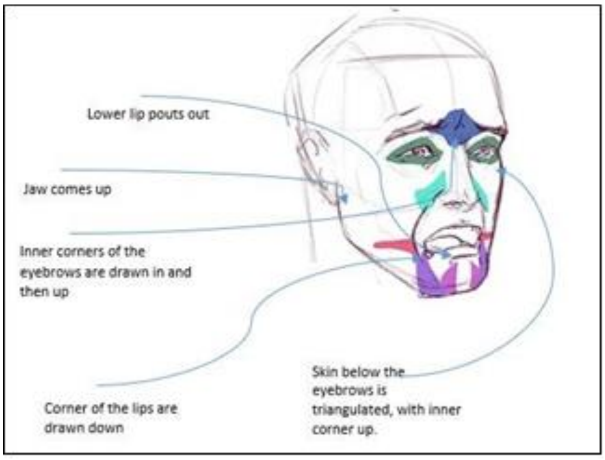

Lower lip pouts out
Jaw comes up
Inner corners of the eyebrows are drawn in and then up
Corner of the lips are drawn down
Skin below the eyebrows is triangulated, with inner corner up.

Figure 6: Sadness Micro-expression

The Equivocator’s Face

- No matter the person, there are seven fundamental feelings that are hard-wired: pleasure, sorrow, disgust, terror, disappointment, rage and contempt. Any of these feelings is reported in very different patterns that are almost impossible to falsify. For only one-fifteenth of a second, micro-expressions of these feelings can leak out. They are a struggle to spot, but it is extremely beneficial to learn to spot these flickering feelings. [30]

Figure 6: Sadness Micro-expression

Based on the form of questions posed when interrogating a suspect, behaviour indicates improvement. The facial expression of a human says a lot about a person's current behavioural condition.[28] There are several ways to identify when the offender is being untruthful movements such as sudden frustration, people also appear to get agitated when lying or the same question is frequently asked, There is a rapid shift in the body language of the defendant when interrogating, twitch of hands and blinking of eyes is often detected, but there are kinds of movements that can be readily detected, but there are certain kinds of micro-facial changes and motions that cannot be noticed when interrogating. There have been too many experiments and numerous approaches to record these micro-facial movements have been attempted. There are, however, several facial hotspots that are likely to serve as indications, according to Kelly J. Todd, Managing Director of Forensic Strategic Solutions. Liars are like tight rope walkers whose aim, when threading their web, is to remain upright [27].

The Maximizer’s Face
- Changes in eye contact
- Tight lips
- Changes in blink rate

The Minimizer’s Face
- Facial blocking
- Hiding in their hair

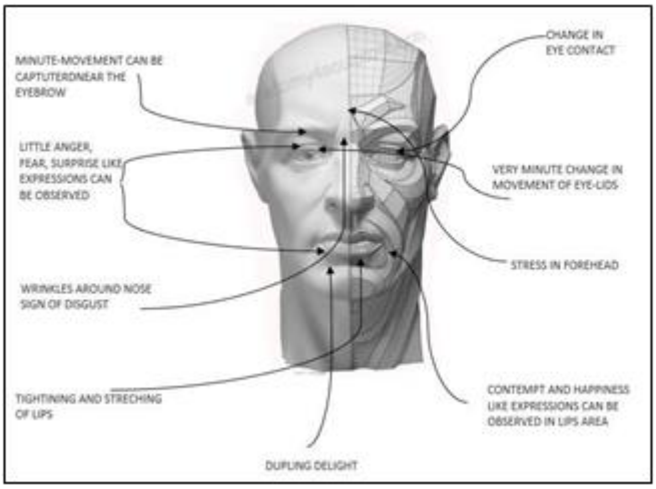

MINUTE-MOVEMENT CAN BE CAPTUTERDNEAR THE EYEBROW
CHANGE IN EYE CONTACT
LITTLE ANGER, FEAR, SURPRISE LIKE EXPRESSIONS CAN BE OBSERVED
VERY MINUTE CHANGE IN MOVEMENT OF EYE-LIDS
STRESS IN FOREHEAD
WRINKLES AROUND NOSE SIGN OF DISGUST
TIGHTINING AND STRECHING OF LIPS
CONTEMPT AND HAPPINESS LIKE EXPRESSIONS CAN BE OBSERVED IN LIPS AREA
DUPLING DELIGHT

Figure 7: different hot-spots while lying

IV. RESULTS

The frequency of micro expressions can be lower than other cues and it is quite difficult to read these expression so our model can be used to catch hold of such liars. At the end of this experiment we will be able to detect easily if the suspect is lying or being untruthful by simply detecting the micro-expressions. The technique of reading micro expressions is an art and is being studied from the time of Darwin. Now in this fast growing up world it is time that we use better techniques and methods to catch hold of such culprits. Expressions and body language are connected to the subconscious mind and to completely trick facial expression is very difficult and using high tech super speed cameras give us an extra edge against such criminal culprits.

V. CONCLUSION

Human emotion is an important subject of research in psychology on the basis of facial micro expressions. It is believed that in many places where psychological understanding is needed, such as police interrogations, airport and border checkpoints, jobs, and clinical testing, the developed method may be useful. For regular review, the Real Time Lie Detector seems very beneficial. It can be used to classify perpetrators, but cannot be used as evidence of a deception that is foolproof.

This research is not an explicit detector of lies, but it extracts micro expressions, which in turn helps to detect lies for both individuals and investigators. Micro expressions show the subject / people's real intentions. Witnessing, examining and recognizing these micro expressions will therefore intensify the process of identifying a lie, but it is a repetitive and hard job for an average individual to understand such impulsive expressions.

VI. REFERENCES

[1]. S. Afzal and P. Robinson. Natural affect data- collection & annotation in a learning context. In ACII, pages 1–7, 2009. 2

[2]. L. Breiman. Random forests. Machine Learning, 45(1):5–32, 2001. 6

[3]. T. Cootes, C. Taylor, D. Cooper, and J. Graham. Active shape models – their training and application. Computer Vision and Image Understanding, 61(1):38– 59, 1995. 3

[4]. P. Ekman. Lie catching and microexpressions. The Philosophy of Deception, Oxford University Press, 2009. 1, 2, 5

[5]. M. G. Frank, M. Herbasz, K. Sinuk, A. Keller, and

[6]. C. Nolan. I see how you feel: Training laypeople and professionals to recognize fleeting emotions. International Communication Association, Sheraton New York City, 2009. 1, 2, 7

[7]. A. Freitas-Magalh˜aes. The psychology of emotions: The allure of human face. Uni. Fernando Pessoa Press, 2007. 1

[8]. A. Goshtasby. Image registration by local approximation methods. IMAVIS, 6(4):255–261, 1988. 3 [8] J. Gottman and R. Levenson. A two-factor model for predicting when a couple will divorce: Exploratory analyses using 14-year longitudinal data.

[9]. Family process, 41(1):83–96, 2002. 1, 2

[10]. X. He, D. Cai, S. Yan, and H. Zhang. Neighborhood preserving embedding. In ICCV, pages 1208–1213, 2005. 5

[11]. S. Koelstra, M. Pantic, and I. Patras. A dynamic texture based approach to recognition of facial actions and their temporal models. PAMI, 32(11):1940–1954, 2010. 2

[12]. N. Michael, M. Dilsizian, D. Metaxas, and J. Burgoon. Motion profiles for deception detection using visual cues. In ECCV, pages 462–475, 2010. 2

[13]. T. Ojala, M. Pietik¨ainen, and T. M¨aenp¨a¨a. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. PAMI, 24(7):971–987, 2002. 4

[14]. S. Polikovsky, Y. Kameda, and Y. Ohta. Facial microexpressions recognition using high speed camera and 3Dgradient descriptor. In ICDP, 2009. 1, 2

[15]. M. Shreve, S. Godavarthy, D. Goldgof, and S. Sarkar. Macroand micro-expression spotting in long videos using spatiotemporal strain. In FG, 2011. 1, 2

[16]. M. Shreve, S. Godavarthy, V. Manohar, D. Goldgof, and S. Sarkar. Towards macro- and micro- expression spotting in video using strain patterns. In Workshop on Applications of Computer Vision, pages 1–6, 2010. 2

[17]. M. Varma and D. Ray. Learning the discriminative powerinvariance trade-off. In ICCV, pages 1–8, 2007. 4

[18]. G. Warren, E. Schertler, and P. Bull. Detecting deception from emotional and unemotional cues. J. Nonverbal Behavior, 33(1):59–69, 2009. 2, 5

[19]. S. Yan, D. Xu, B. Zhang, H. Zhang, Q. Yang, and S. Lin. Graph embedding and extensions: A general framework for dimensionality reduction.

[20]. PAMI, 29(1):40–51, 2007. 5

[21]. Z. Zeng, M. Pantic, G. Roisman, and T. Huang. A survey of affect recognition methods: Audio, visual, and spontaneous expressions. PAMI, 31(1):39–58, 2008. 2

[22]. G. Zhao and M. Pietik¨ainen. Dynamic texture recognition using local binary patterns with an application to facial expressions. PAMI, 29(6):915– 928, 2007. 2, 4

[23]. Z. Zhou, G. Zhao, and M. Pietik¨ainen. Towards a Practical Lipreading System. In CVPR, 2011. 4

[24]. http://www.divaportal.org/smash/get/diva2:83077 4/FULLTEXT01.pdf

[25]. http://csjournals.com/IJCSC/PDF7-1/23 [24]

[26]. https://arxiv.org/ftp/arxiv/papers/1403/1403.0485.pdf

[27]. Polygraph as a Lie Detectorhttp://en.wikipedia.org/wiki/Polygraph

[28]. Gautam Krishna , Chavali Sai Kumar N V , Bhavaraju Tushal , Adusumilli Venu Gopal , research paper, BLEKINGE INSTITUTE OF TECHNOLOGY AUGUST,2014

[29]. https://time.com/5443204/signs-lying-body-language-experts

[30]. Paul Ekman's research paper on detecting micro expressions

[31]. https://www.cbc.ca/natureofthings/features/the-seven-universal-emotions-we-wear-on-our-face

[32]. Forensic strategic solution detecting deception facial expression

[33]. https://www.scienceofpeople.com/microexpressions/

[34]. https://www.youtube.com/watch?v=rGhOuA3rr1k - micro expressions in 4K by Patry Wezowiski-2041.

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Personalized Web Search: A Review

Dr. Avinash S. Kapse[1], Sushama Bhandare[2], Dr. Arvind S. Kapse[3]

[1]Ph.D. (CSE), M.E.(CSE), B.E.(CSE), Diploma (CT), Head of Department & Assistant Professor Department of Information Technology, Anuradha Engineering College, Chikhli.

[2]Student Department of Computer Science & Engineering, Anuradha Engineering College, Chikhli, Maharashtra.

[3]Professor, Information Science & Engineering Department, New Horizon College of Engineering, Bengaluru, Karnataka

ABSTRACT

This topic provides varying search systematically to each user depends upon preferences and information, for a given query. It is basic for overseeing and improving the nature of recognized administrations remembered for looking through example on the web. In any case, numerous client are a lot of made sure about sharing of information in different stage and which makes it significant snag for the wide expansion of PWS. We survey here an overall system that can sum up profiles by learning the questions while keeping up client indicated protection prerequisites. In this paper we attempt to lessen the danger of sharing of information by different undesirable sources and assists with keeping up the parity in the middle of breaking down the information and giving the information which certainly improves the intension of PWS framework and keep up the dignity of the reality.

Keywords : Log Based Method, Profile Based Method, Greedy Approach

I. INTRODUCTION

Personalization is significant for web indexes to improve client experience. It has distinctive precision level for different clients and can be redressed by utilizing various questions for various arrangement of search settings

The current answers for PWS can by and large be sorted into two kinds, to be specific snap log-based techniques and profile-based ones. The snap log based techniques are clear they basically force predisposition to clicked pages in the client's question history. Despite the fact that this way has been affirmed to perform reliably and very well, it can just work with rehashed inquiries from a similar client, which is a much limitation to its appropriateness. In profile-based techniques, it improves the hunt involvement in confounded client intrigue models got from different client profiling strategies. Profile-based strategies can be a lot of viable for practically a wide range of inquiries, yet are uneven under certain conditions.

Limitations of the existing methods:

- Previous system fails to achieve in run time profiling
- Customization of privacy of data is not feasible in existing system.
- Personalized search result need repetitions for user interaction for obtaining personalized result.

- Generally there are two classes of privacy protection problems for PWS. One class includes those parameters that treat privacy as the recognition of an individual. The other includes parameters those consider the sensitivity of the data, particularly the user profiles, exposed to the PWS server.

II. A Review of Proposed System

- We review here a some personalized web search parameters for resolving query according to user specified requirements
- By implementing two specified generalized algorithms it become easy to maximize the accuracy and minimize the information,those algorithm are GreedyDP and GreedyIL

III. Related Works

In this we will try to cover literature review. It mainly taken based on profile-based personalization and privacy protection in PWS system. Many attempts have been made to find the accuracy parameters but the best way is to generalize the general interest of the user. For example, while creating the profile any host need to verify the details of customer for creating the user profile and also by selecting categories of interests. By this profiling method we can search the profile result of the user to the same categories.

Generalized and personal profile data is also used to search the personalized version of page rank for describing the query which is free from priorities of web search. Information about the users is also collected at query time using techniques such as relevance feedback or query refinement. PWS is also reviewed on two aspects, namely the categorization or its representation of profiles, and the accuracy of measurement of personalization. Many works build profiles in hierarchical structures due to their expressive ability, good scalability, and better efficiency. Hierarchical representation based on taxonomy of knowledge can be adopted as per the need. The useless user profile (UUP) protocol is proposed to find out or shuffle the prerequisite of the user. As a result any entity cannot profile a certain individual. A person can denote the degree of privacy protection for her/his sensitive values by specifying in the taxonomy of the sensitive attribute. Some data are maintained which while retrieving use small clicking queries for finding the data easily.

By checking content similarity between web pages and user profiles this type of personalized search is normally used. Some user recommended some typical categories of search pattern. User typical interest are explicitly specified or can be classify according to the need. Search data can be filtered and provide specific platform for searching pattern in accordance with user profiling.

IV. Technologies and environment for personalized web search

4.1 Web Search engine technology

The fundamental reason for web index is that looking through web assets from Internet and present top notch of them t o the client. Web creeping is one of the most significant tasks of the web index. Web crawler follows the assets of WWW in a robotized way or deliberate design. It duplicates the all the visited pages for looking quickly in future. Another usefulness of internet searcher is ordering which gathers and stores information to enhance the speed of data recovery for a given a pursuit inquiry.

.A large portion of web crawlers uphold full-text, normal language information, sound, video and designs moreover.

4.2 PageRank

In 1998, Larry Page and Sergey Brin who were the organizers of Google presented another connecting investigation technique named as PageRank. PageRank is a probabilistic dissemination used to speak to the probability that an individual arbitrarily tapping on connections will show up at a specific page [9]. Principle favorable position of this PageRank examination is convenience for assortments of reports of any size. One of the primary objective of PageRank is to improve the quality and versatility of search. Google utilizes extra room to store the list. This permits the nature of the inquiry to scale viably to the size of the Web as it grows.[2]

V. SYSTEM ARCHITECTURE REVIEW

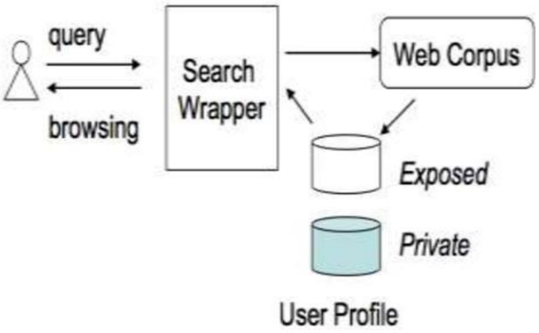


Fig 1. Personalized Query Processing Structure

Procedural Steps
1. Insert query.
2. At Server side Accept Query.
3. At Server Retrieve query list from user.
4. Generate taxonomy repository.
5. Using greedyDP,Identify sensitivity according to risk management and if yes the prun leaf
6. Using greedyIL,
7. if DP(q,G)>threshold
8. insert (t,IL(t)) into Q
9. while(risk(q,G)> threshold)
10. pop up prun leaf
11. if (t has no connections then insert (s,IL(s)) to Q
12. else if
13. merge t into shadow-sibling
14. update values for all operations
15. else
16. return root(R) as G*
17. Display result to user browser.[3]

VI. ADVANTAGES

Various behavior are creating number of problems while maintaining various profiling and due to which it creates the entry to unwanted users. Tis techniques is used to maintain the profiling in an efficient manner without any information leak and help to increase the efficiency and accuarcy in consecutive manner also the framework allows to mention specified and secured privacy requirements using hierarchical profiles

VII. DISADVANTAGES

Data collection and analysis is the most important step in PWS if this step has errors the next implementation stages will be affected to a larger extent. Mapping of the obtained results plays a vital role for user behavioral predications and hence it must be properly taken care otherwise the search process will not result in the desired output.[5]

VIII. CONCLUSION

Information assortment and examination is the most significant advance in PWS if this progression has blunders the following usage stages will be influenced to a bigger degree. Planning of the got outcomes assumes a crucial function for client social predications and consequently it must be appropriately taken consideration in any case the hunt cycle won't result in the ideal output.[5]

IX. REFERENCES

[1]. Z. Dou, R. Song, and J.-R. Wen, “A Large-Scale Evaluation and Analysis of Personalized Search Strategies,” Proc. Int’l Conf. World Wide Web (WWW), pp. 581-590, 2007.

[2]. An Overview Study of Personalized Web Search February 2013 Chanchala Joshi, Vikram University International Journal of Scientific and

Research Publications, Volume 3, Issue 1, January 2013 3 ISSN 2250-3153

[3]. J. Teevan, S.T. Dumais, and E. Horvitz, “Personalizing Search via Automated Analysis of Interests and Activities,” Proc. 28th Ann. Int’l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR), pp. 449-456, 2005.

[4]. M. Spertta and S. Gach, “Personalizing Search Based on User Search Histories,” Proc. IEEE/WIC/ACM Int’l Conf. Web Intelligence (WI), 2005.

[5]. B. Tan, X. Shen, and C. Zhai, “Mining Long-Term Search History to Improve Search Accuracy,” Proc. ACM SIGKDD Int’l Conf. Knowledge Discovery and Data Mining (KDD), 2006.

[6]. K. Sugiyama, K. Hatano, and M. Yoshikawa, “Adaptive Web Search Based on User Profile Constructed without any Effort from Users,” Proc. 13th Int’l Conf. World Wide Web (WWW), 2004.

[7]. X. Shen, B. Tan, and C. Zhai, “Implicit User Modeling for Personalized Search,” Proc. 14th ACM Int’l Conf. Information and Knowledge Management (CIKM), 2005.

[8]. X. Shen, B. Tan, and C. Zhai, “Context-Sensitive Information Retrieval Using Implicit Feedback,” Proc. 28th Ann. Int’l ACM SIGIR Conf. Research and Development Information Retrieval (SIGIR), 2005.

[9]. F. Qiu and J. Cho, “Automatic Identification of User Interest for Personalized Search,” Proc. 15th Int’l Conf. World Wide Web (WWW), pp. 727-736, 2006.

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Data Structures - A Comparative Analysis and Application in Cyber Security

K Reshma, Reem Fatima, Ria Mohan

Department of Information Science & Engineering, New Horizon College of Engineering, Outer Ring Road, Marathahalli, Bangaluru, India

ABSTRACT

Data handling in C is a pre-ordained part of programs. Computer programs often process data, so we require competent ways in which we can access or deploy data. In order to do this, we use a structure called “data structure". Data Structure is a data organization, management, and storage system that enables efficient access and amendment. Data Structures being the mainstay of every software, a good expertise over the subject is essential for all software applications under the field of cyber security. Data Structures is about interpreting data elements in terms of some association, for better organization and storage. In this paper, we'll be drawing a contrast of the various data structures that are used in the C programming language and quoting its applications in cyber security. Doing so will give us a perception on how to capitalize on the performance of a program.

Keywords : Data handling, efficient, organized, data organization, cyber security.

I. INTRODUCTION

A Data structure is a data management, organization, and storage format that facilitates efficient access and alteration. More precisely, a data structure is a set of data values, the relationships among them, and the functions that can be applied to the data.

Data structures deals with the study of how the data is organised in the memory, how effectively the data can be retrieved and manipulated and possible ways in which different data items are logically related. They represent the logical relationship that exists between individual elements of data to carry out certain tasks. [1]

Data structures can be categorized into Primitive data structures and non-primitive data structures. Further non primitive data structures can be grouped as linear data structures and non- linear data structures.

Examples of primitive data structure- int, float, char etc. Examples of non-primitive data structure- arrays, structures etc. Examples of linear data structure- arrays, lists, stacks, queues. Examples of non-linear data structure- trees, graphs.

Arrays are type of data structures that can store a fixed size sequential collection of elements of the same type.[2]

Array is used to store similar data items. Instead of declaring individual variables such as num1, num2, num3,…….numN we can declare one array variable with the same numbers and use num[1], num[2], num[3],….num[N] to represent individual variables. A specific element in array is accessed by index.

Declaring arrays:

datatype
arrayName[size];
ex. Int array[100];
Initialising arrays:

Int a[5]={23,54,67,89,43}

Accessing arrays:

An array element can be accessed by indexing array name.

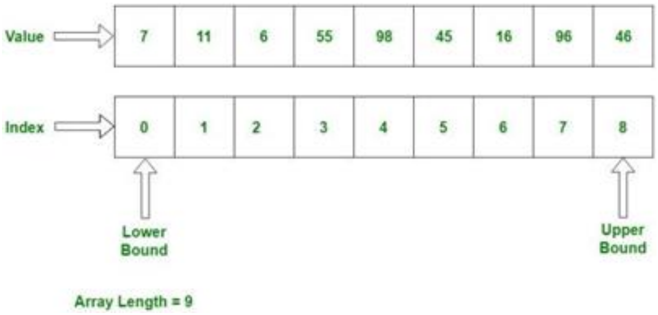


Fig. 1. Representation of an Array

A. *Stack*

A stack is a data structure which stores the elements, retrieves the elements in a sequential way using LIFO (Last In First Out) policy.

LIFO- Last In First Out means that last added element is removed first.

The insertion and deletion operations on stack are done at one end called top. The insertion operation of stack is called push and the deletion operation is called pop.

When an element is inserted into the stack, the overflow condition is checked, when an element is removed from the stack underflow condition is checked. [3]

Overflow:
top==[MAX-1]
Underflow: top==-1

When inserting element in stack, increment top value and insert the element. When removing element from stack, remove top most element and decrement the top index.

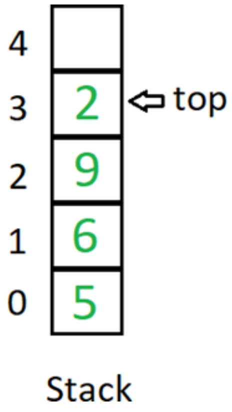


Fig. 2. Representation of a Stack

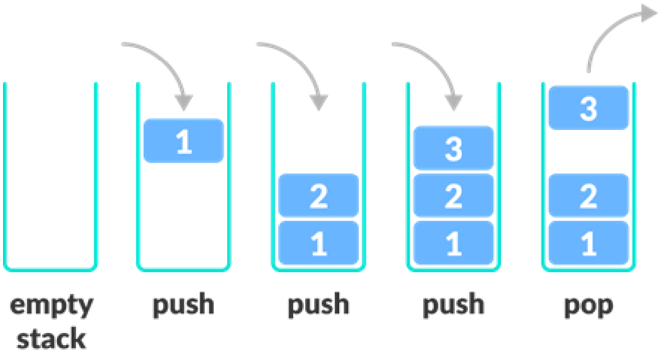


Fig. 3. Stack Operations

B. *Queue*

A queue is a data structure which stores the elements, retrieves the elements in a sequential way using FIFO (First In First Out) policy.

FIFO- First In First Out means that first added element is removed first.

The insertions in a queue are done at the rear end of the queue and the deletions are done at the front end of the queue.

The insertion operation of queue is called en-queue and the deletion operation is called de-queue.

When an element is inserted into the queue, the overflow condition is checked, when an element is removed from the queue underflow condition is checked.[4]

Overflow:
rear==arraysize
Underflow:
front==rear

When inserting element in queue, insert the element to the rear position and then increment rear value. When removing element from queue, initialize the front element to 0 and increment the front value.

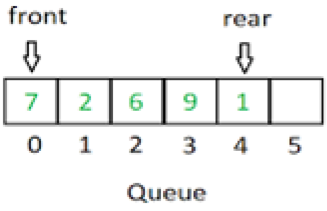


Fig. 4. Representation of a Queue

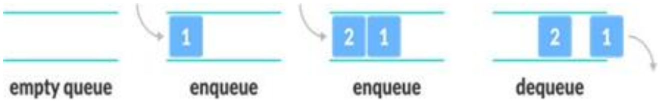


Fig. 5. Queue Operations

D. Linked List

It is a dynamic data structure which consists of non-sequential collection of data items. It is called linear data structure because of its appearance, in which elements are stored at non- contiguous memory locations but are linked to each other using pointers.

Linked list is made up of nodes. Each node consists of a data field and a reference link to the successive node.

Linked list operations involves the traversal of nodes which is done using the temporary variable.[5]

Advantages of linked list over arrays - Dynamic size and ease of insertion/deletion.

Terms involved in linked list:

Link – Each and every link can store some data called an element of the linked list.

Next – Each of the links contain a link to the next link or element called Next.

First – A Linked List as a whole contains the connection link to the first link in the list called First.

Operations supported by a linked list: Insertion – Adds an element to the linked list.

Deletion – Deletes an element from the linked list.

Display – Displays the entire list.

Search – Searches an element in the linked list using the given key.

Delete – Deletes an element in the linked list using the given key or by default.

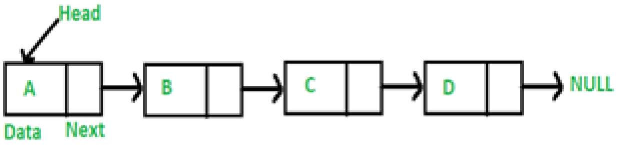


Fig. 6. Representation of a Linked List

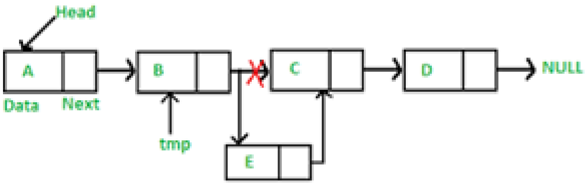


Fig. 7. Linked list Insertion operation

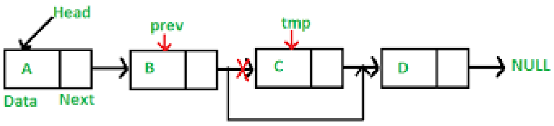


Fig. 8. Linked list Deletion operation

E. Trees

It's a structure that contains nodes which can be connected by edges. Different tree data structures allow quicker and easier access to the data as it is a non-linear data structure.

The types of trees are Binary search tree(most common), AVl tree and B-tree

In this section, we will be seeing an overview of binary search trees. Its main purpose is for data storage, however binary trees have a unique requirement; each node can only have a total number of two children, and each child can again have only two children and so on. Binary search trees fulfill the purpose of both a sorted array and linked lists.

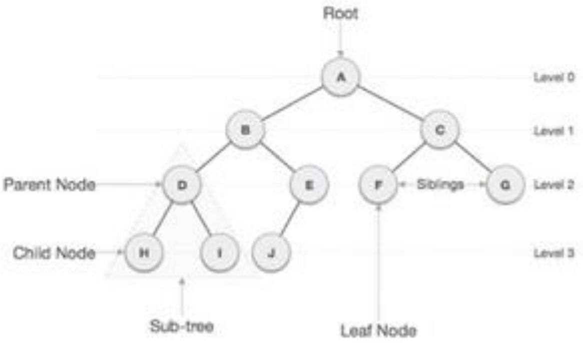


Fig. 9. Representation of a Tree Some terms used in Binary Trees:

Edge: a line connecting two nodes.

Degrees: the complete no. of branches from one node.

Root: the topmost node of tree, and only path from root to other nodes.

Parent: nodes after the root are called parents if they have sub- branches.

Child: each sub node is called a child, and their parent is that node to which they're connected to.

Leaf: if there is a node that has not even one child, it's called leaf node.

Levels: It's to show what generation of parent/child belongs to.

Sub-tree: each segment consisting of a parent and two children apart from the root node is called a sub-tree.

Traversing: methodology for searching a key element in the tree.

Key: the value that the user wishes to find in the tree.

Given a binary tree, there are 3 ways to traverse the tree and find the element the user wishes to find. The 3 operations are called; pre-order, in-order, post-order. After an insertion function is given to take in the input from the user, any of these 3 search operations are executed.

Trees Applications & Advantages:

Time complexity for a non-linear data structure is less.

All the forms of trees are used in a specific environment and it's a customizable data structure.

The stability and reliability that trees lend in terms of security is efficient!

F. Graphs

This data structure is similar to that of trees with certain complexities. Each node contains data and each edge is considered a relationship between the linked data.[6]

For example; On Facebook each element is considered a node and each node is linked, when we post a picture or upload a video onto the platform each element is a node which is connected to your profile using a link (edge).Thus every time someone establishes a node a new relationship is created.

We can write a graph data structure as an ordered pair of (V,E) where V denotes the collection of all vertices (where the nodes reside containing the data) and E is a collection of edges.

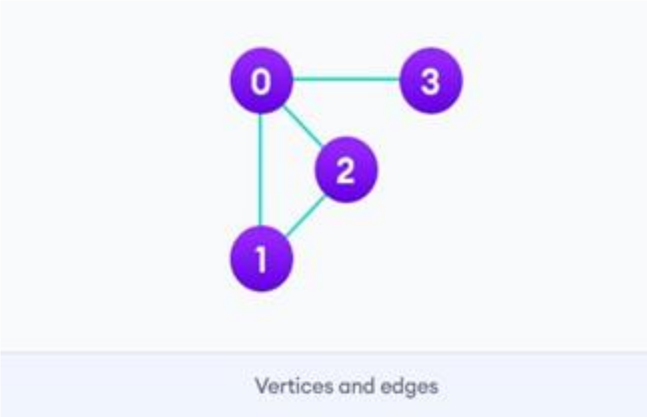


Fig. 10. Representation of a Graph In the above show graph:

V= {0, 1, 2, 3}

E= {(0, 1), (0, 2), (0, 3), (1, 2) G= {V, E}

Graph terminologies:

Adjacency: when there exists an edge that connects two vertices, they're called adjacent vertices. In the above example 2 and 3 are not adjacent.

Path: the designed set of steps that allows us to traverse from one node A to B is a path.

Graph operations:

Function to check if the element is present Traversing the given graph

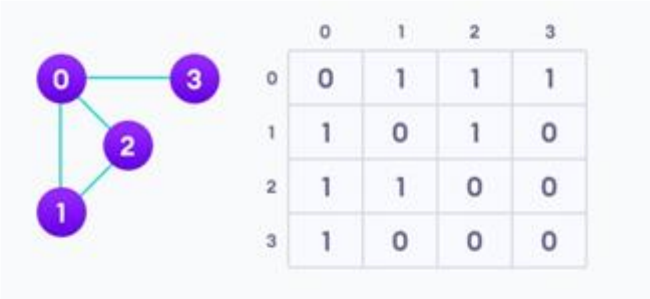
Function to add a vertex and an edge

Function to display the path between two vertices

Graph Representation:

Adjacency matrix: representation as a 2D matrix where the V*V vertices and in this matrix each row and column is denoting a vertex.

If the value of a[i][j] is returning 1, it implies that at the position i, j there is a data element present. Likewise if it returns 0 then there is no data element present.



	0	1	2	3
0	0	1	1	1
1	1	0	1	0
2	1	1	0	0
3	1	0	0	0

Fig. 11. Adjacency matrix

Adjacency list: representation of the graph as a combined array of linked lists.

The index value of the array will denote the vertex, then each element in the linked list will denote the other vertices that is forming an edge/relationship with the vertex given by the array index.

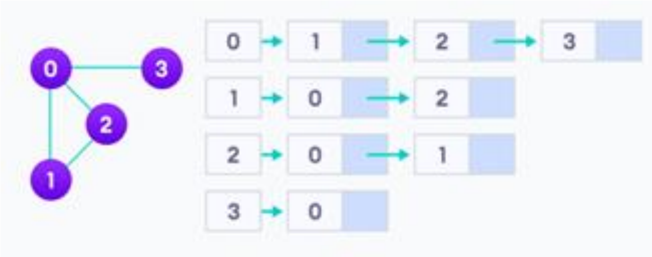


Fig. 12. Adjacency list

G. Application of Data Structures in Cyber Security

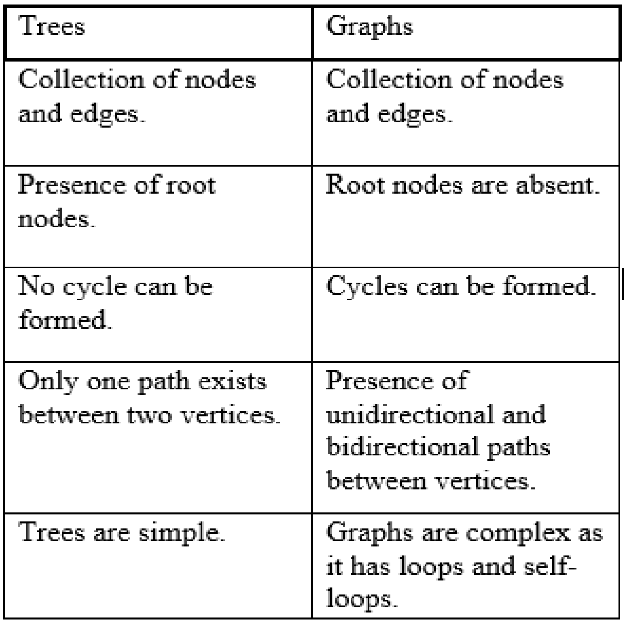
Cryptography is associated with the process of converting typical plain text into indiscernible text and vice-versa. It is a method of accumulating and transmitting data in a particular form so that only those who are authorized and intended to can read and process it. Oblivious data structures, specifically Oblivious Trees, which store relevant data and set of values at its leaves. [9] This property is attained through the use of randomization by the update algorithms.[8] Oblivious tree data structures are in specific used to decipher the privacy problem for incremental digital signatures, as part of cryptography.[10] A new skill for security has been developed which is a permutation of Caesar Cipher and graph traversal and Binary search tree collectively then security will be much more superior to only using Caesar cipher or graph traversal or binary search tree. [7]

During the process of pen testing or web application scan, one may need to understand the code that's written in order to decipher the particulars.

In many standpoints the need to write appropriate algorithms that gratify the needs within cyber security like code encryption, creating certificates, pen testing arises, and in such cases, having a profound comprehension of data structures plays a very important role.

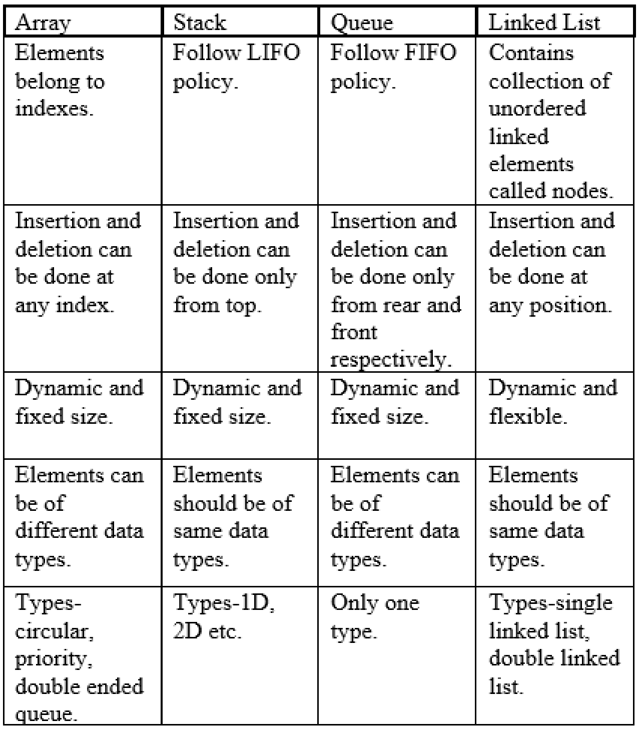
II. COMPARISON TABLES

Table 1. Comparison of Structured Data



Trees	Graphs
Collection of nodes and edges.	Collection of nodes and edges.
Presence of root nodes.	Root nodes are absent.
No cycle can be formed.	Cycles can be formed.
Only one path exists between two vertices.	Presence of unidirectional and bidirectional paths between vertices.
Trees are simple.	Graphs are complex as it has loops and self-loops.

Table 2. Comparison of Unstructured Data



Array	Stack	Queue	Linked List
Elements belong to indexes.	Follow LIFO policy.	Follow FIFO policy.	Contains collection of unordered linked elements called nodes.
Insertion and deletion can be done at any index.	Insertion and deletion can be done only from top.	Insertion and deletion can be done only from rear and front respectively.	Insertion and deletion can be done at any position.
Dynamic and fixed size.	Dynamic and fixed size.	Dynamic and fixed size.	Dynamic and flexible.
Elements can be of different data types.	Elements should be of same data types.	Elements can be of different data types.	Elements should be of same data types.
Types-circular, priority, double ended queue.	Types-1D, 2D etc.	Only one type.	Types-single linked list, double linked list.

III. CONCLUSION

For a programmer one of the most basic and important aspects to decide is; on what data structure their program will be coded in, with the change of data structure the methodology and syntax of their program will change as well.

The key lies in choosing the right data structure for their projects purpose as this will enhance the efficiency of the computer program ease in understanding syntax and stability of the whole project.

A data structure plays a vital role in Big Data Handling, Cyber Security and IOT.

The processing speed component, data search and handling multiple requests from users in a network all depend on the type of data structure used and how it is used.

Specifically in a network of users the right data structure can lead to enhanced cyber security and ensure that the data stays within the network and is stored accurately.

All in all through this paper we can conclude that a data structure is a foundational requirement in cyber security and is the support system for various other aspects of today’s modern technology.

IV. REFERENCES

[1]. Patel, Mayank. Data Structure and Algorithm With C. Educreation Publishing, 2018.

[2]. Bachman, Charles W. "Data structure diagrams." ACM SIGMIS Database: the DATABASE for Advances in Information Systems 1, no. 2 (1969): 4-10.

[3]. Kruse, Robert, and C. L. Tondo. Data structures and program design in

[4]. C. Pearson Education India, 2007.

[5]. Kruse, Robert, and C. L. Tondo. Data structures and program design in

[6]. C. Pearson Education India, 2007.

[7]. Sleator, Daniel D., and Robert EndreTarjan. "A data structure for dynamic trees." Journal of computer and system sciences 26, no. 3 (1983): 362- 391.

[8]. Hoel, Erik G., and Hanan Samet. "A qualitative comparison study of data structures for large line segment databases." In Proceedings of the 1992 ACM SIGMOD international conference on Management of data, pp. 205-214. 1992.

[9]. Forouzan, Behrouz A. Cryptography & network security. McGraw-Hill, Inc., 2007.

[10]. Stinson, Douglas Robert, and Maura Paterson. Cryptography: theory and practice. CRC press, 2018.

[11]. Wang, Xiao Shaun, Kartik Nayak, Chang Liu, TH Hubert Chan, Elaine Shi, Emil Stefanov, and Yan Huang. "Oblivious data structures." In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 215-226. 2014.

[12]. Micciancio, Daniele. "Oblivious data structures: applications to cryptography." In Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, pp. 456-464. 1997.

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Jeevan Setu : Your Life Matters

Yashmitha R, Tejal Lalji Rangani, Anushka Sen
ISE, New Horizon College of Engineering, Bengaluru, Karnataka, India

ABSTRACT

To combat the recent COVID-19 pandemic that has taken over the world, one can make use of the proposed Jeevan Setu: Your Life Matters web application. This proposed system will give real time count of the various hospital requirements to make it easier for citizens of Bengaluru to navigate. Jeevan Setu will contain two categories, both non-COVID and COVID. Accordingly, the update will be divided. It will show the real time general ward bed count, ICU bed count, doctor count of various specialization, nurse count for both the categories. It would help users to get information about their nearest hospital and allow hospitals to update the record. Help desk will also be provided in Jeevan Setu which will contain various emergency contact numbers, ambulance numbers & online links to buy masks, gloves and PPE kits. It would also display the number of active COVID-19 cases, recovered cases and death cases in Bengaluru. The users won't be able to access the hospital database or modify it, they can only view the information being displayed. Hospitals would need to register with Jeevan Setu and unique id would be given to each to ensure no ambiguity. Each hospital can access their respective database and modify it accordingly. The data would be encrypted before storing in the database to improve security, in its future enhancement. Jeevan Setu can also be used after the end of the ongoing pandemic. This is proposed to be an end-to-end web application.

Keywords: COVID-19, web application, healthcare management system, hospital database, encryption, security, unambiguous system, Bengaluru.

I. INTRODUCTION

Hospitals are designed to take and function on an average patient load.[1] In 1984, Peter Reichertz gave a lecture on the behaviour of hospital information system in the past, present and future. From then to now, there has been a marvelous development in medicine as well as in informatics.[2] The COVID-19 pandemic has made it more challenging and difficult to decide which hospital to visit for one's treatment, irrespective of COVID-19 emergency or for general health emergencies. "Jeevan Setu: Your Life Matters" is a proposed web application where solutions are provided for every query regarding hospitals and their facilities. Healthcare professionals and administrators have been confronted with several pressing challenges since the onset of the outbreak such as lack of beds, doctors being occupied with COVID-19 and general care patients, shortage of other healthcare professionals, overworked staffs, unavailability of protective gears and many more. The number of COVID-19 cases in India across all the states have widely spread as of 6th April, 2020.[3] The proposed Jeevan Setu web application displays the real time count of the various hospital facilities to make it easier for Bengaluru citizens to navigate and decide. It would provide the data segregated into two categories – COVID and non- COVID. It will show the real time general ward bed count, ICU bed count, doctor count of various specialization,nurse count for both the categories. It would enable the public to access the information of their nearest hospitals free of cost and allows the hospital to update their records.

Jeevan Setu also proposes to display the number of active COVID-19 cases, recovered cases and death cases in Bengaluru. The users will be barred accessing the hospital database or modify it. Jeevan Setu can also be used after the end of ongoing pandemic. A sample is being developed intended at assimilating supplementary data by storing clinical data so that there is easy communication of data from numerous services.[4]

II. PROPOSED METHODOLOGY

Hospital- end

1. hospital_information()
Registered hospitals with Jeevan Setu are given the permission to control and manage their data that would be viewed by the public. Information concerning bed availability, bed occupancy, beds that will be free in the near future, doctor's availability (quantitative), and price for each bed (private hospitals); for both COVID- 19 and non-COVID wards will be displayed which can be modified. All these records can be maintained and updated by one individual staff or an entire department.

2. department_information()
The data of non-COVID section is segregated department wise. Doctors' name and their specialty are listed and their active hours are dynamically restored 24/7.

User-end:

1. general_information()
At the user end, all the registered hospitals' bed availability, bed occupancy, beds that will get free in the near future, doctors' availability (quantitative), and price for each bed (private hospitals); for both COVID- 19 and non-COVID ward are displayed.

2. other_information()
Doctors' names and their specialty are listed department wise and their active hours are shown 24/7. The data of the hospitals would be displayed in the order of hospitals nearest to the user first, using Google maps making it easier for the user to navigate to the nearest hospital and avoid the extra time wasted in current scenario. In which patients have to travel from one hospital to another in search of beds and doctors.

Help_Desk():

There will be a help desk method in Jeevan Setu that will contain all the emergency contact details, contact numbers of ambulances and also provide links to buy protective gears such as masks, gloves etc. from.

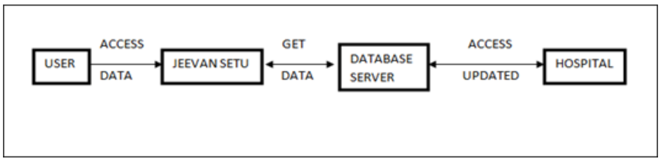


Figure1 Proposed Methodology of Jeevan Setu.

III. IMPLEMENTATION

"Jeevan Setu: Your Life Matters" is a proposed web application. This web application has broadly 2 ends- hospital end and user end.

Hospital end:

There will be a "home" page where a hospital image button will be provided. Clicking it will lead to a new login page. Any user won't be able to login through it as their unique email id and password will have to be registered & saved in the database of Jeevan Setu. Unregistered hospitals would face the same issue. The registered hospitals can login with their credentials and can maintain or modify information regarding bed availability, bed occupancy, beds that will be free in the near future, doctor's availability (quantitative), and price for each bed (private hospitals); for both COVID-19 and non-COVID wards. All of this information will be displayed on the user-end dynamically. The data of non-COVID section is segregated department wise. Doctors' name and their specialty are listed and their active hours are dynamically restored 24/7.

It would be mandatory for hospitals to register with Jeevan Setu and a unique id would be given to each to ensure security. Each hospital can access their respective database and modify it accordingly, thus disallowing any tempering of data. The data edited in the hospital side is stored in the database. The password given to registered hospitals are encrypted to prevent data ambiguity. For future implementation, hospitals can be given the opportunity to use fingerprints during login for higher security.

User end:

The "home" page would have the user login option through which people can login & view the various information provided in Jeevan Setu. At the user end, all the registered hospitals' bed availability, bed occupancy, beds that will get free in the near future, doctors' availability (quantitative), and price for each bed (private hospitals); for both COVID-19 and non- COVID ward are displayed. Doctors' name and their specialty are listed department wise and their active hours are shown 24/7. The data of the hospitals nearest to the user would be displayed first, making it easier for the user to navigate.

Help Desk:

A "help desk" icon will be provided in the "home" page where certain general information will be provided. It will contain all the emergency contacts and the links to buy the protective equipment. Also, a display of the number of COVID-19 active cases, recovered cases and death cases is given.

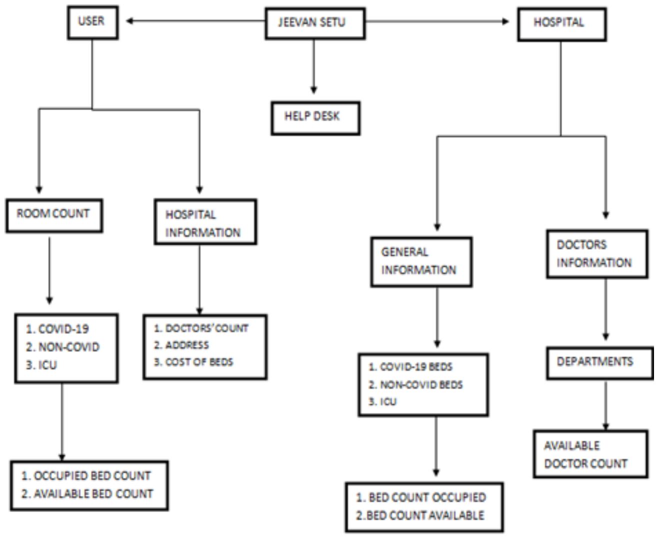


Figure. 2 : The implementation model of Jeevan Setu.

IV. CONCLUSION

The proposed system of Jeevan Setu will be a great help for the public in this tough and trying times of a pandemic. It has the possibility to boost both clinical care and administrative processes, as well as fabricating more cost-effective care and care programs across clinical disciplines and health care divisions.[5] This web application will save a lot of time that is very crucial in the moments of decision making when it's the matter of health. It will give the people an easier way to navigate hospitals around them. This web application will also be a help to the hospitals as they won't need to answer queries of the public's overwhelming demand. All the data is accumulated in one place, saving time. Jeevan Setu will also ensure security and unambiguity of data. The data provided will save time and efforts and might also save lives. This web application can also be used after the end of the current pandemic, thus making it useful in every situation. Automated medication record management system based on hospital information system can be used for future enhancement.[6]

V. REFERENCES

[1]. Brayal D’souza,Avinash Shetty,Nikita Apuri & Joaquim Paulo Moreira, “Adapting a secondary hospital into a makeshift COVID-19 hospital: A strategic roadmap to the impending crisis.”

[2]. Haux, Reinhold. "Health information systems–past, present, future." International journal of medical informatics 75, no. 3-4 (2006): 268-281.

[3]. Andrews, Robert D., and Charles Beauchamp. "A clinical database management system for improved integration of the Veterans Affairs Hospital Information System." Journal of medical systems 13, no. 6 (1989): 309-320.

[4]. Atkinson, C. J., and V. J. Peel. "Transforming a hospital through growing, not building, an electronic patient record system." Methods of information in medicine 37, no. 03 (1998): 285-293.

[5]. ZHU, Man, Dai-hong GUO, Gui-yang LIU, Shao- lai GUO, Chao CHEN, and Qi LAI. "The application and evaluation of electronic medication record management system in PLA general hospital

[6]. Chinese Journal of Drug Application and Monitoring 4 (2008).

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

RACCOON ATTACK : A Timing Attack to Leak Secret Keys

Akansha
Information Science and Engineering, New Horizon College of Engineering Bangalore, India

ABSTRACT

In today's socio-economic atmosphere one of the firmest developing areas of technical infrastructure development is the Internet. The aggregate cyber-attacks over the past decade are posing a thoughtful threat to the digital world. The paper centers around the Raccoon: The Story of a Typical Information stealer. Raccoon stealer was found in April 2o19. Raccoon is a mainstream information stealer these days on account of its low value (USD$75 every week and $2oo every month) and its rich highlights. Otherwise called "Racealer, "Racoon is used to steal sensitive and personal data which includes login credentials, credit card data, cryptocurrency wallets and browser data (cookies, history, autofill) from very nearly 6o applications. "Raccoon," the attack has been described as complex and the vulnerability is "very hard to exploit." While most clients ought to presumably not be worried about Raccoon, a few significant programming merchants have delivered patches and mitigations to ensure customers. Raccoon can permit a man-in-the-middle (MitM) attacker to break encrypted communications that could contain delicate data. However, the attack is only successful if the targeted server reuses public Diffie- Hellman (DH) keys in the TLS handshake (i.e. the server uses static or ephemeral cipher suites such as TLS-DH or TLS-DHE), and if the attacker can conduct precise timing measurements.

Keywords : Fibre reinforced composite, mechanical properties, banana fibre, biodegradable, hand layup

I. INTRODUCTION

A team of researchers has uncovered a theoretical attack on the TLS cryptographic protocol, which can be used to decrypt HTTPS connections between users and servers and to read sensitive communications. As the name implies, Rachkon portrayed the attack as "really difficult for adventure" and its hidden circumstances as "rare". "The attacker needs specific conditions for the Raccoon attack to work," the specialists composed on a site committed to the Raccoon attack. "He needs to be close to the target server to achieve high precision timing measurements. He needs the victim connection to use DH(E) and the server to reuse ephemeral keys. And finally, the attacker needs to detect the original connection."

"For a real attacker, this is a lot to ask for. However, in comparison to what an attacker would need to do to break modern cryptographic primitives like AES, the attack does not look complex anymore. But still, a real-world attacker will probably use other attack vectors that are simpler and more reliable than this attack," as they described.

The hidden weakness has existed for more than 2o years, and it was fixed with the arrival of TLS 1.3.

As we know that it is a server-side vulnerability, there is nothing that clients can do to avoid attacks, apart from guaranteeing that their web browsers don't utilize the problematical cipher suites — the current internet browsers no longer use them. Then again, the researchers have brought up that the timing measurements may not be important to introduce an attack if there is a specific kind of bug in the focused on programming.

F5 Networks, which tracks the defect as CVE-2o2o-5929, has delivered a fix. Mozilla has relegated the vulnerability CVE-2o2o-12413 and incapacitated the DH and DHE ciphers in Firefox 78, however this move was arranged before the Raccoon attack was found. Microsoft has delivered an update for Windows to address the vulnerability, and openSSL, which has allocated the issue a low severity rating, has published an advisory depicting effect and alleviations. However, even if the timing requirements are avoided, a server still needs to reuse DH keys for the attack to work. An analysis conducted by the analysts indicated that over 3.3% of the servers facilitating the Alexa top 1oo,ooo websites reuse keys.

II. A TIMING ATTACK TO LEAK SECRET KEYS

Utilizing time measurements to compromise a cryptosystem and leak sensitive data has been the care of many timing attacks, and Raccoon employs the similar methodology to the Diffie-Hellman (DH) key exchange process during a TLS handshake, which is critical to exchange information over a public network securely.

This shared secret key produced during the exchange enables secure browsing on the Internet, permitting clients to securely visit websites by ensuring the communication against eavesdropping and man-in-the-middle (MitM) attacks.

To break this security wall, the noxious party records the handshake messages between a client and server, utilizing it to start new handshakes to the similar server, and thusly estimating the time it takes for the server to react to the tasks associated with inferring the shared key.

III. ATTACK OVERVIEW

Diffie-Hellman (DH) key exchange is a focused strategy for exchanging keys on a TLS connection. When using Diffie-Hellman, two TLS peers randomly create private keys (a and b) and create their own social buttons: ga mod p and gb mod p. These public buttons are sent to TLS KeyExchange messages. once two keys are found, the client and server can calculate the shared key of the mod mod p - called premaster secret - which is used to insert all of the TLS session keys with a specific access key function.

our Raccoon attack exploits a particular TLS channel; TLS

1.2 (with all one previous variance) recommends that all leading zero bytes leading to the premaster secret are subdivided before use in other calculations. Since pre- encryption is used as an input to the acquisition key function, which relies on hash functions with various time profiles, accurate time measurements can enable the attacker to create an oracle from the TLS server. This oracle tells the attacker whether the secret of the premaster used starts at zero or not. For example, an attacker could send a gavesdrop ga sent to a client, resubmit it to a server, and then decide whether the emerging praster secret starts at zero or not.

Reading a single byte in a pre-existing secret would not help the attacker much. However, here the attack is interesting. Imagine an attacker capturing a ClientKeyExchange message that contains ga value. The attacker will now be able to create ga-related values and send them to the server with a different TLS handshake. Specifically, the attacker builds gri * ga values, leading to earlier secrets gri * b * gab. Depending on the behavior of the server, the attacker may receive values leading to

premature secrets starting with zero. Ultimately, this helps the attacker to develop a statistics collection and use the Hidden Numbers (HNP) solution to register a pre-existing secret created between the client and the server.

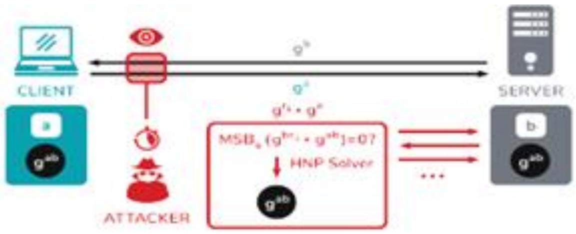


Figure 1: Raccoon attack overview. The attacker passively observes the public DH shares of a client-server connection and uses an oracle in the TLS key derivation to calculate the shared DH secret using a solver for the Hidden Number Problem.

IV. OPERATIONAL METHODS OF "RACCOON"

Let's find out how the infostealer's typical malware works as 'Raccoon'.

Raccoon is widely distributed using one of two methods:

Exploit Kits - A malicious site that displays targeted applications in any browser-based applications and directs the user to a malicious landing page. The landing page contains a code of abuse that takes advantage of the vulnerability and uses it to install malware.

Criminal data theft campaigns (Phishing Attacks) - A type of social engineering, the user is influenced by content that seems innocent to create a vicious payment burden. Usually, the victim receives an email with a Microsoft office document attachment, which contains a malicious macro. Automatically macros are disabled, so the attacker will try to persuade the user to enable macros and after that the malicious code will be applied.

A. Getting started

Most malware and especially MaaS have a C&C server to be able to retrieve data about malware options / features enabled by the attacker and send all the stolen information from the user.

The C&C server for malware is a requirement for malware operation, which is why, in order to keep it secret, malware authors retain the C&C server address in some way to keep it out of reach.

B. Stealer configuration

Like many authentication hackers, a client (e.g. invader) can customize his or her operating system suspension, which can be stored in a binary created by a malware or a C&C server, and then returned to the malware when it uninstalled. In Raccoon, after a client chooses to be suspended, a malware builder generates a client configuration ID and writes this ID to the integrated malware. In this case, the suspension ID is encrypted, Raccoon has another 64-coded encrypted cord. Encryption The configuration ID, using the first key and, after the encryption process, receives the suspension .To obtain complete suspension, the thief must query C&C. The C&C server returns the JSoN containing the required suspension. it's a duck to work

V. CAPABILITIES

Raccoon monitors the scope of applications and uses well- known techniques to extract sensitive information from those applications.

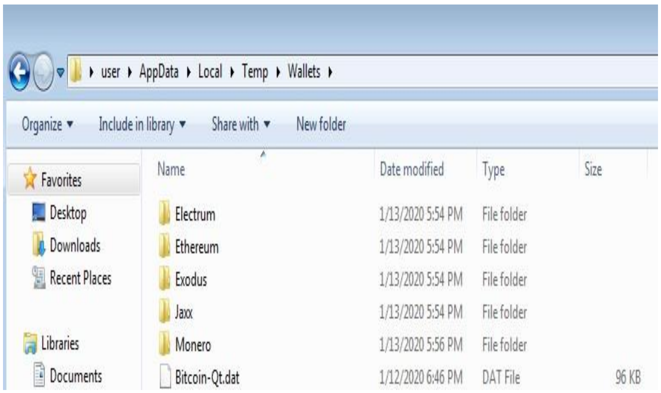
Raccoon uses the same process for each targeted application:

1. Locate the application file containing sensitive information.
2. Copy the file to its operating folder (% Temp%).
3. Create specific application routes to extract and encrypt related information.
4. Write the text file in its operating folder with the stolen dates.

To uninstall and delete data in applications, Raccoon downloads certain DLLs for applications. Config JSoN contains a URL where malware will download those libraries. Raccoon aims at 29 chromium-based programs that include Google Chrome, opera, etc. (complete list below) that have the same folder structure and share the same codebase, leading to the same way to manage sensitive data. Sensitive data in those browsers is stored in the same format as the

"Data Data" application folder containing SQLite data. Most hackers, such as Raccoon, make inquiries about SQL using sqlite3.dll to retrieve user autologin passwords, credit card data, cookies and browser history.

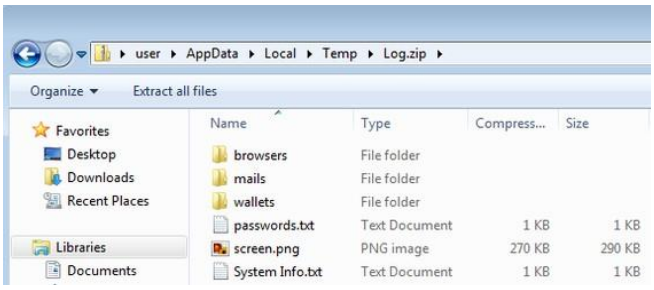
More thieves are relying on the same process for Mozilla- based apps. Since these programs have the same strategy as the folder structure, the strategies for stealing applications are the same. The big difference is the names. The thief is looking at four Mozilla-created browsers including Firefox and SeaMonkey, (full list below) and one Mozilla-based email client, ThunderBird. In those applications, the hijacker removes and writes sensitive information such as username and password, cookies and history. It is worth noting that Raccoon also supports an older version of Mozilla-based apps - it supports Firefox <32 versions, for example. To do so, Raccoon downloads a compressed file containing multiple DLLs for secure access. By using functions from nss3.dll, malware is able to encrypt and extract data from SQLite information and a JSoN log file. While searching for digital wallets, Racoon focuses on popular apps like Exodus, Jaxx and more. Like many hackers, Raccoon searches for those wallet files in the default location of the app, but it also has a wallet scan feature that allows you to find any wallet.dat file.



Name	Date modified	Type	Size
Electrum	1/13/2020 5:54 PM	File folder	
Ethereum	1/13/2020 5:54 PM	File folder	
Exodus	1/13/2020 5:54 PM	File folder	
Jaxx	1/13/2020 5:54 PM	File folder	
Monero	1/13/2020 5:56 PM	File folder	
Bitcoin-Qt.dat	1/12/2020 6:46 PM	DAT File	96 KB

Figure 1 : Stolen Wallets Folder.

Malware collects data about the machine such as oS build and version, programming language, hardware details and installed applications. Additionally, it can take screenshots on the user's machine if that is enabled by the attacker's configuration. After satisfying all its theft skills, Raccoon collects all the files and writes them into a temporary folder into a single zip file called Log.zip. Now it has to restore the zip file to the C&C server and delete all traces itself.



Name	Type	Compress...	Size
browsers	File folder		
mails	File folder		
wallets	File folder		
passwords.txt	Text Document	1 KB	1 KB
screen.png	PNG image	270 KB	290 KB
System Info.txt	Text Document	1 KB	1 KB

Figure 6: Zip File Content.

Raccoon does not use sophisticated methods to send a file back to C&C. It simply finds the C&C manager's URL (from config JSON) and Log.zip file path and sends Log.zip as it is, without encryption, using HTTP POST application.

Raccoon also has functionality to be used as a dropper, a feature that focuses on loading second-class malware download into the victim system. It downloads bad files and uses them. This is most commonly used to use other malware. In this case, the download feature is disabled by JSoN config, but when enabled, Raccoon takes the URLs from the loader_urls key, downloads the file to the temp folder and uses it at ShellExecuteA's call via file path.

VI. POTENTIAL DAMAGE & MITIGATION

This type of data theft can be very damaging to organizations and to an individuals. The attackers generally try to find out impressive details in so that they can find a rise in the right and the can perform their next movement. What is often saved by pure attackers can now be considered in any event, for beginner players who can buy thieves like Raccoon and use them to get sensitive organizational information. In addition, this goes beyond the names and passwords of users who can get instant financial benefits such as credit card data and cryptographic (cryptocurrency) wallets.

Apart from the fact that Raccoon is not the most complex and typical tool present but it is still popular among criminals and it may last to be. To prevent malicious malware theft, organizations can use the solution, including basic understanding techniques such as updating systems and applications, avoiding suspicious attachment or clicking on anonymous URLs. Ensuring that the conclusions are weak is essential to improving the overall security action of the organization.

VII. CONCLUSION

Despite the fact that the Raccoon stealer may not be the most imaginative infostealer available, it is as yet increasing noteworthy foothold in the underground network. In view of tributes from the underground network, The Raccoon group gives solid client support to give cybercriminals a speedy and-simple approach to perpetrate cybercrime without a tremendous individual venture. This has not come without difficulty. The group

has confronted a few open questions in underground discussions, and has gotten some analysis from contenders. Regardless of this, Raccoon has immediately gotten one of the main ten referenced malware in the underground network, notwithstanding being dispatched in mid 2o19. In general, feeling around Raccoon is good, with some considering it the best swap accessible for the now ancient Azorult infostealer. Raccoon's notoriety joined with its restricted list of capabilities yet high selection addresses a developing pattern of the commoditization of malware, as malware creators shoot to make stages for wrongdoing as opposed to carrying out the violations legitimately. As malware creators decide to create MaaS, they should participate in a large number of similar exercises as a real SaaS business: advertising endeavors, depending on sure surveys, responsive client care, and consistently improving highlights in their item. We just anticipate that this pattern should proceed into 2o2o and push the development of MaaS forward.

VIII. REFERENCES

[1]. https://raccoon-attack.com

[2]. Raccoon Attack: Finding and Exploiting Most- Significant-Bit-oracles in TLS-DH(E). Robert Merget, Marcus Brinkmann, Nimrod Aviram, Juraj Somorovsky, Johannes Mittmann, and Jörg Schwenk.

[3]. https://www.zdnet.com/article/raccoon-attack-allows- hackers-to-break-tls-encryption-under-certain-conditions/

[4]. https://www.thesslstore.com/blog/raccoon-attack- researchers-find-a-vulnerability-in-tls-1-2/

[5]. https://thehackernews.com/2o2o/o9/raccoon-ssl-tls- encryption.html

[6]. https://www.securityweek.com/new-raccoon-attack- can-allow-decryption-tls-connections

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Detection of Glaucoma using Convolutional Neural Network

Chethan Kumar N S, Deepak S Nadigar
Assistant Professor, Department of ECE CBIT, Kolar, Karnataka, India

ABSTRACT

Glaucoma, a very complex heterogeneous disease, is the leading cause for optic nerve-related blindness worldwide. Glaucoma is a chronic and irreversible eye disease, which leads to deterioration in vision and quality of life. it is estimated that approximately 60 million people will be affected by the year 2020. For this reason, we developed a system that automatically detects glaucoma. The objective of this research work is to carry out experiments with Convolutional Neural Networks to achieve the automatic detection of this disease. The experiments performed and obtained an average accuracy of 93%. This paper describes, the development of deep learning (DL) architecture with a convolutional neural network for automated glaucoma diagnosis. Deep learning systems, such as convolutional neural networks, can infer a hierarchical representation of images to discriminate between glaucoma and non-glaucoma patterns for diagnostic decisions. The proposed DL architecture contains Ten learned layers: Six convolutional layers and Four fully-connected layers. Dropout and Data Augmentation strategies are adopted to further boost the performance of glaucoma diagnosis. Extensive experiments are performed on the Online database of Kims Hospital.

Keywords : Glaucoma, convolutional neuronal networks.

I. INTRODUCTION

Glaucoma is one of the main leading causes of permanent blindness in the world. Is a type of chronic severe eye disease which causes by retinal changes, generally in the area of the optic nerve head(ONH)[1]. Glaucoma usually common causes of blindness, and is predicted to affect around 80 million peoples by 2020[2].It is a type of chronic disease that leads to vision loss, in which the optic nerve is progressively damaged.As symptoms only occurs when the disease is quite advanced, galucoma is also called it as a silent theif of sight.Althrough glaucoma cannot be cured, its progression can be slowed down by treatment.The main contibution of this research work is to use convolutional neural networks implemented in Tensorflow & Keras for automatic detection of glaucoma by means of analyzing pictures of the fundas of the eye.This pictures were taken at Online dataset of Kim's Hospital.These images were used for traning the CNN. The damage done by glaucoma is irreversible. Early detection and treatment of glaucoma is the only solution. A structural study is performed on selected cores of focused research outcomes for improving in near future[3].

Digital Fundus Image is one of the main and popular modalities to diagnose glaucoma. Since it is possible to acquire DFIs in a noninvasive manner which is suitable for large scale screening, DFI has emerged as a preferred modality for large-scale glaucoma screening. In a glaucoma screening program, an automated system decides whether or not any signs of suspicious for glaucoma are present in an image. Only those images deemed suspect by the system will be passed to ophthalmologists for further examination.

There are no early symptoms of glaucoma and the only source to detect glaucoma at early stage is the structural change that arises in the internal eye. Many autonomous glau- coma detection systems analyze fundus image by calculating its Cup to Disc Ratio (CDR) and categorize the image as glaucoma or healthy. The image processing technique for the early detection of glaucoma. Glaucoma is detected using retinal fundus image. CDR technique is used on different retinal image for glaucoma detection[4].disc diameter[5],ISTN rule[6] and peripapillary atrophy (PPA) [7].
Glaucoma is detected basically by utilizing the medical history, intra-ocular pressure and visual field loss tests together with a manual assessment of the Optic Disc (OD) through ophthalmoscopy. OD is the location where ganglion cell axons exit the eye to form the optic nerve, through which visual information of the photo-receptors is transmitted to the brain. In 2D images, the OD can be divided into two distinct zones: a central bright zone called the optic cup (in short,cup) and a peripheral region called the neuroretinal rim. The loss in optic nerve fibres leads to a change in the structural appearance of the OD, namely, the enlargement of cup region (thinning of neuroretinal rim) called cupping. Since one of the important indicators is the enlargement of the cup with respect to OD, various parameters are considered and estimated to detect the glaucoma, such as the vertical cup to disc ratio (CDR) [4], ISNT rule [5], and peripapillary atrophy (PPA) [6]. Among the structural image cues studied for glaucoma diagnosis, CDR is a major consideration of clinicians [8][9][10].However, clinical assessment by manual annotating the cup and disc for each image is labor-intensive, and automatically segmenting the disc and cup in fundus images is also time consuming. Extracting the optic disc region of interest(ROI) will produce a smaller intial image which takes much lesser time taken to process compared to segmenting disc and cup[11]. In this paper, we consider the image as the input of the proposed deep Convolutional Neural Network (CNN). For glaucoma detection, the disease pattern in DFIs is complex and hidden, which is different from the natural scene images. The analysis task of natural scene images are related to object detection of regions that has an obvious visual appearance (e.g. texture, shape or color). But glaucoma disease patterns could be only observed by the training and expertise of the examiner. Deep learning (DL) is an active research topic which learns discrimi- native representations of data. The DL architectures are formed by the composition of multiple linear and non-linear transfor- mations of the data, with the goal of yielding more abstract and ultimately more useful representations [11]. Convolutional neural networks (CNNs) are deep learning architectures, are recently been employed successfully for image segmentation and classification tasks [12][13][14]. DL architectures are an evolution of multilayer neural networks(NN), involving different design and training strategies to make them compet- itive. These strategies include spatial invariance, hierarchical feature learning and scalability [13].In this paper, effectively capturing the deep features of glaucoma based on deep CNN is our main interest. Therefore, we are motivated to propose a deep learning framework for capturing the discriminative features that better characterize the hidden patterns related to glaucoma. The adopted DL structure consists of Ten layers:Six convolutional layers and Four fully-connected layers, which infers a hierarchical representation of images to discriminate between glaucoma and non-glaucoma patterns for diagnostic decisions. In addition, to reduce the overfitting problem, we adopt response-normalization layers and overlapping-pooling layers. In order to further boost the performance, dropout and data augmentation strategies are also adopted in the proposed DL architecture.This paper is organized as

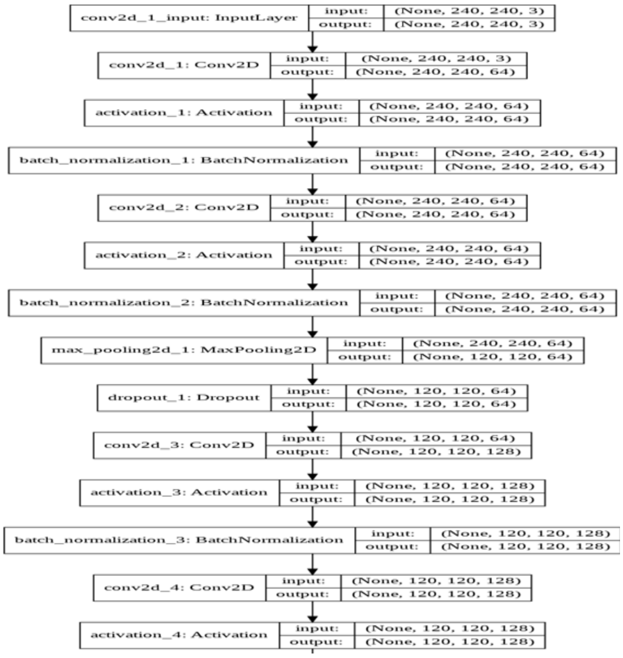
follows.In Section I, we have given an introduction of the background and motivation for the method.In Section II, we introduce the overview of the deep learning architecture. In Section III, we introduce the glaucoma classification based on CNN. Section IV shows the experimental results, followed by the conclusions in the last section.

II. OVERVIEW OF THE DEEP LEARNING ARCHITECTURE

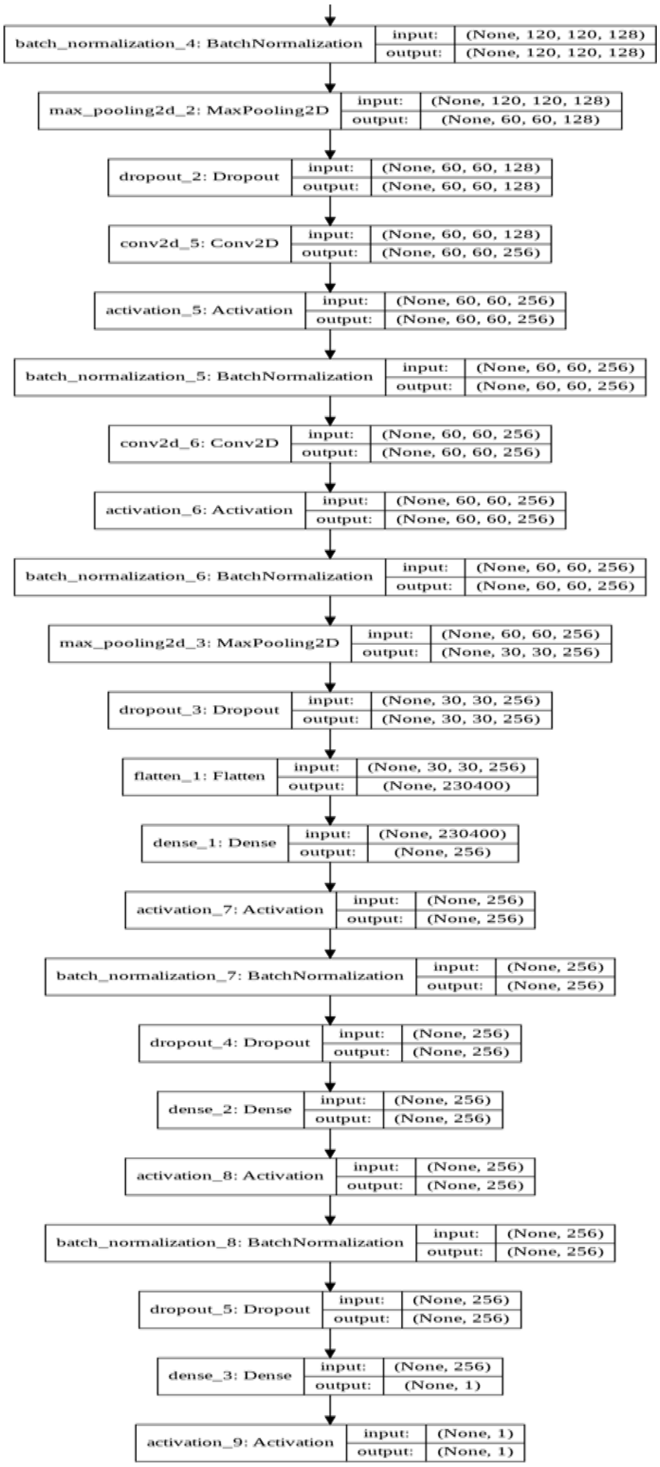
In this paper, the proposed deep learning architecture is based on CNN. As shown in Fig.1 the net of CNN con- tains Ten layers with weights: the Six are convolutional and the remaining Four are fully connected. The output of the last fully-connected layer is fed to a soft-max classifier for glaucoma prediction. Response-normalization layers and overlapping layers are employed in our proposed learning architecture as in [15].

A. Convolutional Layers

Convolutional layers are usually employed to learn small feature detectors based on patches randomly sampled from an image. A feature in the image at some location can be calculated by convolving the feature detector and the image at that location.



conv2d_1_input: InputLayer input: (None, 240, 240, 3) output: (None, 240, 240, 3)
conv2d_1: Conv2D input: (None, 240, 240, 3) output: (None, 240, 240, 64)
activation_1: Activation input: (None, 240, 240, 64) output: (None, 240, 240, 64)
batch_normalization_1: BatchNormalization input: (None, 240, 240, 64) output: (None, 240, 240, 64)
conv2d_2: Conv2D input: (None, 240, 240, 64) output: (None, 240, 240, 64)
activation_2: Activation input: (None, 240, 240, 64) output: (None, 240, 240, 64)
batch_normalization_2: BatchNormalization input: (None, 240, 240, 64) output: (None, 240, 240, 64)
max_pooling2d_1: MaxPooling2D input: (None, 240, 240, 64) output: (None, 120, 120, 64)
dropout_1: Dropout input: (None, 120, 120, 64) output: (None, 120, 120, 64)
conv2d_3: Conv2D input: (None, 120, 120, 64) output: (None, 120, 120, 128)
activation_3: Activation input: (None, 120, 120, 128) output: (None, 120, 120, 128)
batch_normalization_3: BatchNormalization input: (None, 120, 120, 128) output: (None, 120, 120, 128)
conv2d_4: Conv2D input: (None, 120, 120, 128) output: (None, 120, 120, 128)
activation_4: Activation input: (None, 120, 120, 128) output: (None, 120, 120, 128)



batch_normalization_4: BatchNormalization input: (None, 120, 120, 128) output: (None, 120, 120, 128)
max_pooling2d_2: MaxPooling2D input: (None, 120, 120, 128) output: (None, 60, 60, 128)
dropout_2: Dropout input: (None, 60, 60, 128) output: (None, 60, 60, 128)
conv2d_5: Conv2D input: (None, 60, 60, 128) output: (None, 60, 60, 256)
activation_5: Activation input: (None, 60, 60, 256) output: (None, 60, 60, 256)
batch_normalization_5: BatchNormalization input: (None, 60, 60, 256) output: (None, 60, 60, 256)
conv2d_6: Conv2D input: (None, 60, 60, 256) output: (None, 60, 60, 256)
activation_6: Activation input: (None, 60, 60, 256) output: (None, 60, 60, 256)
batch_normalization_6: BatchNormalization input: (None, 60, 60, 256) output: (None, 60, 60, 256)
max_pooling2d_3: MaxPooling2D input: (None, 60, 60, 256) output: (None, 30, 30, 256)
dropout_3: Dropout input: (None, 30, 30, 256) output: (None, 30, 30, 256)
flatten_1: Flatten input: (None, 30, 30, 256) output: (None, 230400)
dense_1: Dense input: (None, 230400) output: (None, 256)
activation_7: Activation input: (None, 256) output: (None, 256)
batch_normalization_7: BatchNormalization input: (None, 256) output: (None, 256)
dropout_4: Dropout input: (None, 256) output: (None, 256)
dense_2: Dense input: (None, 256) output: (None, 256)
activation_8: Activation input: (None, 256) output: (None, 256)
batch_normalization_8: BatchNormalization input: (None, 256) output: (None, 256)
dropout_5: Dropout input: (None, 256) output: (None, 256)
dense_3: Dense input: (None, 256) output: (None, 1)
activation_9: Activation input: (None, 1) output: (None, 1)

Fig. 1. Model summary

III. EXPERIMENTS

To evaluate the glaucoma diagnosis performance of our

Evaluation Criteria

In this work, we utilize the area under the curve (AUC) of receiver operation characteristic curve

(ROC) to evaluate the performance of glaucoma diagnosis. The ROC is plotted as a curve which shows the tradeoff between sensitivity TPR (true positive rate) and specificity TNR (true negative rate), defined as

Experimental Setup

We adopt the same settings of the experiments for glaucoma diagnosis in [19] in this work to facilitate comparisons.The Kims hospital dataset with clinical glaucoma diagnoses, is comprised of 467 glaucoma and 467 normal fundus images.

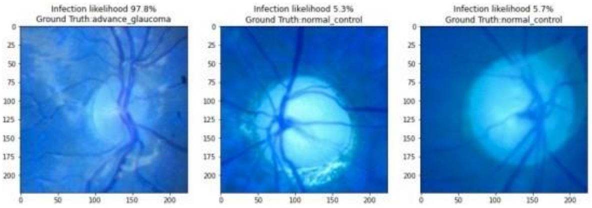

Infection likelihood 97.8%
Ground Truth:advance_glaucoma
Infection likelihood 5.3%
Ground Truth:normal_control
Infection likelihood 5.7%
Ground Truth:normal_control
0
25
50
75
100
125
150
175
200
0
50
100
150
200

Fig. 2. Sample diagnosis results from our proposed algorithm for glaucoma detection. Each fundus image is diagnosed by clinicians and the predicted labels with probabilities by our algorithm.

C. Experimental Results

In order to validate the effectiveness of our deep CNN on glaucoma diagnosis accuracy, we compare the predictions of CNN to state-of-the-art reconstruction-based method [19]. For ORIGA dataset, we adopt the same setting of [19]. The training set contains a random selection of 100 images from the whole 650 images, and the remaining 550 images are used for testing. The AUC values of our method on ORIGA are 0.831. For the state-of-the-art reconstruction-based method, the AUC values are 0.823. In addition, Fig. 2 gives Three sample results by our proposed algorithm. Each fundus image is diagnosed by clinicians and the predicted labels with probabilities by our algorithm.

IV. CONCLUSION

In this paper, we presenting a DL framework for Glaucoma detection based on CNN, CNN is used to capture the Discriminative features that better characterize the hidden patterns to glaucoma. We are adopted DL structure conatins Ten layers:Six convolutional layers and Four fully connected layers. To reduce the overfitting problem, we adpot response-normalzation layers and over lapping-pooling layers. In order to further boost the performance, dropout and data augmentation strategies are utilized in the proposed deep CNN.

V. ACKNOWLEDGMENT

We gratefully thank the Visvesvaraya Technological Univer- sity, Jana Sangama,Belagavi for financial support extended to this research work.

VI. REFERENCES

[1]. J. Flammer and E. Meier, Glaucoma: A Guide for Patients : an Introduction for Care-providers : a Quick Reference, Hogrefe & Huber, 2003.

[2]. Quigley, H.A., Broman, A.T., The number of people with glaucoma worldwide in 2010 and 2020., In: Ophthalmol 2006.

[3]. Chethan Kumar N. S., Dr.Somashekar K., Image Processing Techniques for Automatic Detection of Glaucoma -A Study, International Journal of Latest Technology in Engineering, Management Applied Science Volume VI, Issue VII, July 2017 ISSN 2278-2540.

[4]. C. Patel and M. I. Patel, "Analysis of CDR of Fundus Images for Glaucoma Detection," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, 2018, pp. 1071-1074.,doi: 10.1109/ICOEI.2018.8553707.

[5]. Michael, D., Hancox, O. D., Optic disc size, an important consideration in the glaucoma evaluation.,In: Clinical Eye and Vision Care 1999.

[6]. Harizman, N., Oliveira, C., Chiang, A., Tello, C., Marmor, M., Ritch, R., Liebmann, J. M., The isnt rule and differentiation of normal from glaucomatous eyes.,In: Arch Ophthalmol 2006.

[7]. Jonas, J.B, Fernandez, M.C, Naumann, G.O, Glaucomatous para- papillary atrophy occurrence and correlations.,In: Arch Ophthalmol 1992.

[8]. Wong, D.W.K, Lim, J.H, Tan, N.M, Zhang, Z, Lu, S, Li, H, Teo, M, Chan, K, Wong, T.Y, Intelligent Fusion of Cup-to-Disc Ratio Determination Methods for Glaucoma Detection in ARGALI.,In: Int. Conf. Engin. in Med. and Biol. Soc., pp. 57775780 (2009)

[9]. Xu, Y, Xu, D, Lin, S, Liu, J, Cheng, J, Cheung, C.Y, Aung, T, Wong, T.Y Sliding Window and Regression based Cup Detection in Digital Fundus Images for Glaucoma Diagnosis.,In: MICCAI 2011

[10]. Xu, Y, Liu, J, Lin, S, Xu, D, Cheung C.Y, Aung, T, Wong, T.Y,Efficient Optic Cup Detection from Intra-image Learning with Retinal Structure Priors.,In : MICCAI 2012

[11]. Zhang, Z, Lee, B.H, Liu, J, Wong, D.W.K, TAN N.M, Lim, J.H, Yin, F.S, J.H, Huang, W.M, Li, H Optic disc region of interest localization in fundus image for glaucoma detection in argali.,In: Proc. of Int. Conf. on Industrial Electronics Applications, pp. 1686 1689 (2010)

[12]. Krizhevsky, A, et al. Imagenet classification with deep convolutional neural networks.,In: NIPS 2012

[13]. Bengio, Y, et al. Representation learning: A review and new perspectives..,In: Arxiv 2012

[14]. Le, Q.V, et al. Building high-level features using large scale unsuper- vised learning.,In: ICML 2011

[15]. Krizhevsky, A, et al. Imagenet classification with deep convolutional neural networks.,In: NIPS 2012

[16]. Liu, J, Wong, D. W. K, Lim, J. H, Li, H, Tan, N. M, Zhang, Z, Wong, T. Y, Lavanya, R, ARGALI: An automatic cup-to-disc ratio measurement system for glaucoma analysis using level-set image pro- cessing.,In: 13th International Conference on Biomedical Engineering (ICBME) 2008

[17]. Hinton, G.E, Srivastava, N, Krizhevsky, A, Sutskever, I, Salakhutdinov, R.R, Improving neural networks by preventing co-adaptation of feature detectors.,In: NIPS 2012

[18]. Ciresan, D.C, Meier, U, Masci, J, Gambardella, L.M, Schmidhuber, J, High-performance neural networks for visual object classifica- tion.,In: Arxiv 2011

[19]. Xu, Y, Lin, S, Wong, T.Y, Liu, J, Xu, D, Efficient Reconstruction- Based Optic Cup Localization for Glaucoma Screening.,In: MICCAI

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Effective Video Copy Detection Technique of Multimedia Content in Cloud Environment

Shubham Dilip Vyawahare[1], **Dr. Avinash Kapse**[2]
[1]Department of Information Technology, Anuradha Engineering College, Chikhli, Maharashtra, India
[2]Associate Professor & HOD, Department of Information Technology, Anuradha Engineering College, Chikhli, Maharashtra, India

ABSTRACT

In a view of large-scale multimedia content protection systems and the charges to provide cloud infrastructures to provide cost efficiency, rapid deployment, scalability, and elasticity to accommodate varying workloads. We proposing a system that can be used to protect different multimedia content types, including 2-D videos, 3-D videos, images, audio clips, songs, and music clips. It can be implemented on private and/or public clouds. We design a system with two method processing: (i) Creating digital signatures, and (ii) Comparison database to recognized modifications. The signature method creates robust and representative signatures of contents. Comparison with storage that is real in cloud with the available content. The high accuracy and scalability of the proposed system include high database and storage content. In addition, we compared our system to the protection system used by some videos channels.

Keywords : Cloud storage, Digital signatures, scalability, protection channels and database.

I. INTRODUCTION

The existing mechanism a new significant privacy issue introduced in the case of shared data with the use of the leakage of identity privacy to public verifiers. The traditional approach for checking data correctness is to retrieve the entire data from the cloud, and then verify data integrity by checking the correctness of signatures.

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met:

1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user;

2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.

To support a privacy-preserving mechanism .

To make public auditing on shared data stored in the cloud using various encrytion algorithm.

II. Literature Survey

Public Auditing Mechanism

A new public auditing mechanism for shared data with efficient user revocation in the cloud. When a user in the group is revoked, we allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. The group can save a significant amount of computation and communication resources during user revocation. [3]

A secure and efficient RDC scheme for network coding-based distributed storage systems that rely on untrusted server. RDC-NC scheme can be used to ensure data remains intact when faced with data corruption, replay, and pollution attacks. The RDC-NC is inexpensive for both clients and servers. [4]

Short Group Signatures: Signatures in our scheme are approximately the size of a standard RSA signature with the same security. The group signature is based on the Strong Diffie-Hellman assumption and a new assumption in bilinear groups called the Decision Linear. [5]

Storing Shared Data on the Cloud via Security-Mediator: We believe is the right approach to achieve anonymity in storing data to the cloud with publicly-verifiable data-integrity in mind. The de couples the anonymous protection mechanism from the provable data possession mechanism via the use of security mediator. They minimize the computation and bandwidth requirement of this mediator, but also minimize the trust placed on it in terms of data privacy and identity privacy. [6]

III. Module

User Registration:

For the registration of user with identity ID the group manager randomly selects a number. Then the group manager adds into the group user list which will be used in the traceability phase. After the registration, user obtains a private key which will be used for group signature generation and file decryption.

Registration

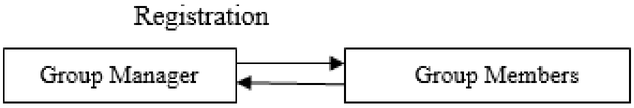


Fig 1: Key Distribution

Public Auditing:

Homomorphic authenticators are unforgeable verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure an auditor that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator. Overview to achieve privacy-preserving public auditing, we propose to uniquely integrate the Homomorphic authenticator with random mask technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random function (PRF). The proposed scheme is as follows:

- Setup Phase
- Audit Phase

Sharing Data:

The canonical application is data sharing. The public auditing property is especially useful when we expect the delegation to be efficient and flexible. The schemes enable a content provider to share her data in a confidential and selective way, with a fixed and small cipher text expansion, by distributing to each authorized user a single and small aggregate key.

Integrity Checking:

Hence, supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Now we show how our main scheme can be adapted to build upon the existing work to support data dynamics, including block level operations of modification, deletion and insertion. We can adopt this technique in our design to achieve privacy-preserving public risk auditing with support of

IV. Algorithm Used

Definition

The Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector. (Encryption for the US military and other classified communications is handled by separate, secret algorithms.)In January of 1997, a process was initiated by the National Institute of Standards and Technology (NIST), a unit of the U.S. Commerce Department, to find a more robust replacement for the Data Encryption Standard (DES) and to a lesser degree Triple DES.

The specification called for a symmetric algorithm (same key for encryption and decryption) using block encryption (see block cipher) of 128 bits in size, supporting key sizes of 128, 192 and 256 bits, as a minimum.

The algorithm was required to be royalty-free for use worldwide and offer security of a sufficient level to protect data for the next 20 to 30 years. It was to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defenses against various attack techniques. The entire selection process was fully open to public scrutiny and comment, it being decided that full visibility would ensure the best possible analysis of the designs.

In 1998, the NIST selected 15 candidates for the AES, which were then subject to preliminary analysis by the world cryptographic community, including the National Security Agency. On the basis of this, in August 1999, NIST selected five algorithms for more extensive analysis. These were:

- MARS, submitted by a large team from IBM Research.
- RC6, submitted by RSA Security.
- Rijndael, submitted by two Belgian cryptographers, Joan Daemen and Vincent.
- Rijmen Serpent, submitted by Ross Andersen, Eli Biham and Lars Knudsen
- Two fish, submitted by a large team of researchers including Counterpane's.
- Respected cryptographer, Bruce Schneier.

Implementations of all of the above were tested extensively in ANSI C and Java languages for speed and reliability in such measures as encryption and decryption speeds, key and algorithm set-up time and resistance to various attacks, both in hardware- and software-centric systems.

Once again, detailed analysis was provided by the global cryptographic community (including some teams trying to break their own submissions). The end result was that on October 2, 2000, NIST announced that Rijndael had been selected as the proposed standard. On December 6, 2001, the Secretary of Commerce officially approved Federal Information Processing Standard (FIPS) 197, which specifies that all sensitive, unclassified documents will use Rijndael as the Advanced Encryption Standard.

Also see cryptography, data recovery agent (DRA)RELATED GLOSSARY TERMS: RSA algorithm (Rivest-Shamir-Adleman), data key, greynet (or graynet), spam cocktail (or anti-spam cocktail), fingers canning (fingerprint scanning),munging, insider threat, authentication server, defense in depth, nonrepudiation.

High-level description of the algorithm:

1. Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule.

2. Initial Round

AddRoundKey— each byte of the state is combined with the round key using bitwise xor.

3. Rounds

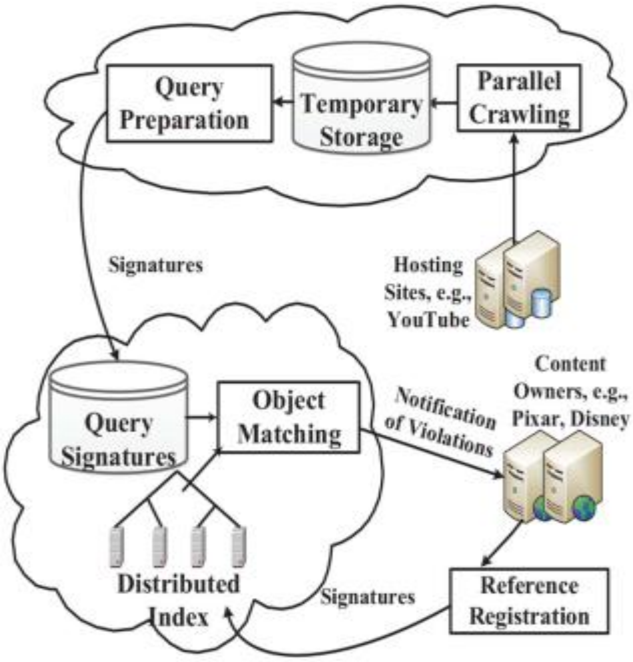
- Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
- Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
- Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

- Add Round Key

4. Final Round (no Mix Columns)

- Sub Bytes
- Shift Rows
- Add Round Key

Diagrams



Examples

In this appendix, twenty examples are provided for the MAC generation process. The underlying block cipher is either the AES algorithm or TDEA. A block cipher key is fixed for each of the currently allowed key sizes, i.e., AES-128, AES-192, AES-256, two key TDEA, and three key TDEA. For each key, the generation of the associated sub keys is given, followed by four examples of MAC generation with the key.

The messages in each set of examples are derived by truncating a common fixed string of 64 bytes. All strings are represented in hexadecimal notation, with a space (or a new line) inserted every 8 symbols, for readability. As in the body of the Recommendation, K1 and K2denote the sub keys, M denotes the message, and T denotes the MAC. For the AES algorithm examples, Tlen is 128, i.e., 32 hexadecimal symbols, and K denotes the key. For the TDEA examples, Tlen is 64, i.e., 16 hexadecimal symbols, and the key, K, is the ordered triple of strings, (Key1, Key2, and Key3). For two key TDEA, Key1 = Key3.

D.1 AES-128

For Examples 1–4 below, the block cipher is the AES algorithm with the following 128 bit key: K 2b7e1516 28aed2a6 abf71588 09cf4f3c.

Sub key Generation CIPHK (0128) 7df76b0c 1ab899b3 3e42f047 b91b546f K1 fbeed618 35713366 7c85e08f 7236a8de

K2 f7ddac30 6ae266cc f90bc11e e46d513b

Example Explanations

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext.

The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

Ring signature (digital Signature):

In cryptography, a ring signature is a type of digital signature that can be performed by any member of a group of users that each have keys. Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people. One of the security properties of a ring signature is that it should be difficult to determine which of the group members' keys was used to produce the signature.

Ring signatures are similar to group signatures but differ in two key ways.

Suppose that a group of entities each have public/private key pairs, (PK1, SK1), (PK2, SK2), (PKn, SKn). Party i can compute a ring signature σ on a message m, on input (m, SKi, PK1, PKn). Anyone can check the validity of a ring signature given σ, m, and the public keys involved, PK1, PKn.

If a ring signature is properly computed, it should pass the check. On the other hand, it should be hard for anyone to create a valid ring signature on any message for any group without knowing any of the secret keys for that group.

V. Conceptualization

Cloud Computing:

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation.

Cloud computing, or something being in the cloud, is an expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. Cloud computing is a term without a commonly accepted unequivocal scientific or technical definition.

In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. The phrase is also more commonly used to refer to network-based services which appear to be provided by real server hardware, which in fact are served up by virtual hardware, simulated by software running on one or more real machines.

Such virtual servers do not physically exist and can therefore be moved around and scaled up (or down) on the fly without affecting the end user arguably, rather like a cloud.

Cloud computing relies on sharing of resources to achieve coherence and economies of scale similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

There are many types of public cloud computing

- ✓ Infrastructure as a service (IaaS)
- ✓ Platform as a service (PaaS)
- ✓ Software as a service (SaaS)
- ✓ Storage as a service (STaaS)
- ✓ Security as a service (SECaaS)
- ✓ Data as a service (DaaS)
- ✓ Test environment as a service (TEaaS)
- ✓ Desktop as a service (DaaS)
- ✓ API as a service (APIaaS)

The business model, IT as a service (ITaaS), is used by in-house, enterprise IT organizations that offer any or all of the above services. Using software as a service, users also rent application software and databases. The cloud providers manage the infrastructure and platforms on which the applications run.

End users access cloud-based applications through a web browser or a light-weight desktop or mobile app while the business software and user's data are stored on servers at a remote location. Proponents claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand.

Application of Cloud computing:

- ✓ Autonomic computing — Computer systems capable of self-management.
- ✓ Client–server model — Client–server computing refers broadly to any distributed application that distinguishes between service providers (servers) and service requesters (clients).
- ✓ Grid computing — "A form of distributed and parallel computing, whereby a 'super and virtual computer' is composed of a cluster of networked, loosely coupled computers acting in concert to perform very large tasks."
- ✓ Mainframe computer — Powerful computers used mainly by large organizations for critical applications, typically bulk data processing such as census, industry and consumer statistics, police and secret intelligence

services, enterprise resource planning, and financial transaction processing.

- ✓ Utility computing — The "packaging of computing resources, such as computation and storage, as a metered service similar to a traditional public utility, such as electricity."
- ✓ Peer-to-peer — Distributed architecture without the need for central coordination, with participants being at the same time both suppliers and consumers of resources (in contrast to the traditional client–server model).
- ✓ Cloud gaming - Also called on-demand gaming is a way of delivering to games to computers. The gaming data will be stored in the provider's server, so that gaming will be independent of client computers used to play the game.

VI. Characteristics

Agility improves with users' ability to re-provision technological infrastructure resources.

Application Programming Interface (API) accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers. Cloud computing systems typically use REST-based APIs.

Cost is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure.

This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks.

Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation (in-house).The e-FISCAL project's state of the art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

Device and location independence enable users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.

Virtualization technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.

Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

Peak-load capacity increases (users need not engineer for highest possible load-levels)

Utilization and efficiency improvements for systems that are often only 10–20% utilized.

Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.[30]

Scalability and elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak loads.

Performance is monitored, and consistent and loosely coupled architectures are constructed using web services as the system interface.

Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

Virtualization

Virtualization (or virtualization) is the creation of a virtual (rather than actual) version of something, such as a hardware platform, operating system (OS), storage device, or network resources.

While a physical computer in the classical sense is clearly a complete and actual machine, both subjectively (from the user's point of view) and objectively (from the hardware system administrator's point of view), a virtual machine is subjectively a complete machine (or very close), but objectively merely a set of files and running programs on an actual, physical machine (which the user need not necessarily be aware of). Virtualization can be viewed as part of an overall trend in enterprise IT that includes autonomic computing, a scenario in which the IT environment will be able to manage itself based on perceived activity, and utility computing, in which computer processing power is seen as a utility that clients can pay for only as needed.

The usual goal of virtualization is to centralize administrative tasks while improving scalability and overall hardware-resource utilization. With virtualization, several operating systems can be run in parallel on a single central processing unit (CPU). This parallelism tends to reduce overhead costs and differs from multitasking, which involves running several programs on the same OS.

Feasibility Study

Feasibility study is the test of a system proposal according to its workability, impact on the organization, ability to meet user needs, and effective use of recourses. It focuses on the evaluation of existing system and procedures analysis of alternative candidate system cost estimates. Feasibility analysis was done to determine whether the system would be feasible.

The development of a computer based system or a product is more likely plagued by resources and delivery dates. Feasibility study helps the analyst to decide whether or not to proceed, amend, postpone or cancel the project, particularly important when the project is large, complex and costly. Once the analysis of the user requirement is complement, the system has to check for the compatibility and feasibility of the software package that is aimed at. An important outcome of the preliminary investigation is the determination that the system requested is feasible.

Technical Feasibility:

The technology used can be developed with the current equipment's and has the technical capacity to hold the data required by the new system.

- This technology supports the modern trends of technology.
- Easily accessible, more secure technologies.

Technical feasibility on the existing system and to what extend it can support the proposed addition. We can add new modules easily without affecting the Core Program. Most of parts are running in the server using the concept of stored procedures.

Operational Feasibility:

This proposed system can easily implemented, as this is based on JSP coding (JAVA) & HTML .The database created is with My Sql server which is more secure and easy to handle. The resources that are required to implement/install these are available. The personal of the organization already has enough exposure to computers. So the project is operationally feasible.

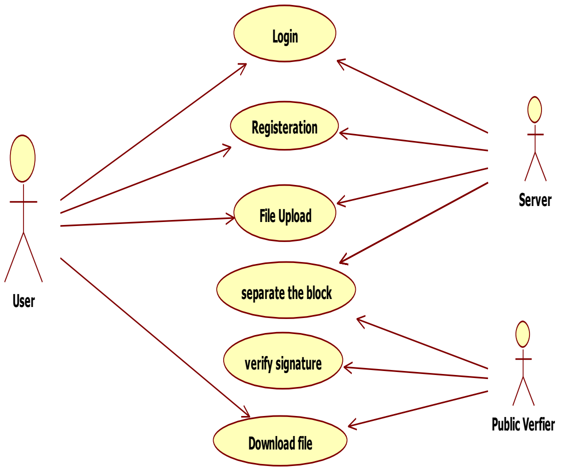
Economic Feasibility:

Economic analysis is the most frequently used method for evaluating the effectiveness of a new system. More commonly known cost/benefit analysis, the procedure is to determine the benefits and savings that are expected from a candidate system and compare them with costs. If benefits outweigh costs, then the decision is made to design and implement the system.

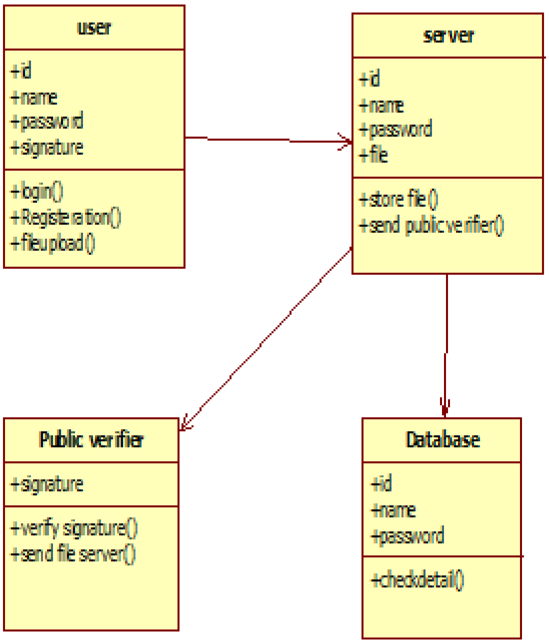
An entrepreneur must accurately weigh the cost versus benefits before taking an action. This system is more economically feasible which assess the brain capacity with quick & online test.

VII. System Design and deployment

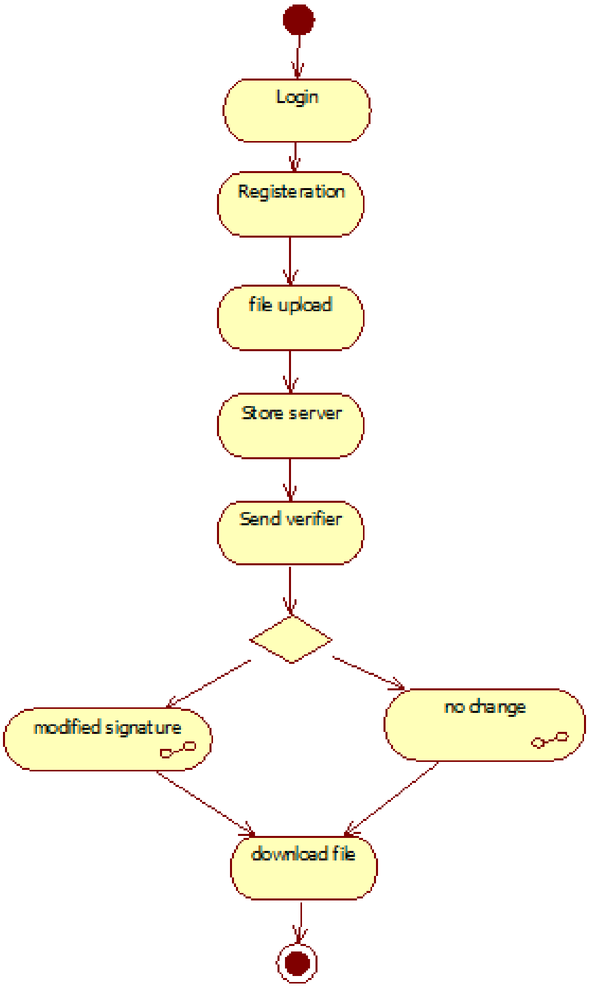
Use Case Structure



Class Diagram



Activity Diagram



VIII. EXISTING SYSTEM

The existing mechanism a new significant privacy issue introduced in the case of shared data with the use of the leakage of identity privacy to public verifiers. The traditional approach for checking data correctness is to retrieve the entire data from the cloud, and then verify data integrity by checking the correctness of signatures.

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy

IX. LIMITATIONS

As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted.

They do not perform the multiple auditing task in simultaneously.

X. PROPOSED SYSTEM

The propose system a privacy-preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphism authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block.

To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing. There are two interesting problems we will continue to study for our future work. One of them is traceability, which means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations

XI. ADVANTAGES

The proposed system can perform multiple auditing tasks simultaneously. They improve the efficiency of verification for multiple auditing tasks. High security provide for file sharing.

XII. CONCLUSION

In this paper, we propose the system, the first privacy-preserving public auditing mechanism for shared data in the cloud for protecting the multimedia content. With this system, the public verifier is able to efficiently audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can preserve identity privacy for users. An interesting problem in our future work is how to efficiently audit the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third party auditor.

XIII. REFERENCES

[1]. Abdelsadek, “Distributed index for matching multimedia objects,” M.S. thesis, School of Comput. Sci., Simon Fraser Univ., Burnaby, BC, Canada, 2014.

[2]. Abdelsadek and M. Hefeeda, “Dimo: Distributed index for matching multimedia objects using MapReduce,” in Proc. ACMMultimedia Syst. Conf. (MMSys’14), Singapore, Mar. 2014, pp. 115–125.

[3]. M. Aly, M. Munich, and P. Perona, “Distributed Kd-Trees for retrieval from very large image collections,” in Proc. Brit. Mach. Vis. Conf. (BMVC), Dundee, U.K., Aug. 2011.

[4]. J. Bentley, “Multidimensional binary search trees used for associative searching,” in Commun. ACM, Sep. 1975, vol. 18, no. 9, pp. 509–517.

[5]. P. Cano, E. Batle, T. Kalker, and J. Haitsma, “A review of algorithms for audio fingerprinting,” in Proc.

[6]. Privacy-Preserving Public Auditing for Secure Cloud Storage (I. Agudo, D. Nu˜ nez, G. Giammatteo, P. Rizomiliotis, and C. Lambrinoudakis, “Cryptography goes to the cloud,” in Secure and Trust Computing, Data Management, and Applicat., 2011, pp. 190– 197.)

[7]. Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data (G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proc. 14th ACM conf. Compu. Commun. Security (CCS), 2007, pp. 598–609.)

[8]. Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud (G. Ateniese, A. Faonio, and S. Kamara, “Leakage-resilient identification schemes from zero-knowledge proofs of storage,” in IMA Inte. Conf. Cryptography and Coding, 2015, pp. 311–328)

[9]. Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud (G. Ateniese,

R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secure and Privacy in Commun. Netw. (SecureComm), 2008, pp. 1–10.)

[10]. Remote Data Checking for Network Coding-based Distributed Storage Systems(K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: theory and implementation," in Proc. 2009 ACM Workshop Cloud Computing Security (CCSW), 2009, pp. 43–54.)

[11]. Short Group Signatures(L. Chen, "Using algebraic signatures to check data possession in cloud storage," Future Generation Computer Systems, vol. 29, no.7, pp. 1709–1715, 2013.)

[12]. Storing Shared Data on the Cloud via Security-Mediator (Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of retrievability viahardness amplification," in Proc. Theory Cryptography Conf. (TCC), 2009, pp. 109–127.,)

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Credit Card Reader with Face Recognition Based on Webcam and Multimodal Biometrics

Vismaye M, Harshitha Gowda, Keerthishree V, Nidhish VP

ISE, New Horizon College of Engineering, Bangalore, Karnataka, India

ABSTRACT

This paper is focused on proposing a method for transactions on a credit card with face recognition using a web cam. This system initiates transfers based on detection/recognition of the face that is linked with the card. Considering the security issues in detail, when the visa card is used for the transactions, we just scan it which can cause lot of security issues if stolen or misplaced. With face recognition it will become secure and safe, giving a two-step verification. Now considering multimodal biometrics, the paper focuses on face-iris multimodal biometrics. The iris recognition system is composed of segmentation, normalization, feature encoding, and matching. This is to be done to avoid the drawbacks that would occur with only face recognition.

I. INTRODUCTION

In the modern era every individual wants many different modes of payment. Businesses have increased gradually due to enormous payment methods, but how safe can they be? Statistics say that the cybercrimes like Credit card frauds have been increasing gradually over the past few years. It is still the most known cybercrime that is been happening and there is still no measure to control it. The Fundamental issues that every credit card user faces is that they do not have a secure online transaction procedure. The biggest risk that is faced is credit card fraud which can lead to heavy losses. Technology is being used in the wrong way, there are multiple ways where the same technology can be used to reduce the cybercrime(s).

CONCEPTS OF BIO METRICS

Biometrics can be characterized as estimations identified with body and computations identified with human qualities. Biometrics confirmation is utilized for recognizable proof and access control.
Biometric identifiers are the unmistakable, quantifiable qualities. Biometric identifiers are frequently arranged as physiological versus social qualities. Physiological qualities are identified with the state of the body. A couple of models are unique mark, palm veins, face acknowledgment, palm print, iris acknowledgment, retina.

FACIAL RECOGNITION

A facial acknowledgment framework is an innovation fit for distinguishing and confirming a person. There are various techniques in which the facial acknowledgment innovation works, however all in all, they work by looking at chosen facial highlights from given picture with faces inside an information base. It is commonly utilized as access control in security frameworks and can be contrasted with different biometrics, for example, unique mark or eye iris acknowledgment frameworks.

IRIS RECOGNITION

The Iris Recognition system being a biometric identification system, uses mathematical patter In the modern era every individual wants many different modes of payment. Businesses have increased gradually due to enormous payment methods, but how safe can they be? Statistics say that the cybercrimes like Credit card frauds have been increasing gradually over the past few years. It is still the most known cybercrime that is been happening and there is still no measure to control it. The Fundamental issues that every credit card user faces is that they do not have a secure online transaction procedure. The biggest risk that is faced is credit card fraud which can lead to heavy losses. Technology is being used in the wrong way, there are multiple ways where the same technology can be used to reduce the cybercrime(s).

CONCEPTS OF BIO METRICS

Biometrics can be characterized as estimations identified with body and computations identified with human qualities. Biometrics confirmation is utilized for recognizable proof and access control.

Biometric identifiers are the unmistakable, quantifiable qualities. Biometric identifiers are frequently arranged as physiological versus social qualities. Physiological qualities are identified with the state of the body. A couple of models are unique mark, palm veins, face acknowledgment, palm print, iris acknowledgment, retina. Facial recognition

A facial acknowledgment framework is an innovation fit for distinguishing and confirming a person. There are various techniques in which the facial acknowledgment innovation works, however all in all, they work by looking at chosen facial highlights from given picture with faces inside an information base. It is commonly utilized as access control in security frameworks and can be contrasted with different biometrics, for example, unique mark or eye iris acknowledgment frameworks.

IRIS RECOGNITION

The Iris Recognition system being a biometric identification system, uses mathematical pattern-recognition techniques to recognize the data.

It uses video camera technology infrared illumination to acquire rich detailed images of the eye.

WHY IRIS RECOGNITION SYSTEM OVER FACIAL RECOGNITION SYSTEM?

There is no full proof biometrics system but the iris recognition is known to be one of the most secure and renowned for not being faked. There are a few disadvantages to a facial recognition system like, a facial recognition system needs light at all time to authenticate, it needs an accurate reference photograph, one of the major drawbacks was discovered when Apple co. had launched their flagship smart phone the Apple iPhone X. The security access methods to this phone are facial recognition and a pin/password. The drawback is that an identical twin or an identical person that is a person with similar facial features could access the data and the contents in the phone. Even though this is a very rare case such a variable need's to be considered when it relates to the subject of authentication of an individual. The iris individual has a different pattern. There are n- recognition techniques to recognize the data. It uses video camera technology infrared illumination to acquire rich detailed images of the eye.

II. PROPOSED METHOD

The proposed system provides a safe method for credit card transactions which will integrate two step verification system. The basic level of verifications will be the OTP (one-time password) which will be valid only for a few mints, a second level of verification that can be added is the main subject of this paper that is a verification system using the bio metrics of the user.

One of the existing frameworks looks after the security making sure that there exists a secured payment procedure between the credit card and the holder and subsequently guarantees that card number stays obscure to some other substance. There exists another sort of framework that gives a recommendation, a recognition model to be accessible to catch the conceivable abnormal exchange.

MULTI MODAL BIOMETRICS

Technologists are centred around utilizing biometrics for validation as a safety effort. The expansion of biometrics (three-factor verification) can guarantee and secure the identity of the client. The favorable position for biometrics is that they can only with significant effort be duplicated as they are one of a kind to the client. On the opposite side, this sort of confirmation is less advantageous for shoppers as it for the most part requires a more extended time duty for the checkout cycle as the dealer is requiring an extra factor of verification.

FACIAL RECOGNITION

Advancement application that recognizes 80 nodal centers around the human face and contemplates these concentrations to a painstakingly set aside picture to confirm the character of a specific individual through model ID. Transcendence of modernized cameras on phones, PCs and work zones makes "pay by face" an accessible alternative. May require use of explicit camera foundation on devices; may anticipate that customers should pay additional charges and may raise some security stresses over the limit of facial pictures in information bases. Utilized in US-VISIT (United States Visitor and Immigrant Status Indicator Technology) to check the photographs of new wayfarers attempting to get segment to the United States against those submitted at the hour of visa issuance.

Figure 1: Facial Recognition

IRIS RECOGNITION

Iris Recognition Technology that analyses the subjective case of the iris to see and perceive a person. Image of the iris can be discovered using a standard camera and planning a person's iris with the set aside structure is significantly precise. The iris is difficult to channel from a decent way and can be obscured by eyelashes or eyelids. There can be inconvenience in scrutinizing the iris of people who have cascades or are outwardly debilitated. Iris affirmation is correct currently used for physical access control.

Figure 2 : Iris Recognition

III. METHODOLOGY

BIOMETRIC IRIS RECOGNITION

The process of iris recognition consists of 3 following steps

IMAGE CAPTURE

In this process the image of iris of the person will be captured. It must be ensured that iris is properly focused and image must be captured with clarity.

IRIS LOCATION AND IMAGE OPTIMIZATION

In this progression picture of the iris will be streamlined and iris limits and focal point of the understudy will be distinguished. Consequently, the region of the iris picture will be brake down which will help for include extraction. when the region which is utilized for include extraction is examined improvement of iris locale is finished by eliminating profound shadows and bits which are secured by eyelids. The iris locale which is enhanced will be standardized in a rectangular square and measurements will be fixed which will be contrasted and other filtered pictures of iris. We can't analyze the iris picture that is upgraded with put away iris pictures, the pictures that are put away in the biometric information base are called biometric layouts and this will contain the encoded organized highlights of iris which will be separated from the picture subsequent to applying Daugman's elastic sheet model. Matching and storage of biometric template. The biometric layout is to put away in biometric information base when the enlistment of the individual is done, on the off chance that the examined picture of iris utilized for validation, at that point the biometric format of the checked picture will be coordinated with biometric format which is put away in information base. Biometric face recognition.

HAAR CASCADE

Haar Cascade, algorithmic guideline is utilized to distinguish objects in an image or video. It's known for distinguishing countenances and parts of pictures. Haar Cascade is superimposing the positive pictures over an assortment of negative pictures. The learning is generally done on a worker and on different stages. Higher outcomes are acquired by exploitation of top quality pictures and expanding the amount of stages that the classifier is prepared. The algorithmic principle has four phases: Haar Feature Choice, making Integral pictures, Adaboost training, Cascading Classifiers. For the most part, 3 kinds of choices are utilized. The 2 rectangular choices are that the differentiation of the pixels at timespans rectangular areas. These locales have same structure and size and are on a level plane or vertically adjacent.3 rectangular alternatives are processed by taking the absolute of 2 external parallelograms at that point are eliminated with the complete in a really focus square shape. Further, inside the four square shapes highlights figures the differentiation between inclining sets of square shapes.

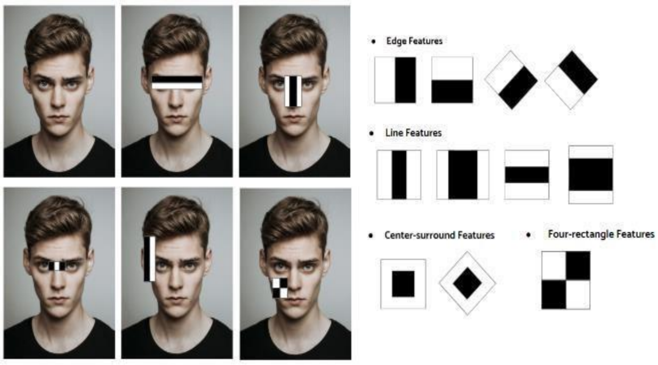


Figure 3: Haar Cascade Algorithm FACE RECOGNITION

Face detection refers to the psychological method by which an individual's face is scanned. Face Detection is the first and essential step for face recognition. It's required for object detection and might be used in several platforms like security, bio-metrics, enforcement, diversion, personal safety, etc. It's also used to observe faces in real time for police investigation. It's widely used in cameras to spot multiple appearances within the frame Example Mobile cameras and DSLR's. Firstly, an image of an individual's face is captured from a photograph or video. After that, identity verification package reads your facial features. Key factors of facial recognition embodies the space between your eyes as well as the distance between forehead and chin. The package identifies facial landmarks, one system identifies sixty-eight of them, which is the key to identify your face. Then your facial signature and a mathematical formula is compared to an information of far formed faces. And at last a determination is created. Your face print dataset could match with a picture in the database.

GLCM

It stands for Gray-level Co-occurrence matrix. The GLCM perform portray the vibe of an image by calculative anyway for the most part matches of pel with explicit qualities and in an extremely indicated spatial relationship happen in a picturef (Δx , Δy) or (d, ɵ)., making a GLCM. A GLCM may be a matrix wherever the quantity of rows and columns is up to the quantity of grey levels, G, within the image. The framework segments P (I, j | Δx, Δy) is that the recurrence with that 2 pixels, isolated by a pel separation (Δx, Δy), happen at spans a given neighbourhood, one with force 'I' and furthermore the distinctive with power 'j'. The grid parts P (I, j | d, ɵ) contains the subsequent request applied mathematical probability esteems for changes between dim levels 'I' and 'j' at a chose dislodging separation d and at a chose edge (ɵ). Utilizing a sizeable measure of force levels G suggests putting away a lot of transitory data, for example a G × G grid for each blend of (Δx , Δy) or (d, ɵ).

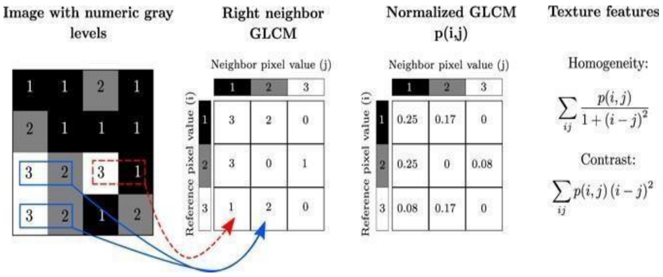


Image with numeric gray levels
Right neighbor GLCM
Normalized GLCM p(i,j)
Texture features
Neighbor pixel value (j)
Reference pixel value (i)
Homogeneity:
$\sum_{ij} \frac{p(i,j)}{1+(i-j)^2}$
Contrast:
$\sum_{ij} p(i,j)(i-j)^2$

Figure 4 : GLCM Algorithm

HOW DOES IT WORK?

As per the proposed system this is a method in which the user of the credit card has a secure platform for transactions.

The working of the model will be as follows: While a customer registers in the bank for a credit card his/her biometrics (iris and facial features) has to be recorded. This set of database can be accessed only by an authorized electronic card machine with an IR scanner. The process will contain 2 steps of verification where in the first step the credit card holder will receive an otp or enter a pin for the basic level of verification. In the second level of verification the merchant will have to use a camera with IR Scanners to scan the iris and facial features of the individual to authenticate the transaction. In case of online transactions, the user can utilize the camera with an external IR scanner to authenticate his/her transactions.

ALGORITHM

1. Start
2. An individual's personal details must be entered.
3. An individual's face and iris is scanned.
4. After scanning the face for registration, form must be submitted.
5. Payment details must be entered.
6. The features is compared with the database.
7. If the results match, then the transaction becomes successful.
8. Stop

FLOWCHART

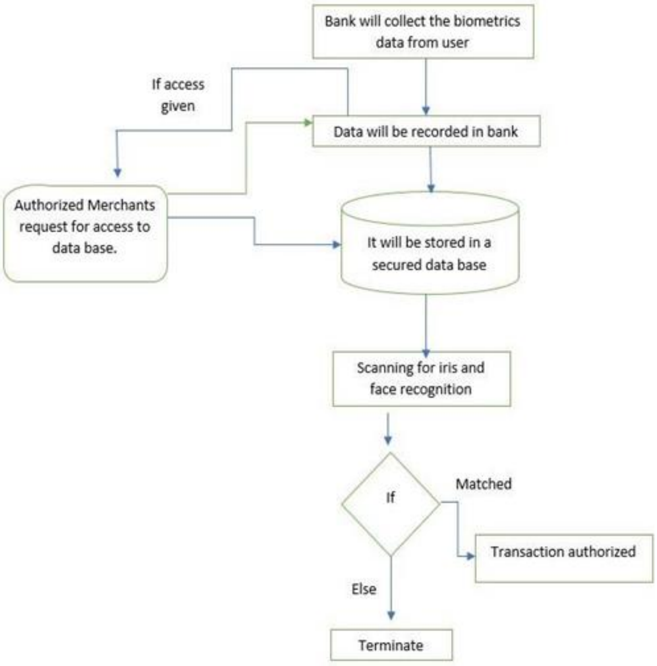

Bank will collect the biometrics data from user
If access given
Data will be recorded in bank
Authorized Merchants request for access to data base.
It will be stored in a secured data base
Scanning for iris and face recognition
If
Matched
Transaction authorized
Else
Terminate

Figure 5 : Flowchart of the execution

III. RESULTS

The user registers in the bank with his biometrics which has to match while transaction is occurring to keep the transaction highly secured.

IV. CONCLUSION

If the above method is followed the user will have a safe and secured platform for transactions. Cyber frauds can be avoided and helps in high security of the credit card transaction system for each individual.

V. REFERENCES

[1]. Recognition https://www.sciencedirect.com/topics/computer-science/iris-recognition

[2]. Biometrics https://www.verifi.com/resources/understandin g-biometrics-in-credit-card-security/

[3]. https://fidentity.com/blog/facial-recognition-vs-iris-scanning/

[4]. https://www.researchgate.net/publication/324953705_A_Robust_Multi-Biometric_System_with_Compact_Code_for_Iris_and_Face

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

A New Approximate Adder with Block-based Carry Speculation for High- Speed Applications

Dr. Boda Saroja*[1], Rajesh Gundlapalle[2]

[1]Department of Electronics and Communication Engineering, Vemu Institute of Technology, Chittoor, A.P, India.

[2]Department of Electronics and Communication Engineering, New Horizon College of Engineering, Bangalore, Karnataka, India

ABSTRACT

In any digital signal processing operation adders play an important role. Here, a high speed adder based on block-based carry speculation is proposed. Its structure is dependent on the separation of the additive from other summer blocks that are not integrated into their properties which can be selected from various additives such as broadcast carriers or parallel prefix adders. Here, the acquisition output for each block is considered based on the installation of the block itself and that of the next block. The block extension used in this case is a modified flexible extension with less space and delay compared to the Parallel Supplement connector circuit. In this case, we recommend high performance but low power / power based block-carry that carries a limited design structure called BCSA Adder. To minimize the risk, we suggest a way to predict the exit of a block based on its features and on the next block.

Keywords : Parallel Prefix Adder, BCSA Adder, Power/energy Consumption.

I. INTRODUCTION

The basic operators of approximate adders in performing arithmetic operations are deliberated in this paper. Approximate/estimated adders have been acquired numerous consideration by the designers. In the cutting edge estimated adders, where a large portion of them depend on the convey spread structures, the vitality and speed gains have been accomplished by equipment controlling, rationale improvement, and voltage over scaling. Although a portion of the adders depended on a configurable precision, others had a fixed accuracy level. The precision configurability forced a few overheads regarding postponement, region, and force which could restrict their utilization in certain applications where such re-configurability isn't required.

In this paper, a high-performance but low-power structure is proposed that produces a standardized structure called the BCSA adder. In this setting, the adder is divided into several non-interlocking blocks, which, in the worst case, exit the block depends on the exit of the previous block. To further reduce the critical approach, we propose a way to predict block release on the basis of its characteristics and the next block. The structure has low hardware weight, which leads to low latency (on average, about one block) and very high quality. In order to achieve lower accuracy losses, a debugging and retrieval system is recommended, which significantly reduces operating error rate. The efficiency of this additive is compared to that of other bees. Finally, the efficiency of the adder is analysed.

The previous works in the improving the adder structures by approximation methods are briefed as Carry Look Ahead adders, Carry Skip adders and Block based Prediction of Carry adders viz RAPCLA [1], ACSA [2], ACAA [3], HABA [4] SARA[5]. These structures suffers from critical path delay and high power consumption at times compromised with area. However, it has suffered from high delay although it has a high output precision. In most of the approximate adders, the carry input of each block is selected based on the input of the previous blocks. In this work, however, we propose an approximate adder that the carry input is speculated.

II. METHODS AND MATERIAL

A. *Adder with Error Recovery Unit:*

Fig.1 illustrates the generalized approximate adder with carry prediction unit. The improvement in accuracy is achieved by increasing the output error recovery. The error is as much as reduced by appropriate selection of carry input on the succeeding block. Hence, the carry output is selected with the highest possible accuracy in each of the every case. The idea behind the carry output selection for the four cases (K_0^{i+1}= 0 and G_{l-1}^{i}= 0), (K_0^{i+1}= 0 and G_{l-1}^{i}= 1), (K_0^{i+1}= 1 and G_{l-1}^{i}= 0) and (K_0^{i+1} = 1 and G_{l-1}^{i} = 1) are considered. The speculations in carry speculated carry (C_{Prdt}^{i}) is correct for the three cases are well predicted except for the first case. Thereby, shortening the critical path, C_{Prdt}^{i} is selected as the carry output of the ith block. Therefore, in the proposed approach, C_{Prdt}^{i}. is selected as the C_{in}^{i+1}.

Between these cases, the carry in the first stage is distributed in two blocks. In the third case, although the block input is executed and no longer distributed, the carry input is used to obtain the first block measurement. Therefore, if the input in this case is incorrect, it affects the accuracy of the sum output, Likewise, for all other 3 cases the average length of the carry distribution is close to one, illustrated in Fig. 2.

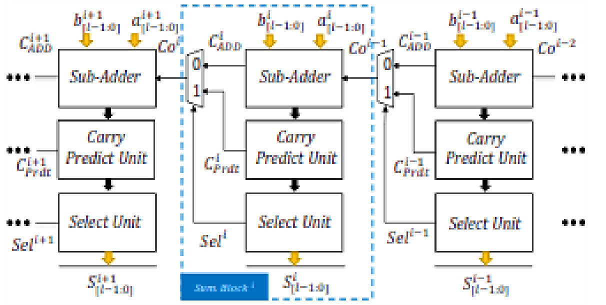


Figure 1 Generalized Approximate Adder with Carry Prediction.

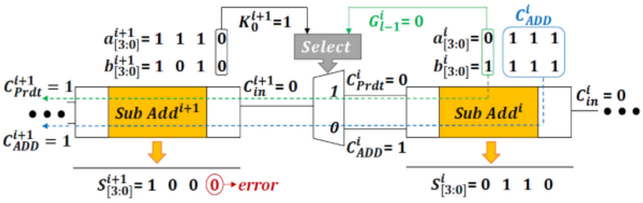


Figure 2 Approximate adder without Error Recovery Unit (ERU).

Hence, to improve the accuracy of the proposed connector, an error detection unit is suggested Fig. 3, that brings the first bit of the *ith* block S_0^{i} by,

$$S_0^{i+1} = \left(K_0^{i+1}.C_{Add}^{i}\right) + \left(P_0^{i+1}\oplus C_{in}^{i+1}\right) \qquad (1)$$

The first bit of (i+1)th block’s summation output is predicted by the equation,

$$P_0^{i+1}\oplus C_{in}^{i+1}\left(C_{in}^{i+1} = C_{Prdt}^{i}\right) \qquad (2).$$

The ERU is will not be in the path of addition process. This improves the accuracy of Error Recovery Unit (ERU) without increasing the further delay

B. *Proposed adder with new PPA:*

In this adder, ripple carry adder is used in the sub adder. So instead of using ripple carry adder if we use parallel prefix adder, reduce the delay of the adder. Hence to improve the delay use Parallel Prefix Adder (PPA) like Brent-kung adder and new parallel prefix adder.

C. Error Recovery Unit:

The transmitted message is vulnerable to noise or data corruption. The additional error detection codes details given to the digital message helps in detecting the occurrence of errors during message transmission. A simple example of an error detection code is a unity check.

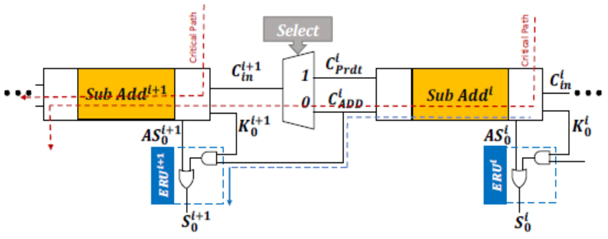


Figure 3 Proposed adder with new PPA with Error Recovery Unit (ERU).

In debugging codes, unity testing has an easy way to find errors and a complex way to find a fraudulent location. Once the corrupted bit is found, its value is restored (from 0 to 1 or 1 to 0) to receive the first message.

Therefore, the error recovery unit is used to detect and correct errors using different techniques.

D. Brentkung adder:

Brentkung adder of 8-bit width are used in the sub adders. Four 8-bit Brentkung adders are used in order to implement the 32-bit adder. Intermediate prefixes in small groups are computed in parallel prefix adders and then find the large group prefixes, until all the carry bits are computed. Parallel prefix addition of the operands 'A' and 'B' of width 'n' is done in pre-processing, carry generation and post processing stages.

In preprocessing stage, carry input is generated from propagated signals for each adder. These propagation signals are given by the equation 3 & 4.

$$\mathrm{Pi} = \mathrm{Ai} \oplus \mathrm{Bi} \tag{3}$$

$$\mathrm{Gi} = \mathrm{Ai.\,Bi} \tag{4}$$

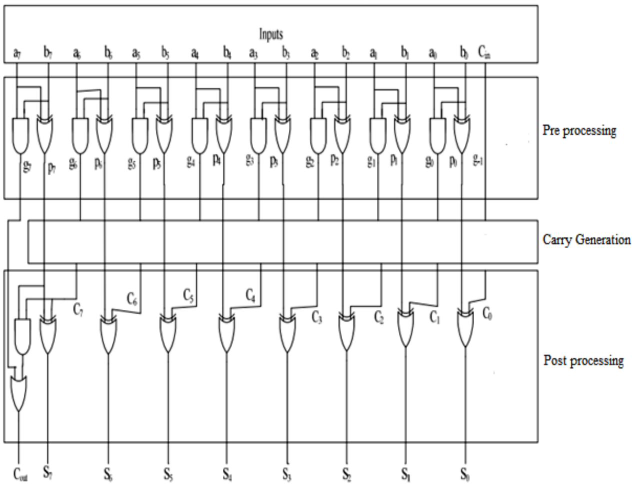

Inputs
a7 b7 a6 b6 a5 b5 a4 b4 a3 b3 a2 b2 a1 b1 a0 b0 Cin
Pre processing
g7 p7 g6 p6 g5 p5 g4 p4 g3 p3 g2 p2 g1 p1 g0 p0 g-1
Carry Generation
C7 C6 C5 C4 C3 C2 C1 C0
Post processing
Cout S7 S6 S5 S4 S3 S2 S1 S0

Figure 4 Overall architecture of PPA

In carry generation stage, the carries corresponding to each bit are generated. Execution is done in parallel form. After the counting of the same carriers, these are divided into smaller pieces. It uses generation and propagation as intermediate signals given by numbers 5 & 6. After the computation of carries in parallel they are divided into smaller pieces.

$$\mathrm{P}_{(\mathrm{i:k})} = \mathrm{P}_{(\mathrm{i:j})} \cdot \mathrm{P}_{(\mathrm{j-1:k})} \tag{4}$$

$$\mathrm{G}_{(\mathrm{i:k})} = \mathrm{G}_{(\mathrm{i:j})} + \left(\mathrm{G}_{(\mathrm{j-1:k})} \cdot \mathrm{P}_{(\mathrm{i:j})}\right) \tag{5}$$

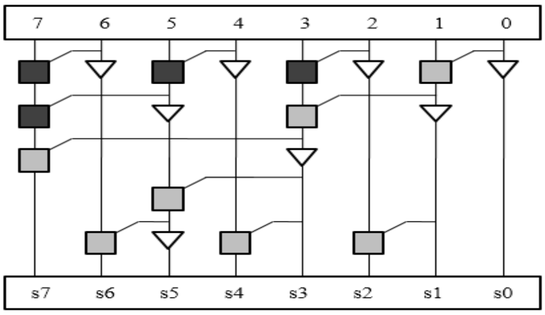


Figure 5 Carry Generation Design of 8-bit Brent kung adder.

This carry is generated by using different cell structures called Gray cell, Black cell and Buffer cell shown in Fig.6. By using this cell structures, final carry is calculated and are same for all parallel prefix adders but the design of carry generation is different.

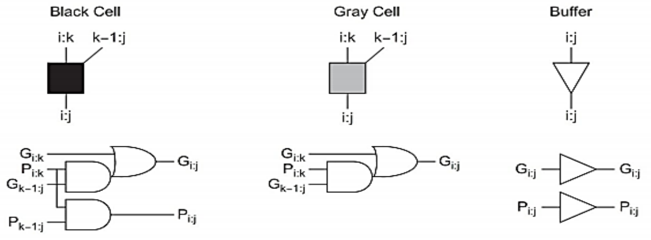


Figure 6 Black Cells, Gray Cells and Buffer cell used for carry generation stage.

The Post Processing Stage created the sum bits either by utilizing straightforward XOR entryways or by the utilization of restrictive entirety adders. In restrictive aggregate adders, for each bit position, two tentative sum will be produced and the right one will be chosen when the relevant carry for that bit arrives.

E. New parallel prefix adder:

A parallel prefix adder is used to improve the delay when of the adder when compare to the existing adder. This parallel prefix adder also contains three stages. Processing, carry generation stage and post processing stage. it is similar to the Brent kung adder but the carry generation stage is different. In this adder also contains black cells and gray cells but the design is different. The 8 bit proposed parallel prefix adder is shown in the Fig. 7.

Hence by using parallel prefix adder like Brent kung and proposed parallel prefix adder in place of ripple carry adder we can reduce the delay when compare to the existing adders

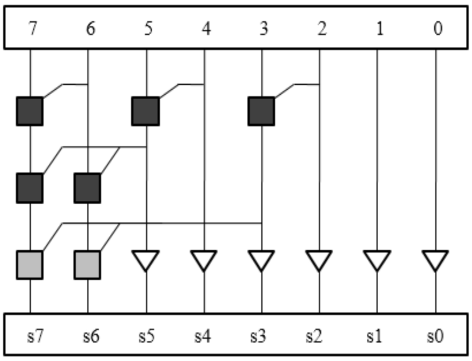


Figure 7 Proposed Parallel Prefix Adder

III. RESULTS AND DISCUSSION

For experimentation, a random 32-bit data's are experimented on 2 and 4 block sizes. The simulation is performed in Xlinx IDE. The RTL schematic is shown in figure 8. The layout design for the proposed architecture is viewed in figure 9. The simulation output is shown in figure 10.

The error rate(ER) metric is considered for analysing the proposed scheme more specifically Relative Error Distance Rate [RED rate]. The RED for 32-bit Adder with two separate block sizes 2 and 4 are projected in TABLE I.

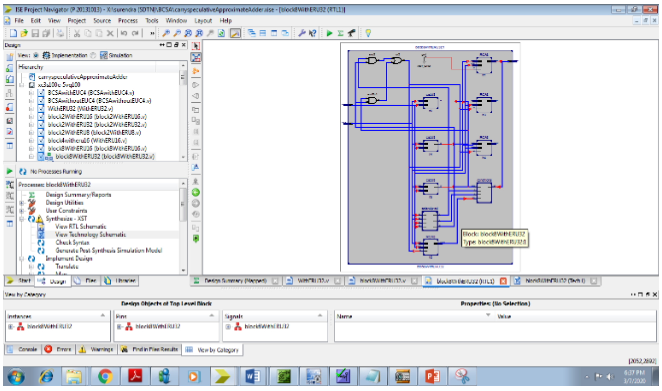


Figure 8 RTL Schematic

The metrics used for analysing error rate with 2 and 4 block sizes are depicted in TABLE I, despite of the study being performed on different block sizes viz., 2, 4 ,8 and 16. The error rate is extracted for 2^{16} unvarying random 8-bit numbers (16- and 32-bit) adders shown in figure 11. Accuracy rises with the increase in block size for adders. The percentages of the summation results with RED rate for 8-bit adders with the block size of 4 is depicted in TABLE II.

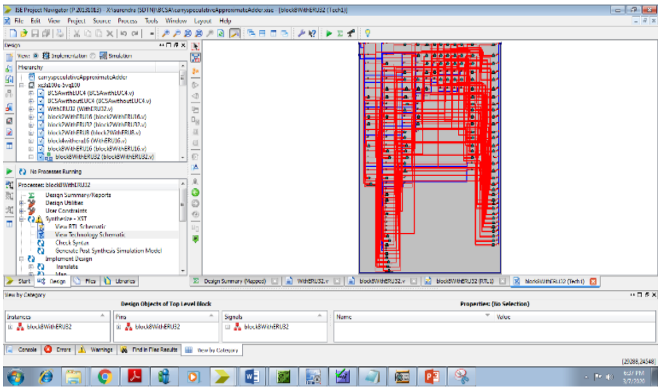


Figure 9 Layout Schematic

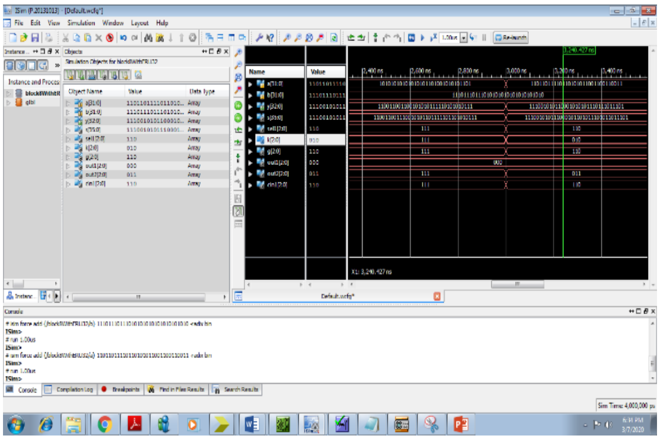


Figure 10 Simulation output

The RED is extracted by employing without '1/|*N*|' term. As the values of TABLE II show the outputs of the BCSA without ERU and with ERU, which produced 100% accuracy except for 5% and 10% RED rate.

Table 1 Accuracy Results for 32-Bit Adders

Proposed BCSA		32-bit date
Adder Type	Block Size	ER (%)
BCSAERU	2	74.66
BCSAERU	4	16.66
BCSA	2	87.62
BCSA	4	45.94

Table 2 Results of 32- bit Adder with RED

RED(%)	≤ 5%	≤ 10%	≤ 20%	≤ 50%	≤ 100%
BCSA WITHOUT ERU	94.50 %	94.50 %	100%	100%	100%
BCSA WITH ERU	100%	100%	100%	100%	100%

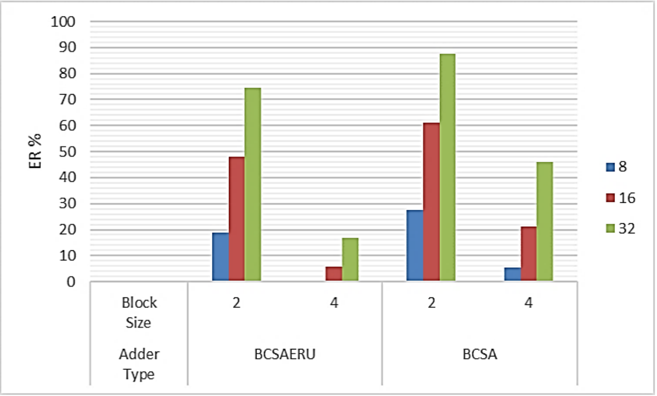


Figure 11 ER for 8 bit, 16 bit and 32 bit adders.

IV. CONCLUSION

In this case, we proposed a hypothetical block-based (BCSA), which was based on separating the adder directly into unconnected blocks that work in parallel. Each block can be named after any desired type of adders. In this extension, the length of the bearing chain was reduced and used to measure the bearing. The designated logic was suggested to look at the acquisition input of each block based on the other operator insertion of current and subsequent block components. In addition, to reduce the delay we use the novel structure of the parallel startup compound where the delay and location are better compared to other similar start additives. By reducing the loss of accuracy, the error detection method and recovery method have been suggested.

V. REFERENCES

[1]. M. Pashaeifar, M. Kamal, A. Afzali-Kusha, and M. Pedram, “Approximate Reverse Carry Propagate Adder for Energy-Efficient DSP Applications,” IEEE TVLSI, vol. 26, no. 11, pp. 2530-2541, 2018.

[2]. O. Akbari, M. Kamal, A. Afzali-Kusha, and M. Pedram, “RAP-CLA: A reconfigurable approximate carry look-ahead adder,” IEEE TCAS-II, vol. 65, no. 8, pp. 1089–1093, 2018.

[3]. H. Esmaeilzadeh, A. Sampson, L. Ceze, and D. Burger, "Neural Acceleration for General-Purpose Approximate Programs, " In Proc. of Micro, pp.449-460, 2012.

[4]. M. Bilal, S. Masud, and S. Athar, “FPGA Design for Statistics-Inspired Approximate Sum-of-Squared-Error Computation in Multimedia Applications,” IEEE TCAS-II, vol. 59, no. 8, pp. 506-510, 2012.

[5]. A. B. Kahng, S. Kang, "Accuracy-configurable adder for approximate arithmetic designs," In Proc. DAC, pp.820-825, 2012.

[6]. M. Samadi, J. Lee, D.A. Jamshidi, A. Hormati and S. Mahlke, “SAGE: self-tuning approximation for graphics engines”. Proc. Micro, pp.13-24, 2013.

[7]. Y. Kim, Y. Zhang, and P. Li. “An energy efficient approximate adder with carry skip for error resilient neuromorphic VLSI systems,” In Proc. ICCAD, pp. 130–137, 2013.

[8]. R. Ye, T. Wang, F. Yuan, R. Kumar and Q. Xu, “On Reconfiguration-Oriented Approximate Adder Design and Its Application,” In Proc. ICCAD, pp. 48-54, 2013.

[9]. B. K. Mohanty, S. K. Patel, "Area–delay–power efficient carry select adder", IEEE Trans. Circuits Syst. II Exp. Briefs, vol. 61, no. 6, pp. 418-422, Jun. 2014.

[10]. M. Kamal, A. Ghasemazar, A. Afzali-Kusha, and M. Pedram, “Improving efficiency of extensible processors by using approximate custom instructions,” in Proc. DATE, 2014. 11J. Hu and W. Qian, "A new approximate adder with low relative error and correct sign calculation," In Proc. IEEE DATE, pp. 1449-1454, 2015.

[11]. M. Shafique, W. Ahmad, R. Hafiz and J. Henkel, "A low latency generic accuracy configurable adder," In Proc. DAC, pp. 1-6, 2015.

[12]. "NanGate - The Standard Cell Library Optimization Company", 2016, Online]. Available: http://www.nangate.com/.

[13]. H. Jiang, C. Liu, L. Liu, F. Lombardi and J. Han, “A review, classification and comparative evaluation of approximate arithmetic circuits,” ACM JETCAS, vol. 13, no. 4, Article no. 60, 2017.

[14]. W. Xu, S. S. Sapatnekar, and J.Hu. "A Simple yet Efficient Accuracy Configurable Adder Design,” In Proc. ISLPED, 2017.

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Rapid Multiplier Architecture for Area and Power Optimization

Rajesh Gundlapalle[1], Sankarappa*[2], Dr. Boda Saroja[3]
[1]Department of Electronics and Communication Engineering, New Horizon College of Engineering, Bangalore, Karnataka, India
*[2&3]Department of Electronics and Communication Engineering, Vemu Institute of Technology, Chittoor, A.P, India

ABSTRACT

The interest in unique devices has increased with the special development of low power, digital signal processing (DSP) systems used in mobile computers and portable multimedia applications. Multipliers plays a major role including its DSP program. Operator duplication is often used not only on DSP chips but also on many public key cryptosystems such as Elliptic Curve Cryptography (ECC) and RSA. The proposed 4-bit Vedic multiplier's performance is analysed in terms of average power dissipation, delay, and also scaling effect of supply voltage.

Keywords : Public-key cryptosystems, Elliptic Curve Cryptography (ECC) and RSA.

I. INTRODUCTION

The multiplier plays an important role in electronic systems where repetition can be used in Digital Signal Processing applications such as convolution and fft. There is therefore a need for high speed and dynamic dynamics on a daily basis.

In the current case there are various types of repetition available such as Array Multiplier, Wallace Tree Multiplier Dock Repeat, but retrieval of members similar to the Wallace tree multiplier will simply increase the positive numbers, so that overcoming this duplicate of booths is built but duplicate booth applies to smaller designs.

The Vedic extension has been introduced to resolve the redundancy. Vedic repetition will increase both positive as well as negative numbers. The strength and delay of multiplication are increased and decreased respectively using Gate Diffusion Input (GDI) techniques.

Sri Bharati Krishna Tirtha Maharaja introduced the calculation of Vedic figures from the Vedas known as the Indian Sanskrit during the period 1911-1918. Vedic Mathematics relies on 16 sutras, numerical operations, arithmetic and dynamic arithmetic. The most widely used sutra is Urdhva Tiryagbhyam which provides a successful restoration. Decreased power consumption in integrated circuits has used a variety of methods. The GDI cycle has been used to reduce energy consumption and acceleration [2]. Standard CMOS circuit and GDI Mux based circuit breaker circuit and related investigations. In 2 X 2 Repetition of Vedas AND door and expansion of large parts are outstanding.

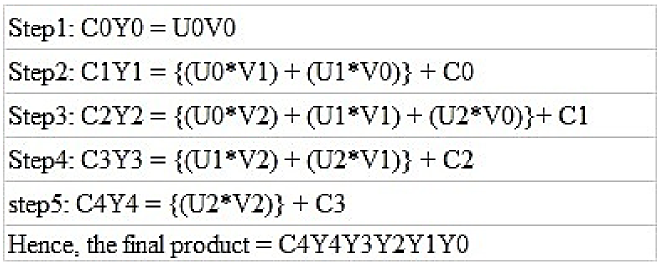
II. METHODS AND MATERIALS

A. Vedic Mathematics:

Vedic-arithmetic is an exceptionally old framework that can be applied legitimately to different parts of science, for example, variable based maths, math, and so forth. It eliminates vulnerability by eliminating superfluous strides before estimating any outcomes. There are 16 sutras in Vedic-arithmetic Urdhva Tiryakbhyam (UT) and Nikhilam Navatashcaramam Dashatah (NND) used to quantify the augmentation of any two numbers. Normally, the NND sutra is favored by huge pieces and UT sutra is favored by littler numbers. The UT sutra is consequently utilized in this work.

B. Urdhva Tiryakbhyam (UT):

Urdhva Tiryakbhyam (UT) means "vertical and transverse" operation which will multiply two numbers with any basis. The two 3-bit numbers, say U [2:0] and V[2:0] are multiplied to obtain a carry denoted by C[3:0] and Y[2:0] denotes partial production of the commodity. Then the following steps need to be taken:



Step1: C0Y0 = U0V0
Step2: C1Y1 = {(U0*V1) + (U1*V0)} + C0
Step3: C2Y2 = {(U0*V2) + (U1*V1) + (U2*V0)}+ C1
Step4: C3Y3 = {(U1*V2) + (U2*V1)} + C2
step5: C4Y4 = {(U2*V2)} + C3
Hence, the final product = C4Y4Y3Y2Y1Y0

C. Two Bit Vedic Multiplier:

This method is described below in two numbers, 2-input bits of ‘A’ and ‘B’ where A = a_1a_0 and B = b_1b_0. Next, the less important pieces’ increase, which gives very little noticeable end product (vertical). Then the multiplicand LSB is multiplied by the next high multiplication value and added by the LSB multiplication product and the next higher multiplicand fraction (crosswise). The sum provides a second item of the final product and the carrying is added to the partial product obtained by multiplying the bits that are most important to provide the quantity and handling.

The sum amount is the corresponding third indicator and the bearing is one-fourth of the final product. The 2X2 Vedic multiplication module is operated using four inputs AND gates and two additions. It is found that the construction of Vedic 2x2 hardware is similar to traditional Array Multi 2x2 bit architecture. It is therefore assumed that the repetition of 2-bit binary numbers in the Vedic method did not have a significant impact on the development of the multiplication efficiency. Specifically, the total delay is only 2-half of the add-on delay after the production of the final products, which is very close to the Array duplicate. Thus, a 4x4 bit Vedic multiplier using a 2x2 bit multiplier turns into a building block. The same method can be changed for 4 & 8 input pieces. But with the highest number of input bits, a small change is required.

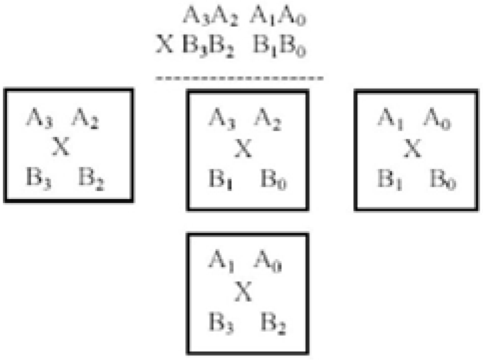


Figure 1 Sample Presentation for 4x4 bit Vedic Multiplication

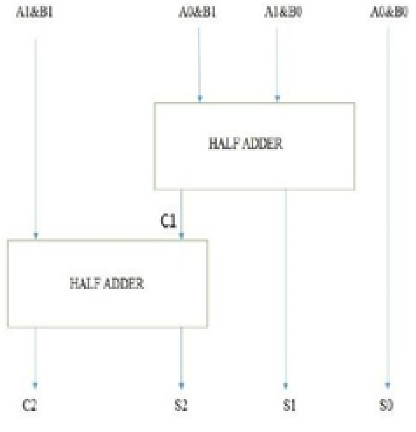


Figure 2 2-bit Multiplier with HA’s

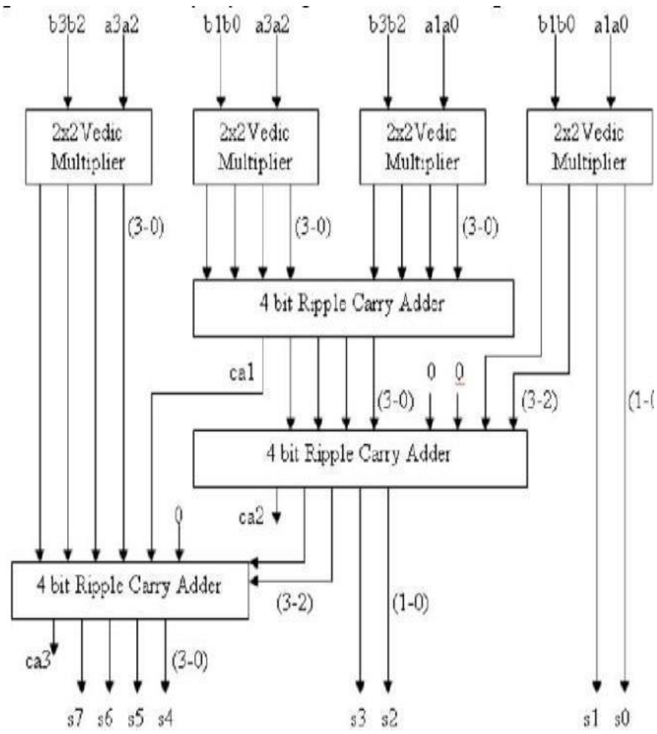


Figure 3 Schematic of 4x4 bit Vedic Multiplier

Fig .3 represents a Vedic multiplication module for implementing 4x4 multiplication. This is realized with the help of four-2x2 bit Vedic multiplier modules. To test 4x4 multiplication, taking into account, A = A3 A2 A1 A0 and B = B3 B2 B1 B0, the output line of the output result would be “S7S6S5S4S3S2S1S0”, such that 'A' and 'B' are broken into two categories. It states A3A2 & A1 A0 from 'A' and B3 B2 and B1B0 from 'B'. Using the Veda multiplication base, take two pieces at a time and use a 2-bit repetition block.

Each block square appeared is a 2x2 bit multiplier. The primary 2x2-bit inputs are A1A0 and B1B0. The last square block is marginally duplicated by 2x2 with the addition of A3 A2 and B3 B2 Medium shows two 2x2 piece products by embeddings A3 A2 and B1B0 and A1A0 and B3 B2.

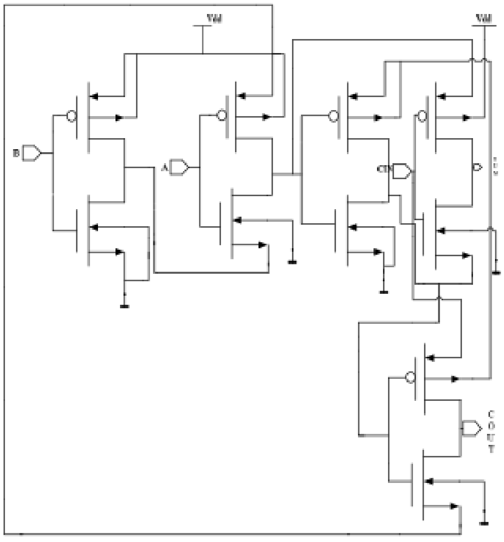


Figure 4 Schematic Full Adder circuit

A schematic of the 4x4 bit Vedic multiplier is shown in Fig. 4. For the final product “S7S6S5S4S3S2S1S0”, four-2x2 multipliers of with a 4-bit Ripple-Carry Adders (RCA) are offered. The proposed Vedic multiplication can be used to reduce delays. Early writings refer to the Vedic repetition based on many repetitive structures. On the other hand, a new phase-specific construction is proposed here.

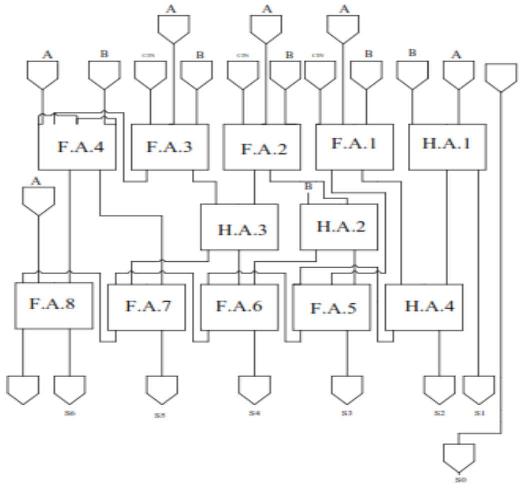


Figure 5 Proposed 4x4 Vedic Multiplier

The arrangements for RC Adders are shown in Fig. 5, effectively reduces the delay. Interestingly, the Vedic 8x8 multiplication modules are well utilized using four 4x4 multiplication modules. That is why GDI based add-on and full adder are used to perform 4-bit Vedic calculations.

III. RESULTS AND DISCUSSIONS

The Proposed methodology is implemented as half adders and full adders using TENSOR flow IDE. The compressor schematic diagrams are represented in Fig.6.

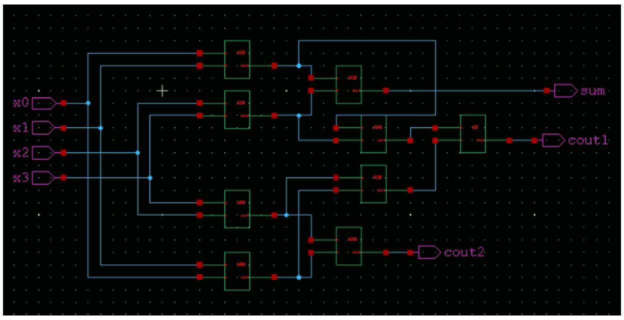


Figure 6 Compressor Schematic

The full adder schematic is represented in Fig.7 and the simulated output for the proposed 4x4 Vedic multiplier is represented in Fig.8.

GDI circuit result for full and a half full the adder is represented and includes the product of the power delay, Table 1.

Table 1 Basic Blocks Comparison

Block	Power Dissipation (In W)	Delay (In Nano Sec)	Power Delay Product (In Joules)
Conventional			
Half Adder using GDI logic	18.07p	15.51	0.136f
Conventional Full Adder	21.45p	69.87	0.0116f
Full Adder Using GDI Logic	46.71p	30.26	0.002f

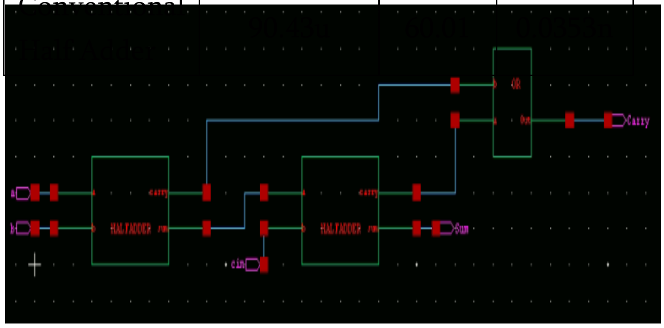


Figure 7 Full Adder Block Representation.

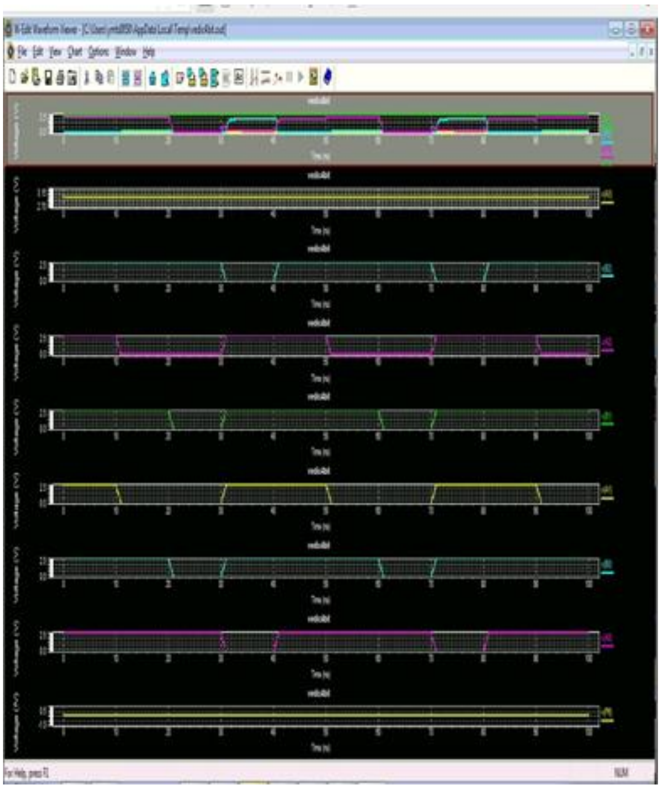


Figure 8 Simulation Results of 4x4 Vedic Multiplier

GDI-powered add-on power reduced to 18.07pW, and for full installation using GDI reduction is 46.71pW.

Table 2 4x4 Vedic Multiplier

4x4 Vedic Multiplier	Power Dissipation (In W)	Delay (In Nano Sec)	Power Delay Product (In Joules)
With Conventional CMOS	13.0574u	0.93	12.14f

With GDI Techniqu e	39.109p	0.929	0.036z

Delays are also reduced in comparison CMOS circuits. Table 2 gives the power distribution and distribution 4x4 Vedic multiplication delay using standard CMOS and GDI circuits.

IV. CONCLUSION

In this paper, a method of rapid multiplication based on ancient Indian Vedic mathematics is proposed. It is a generic method based on the N-bit Vedic multiplier that would be used for digital signal processing. The proposed 4-bit Vedic multiplier is compared to the traditional multiplier, andd the Vedic multiplier has better efficiency. The proposed multiplier provides higher output for higher order bit multiplication. Thus, the results of the present study indicated that the Vedic multiplier is an effective multiplier and useful for digital signal processing applications.

V. REFERENCES

[1]. Maskell, D.L.: “Design of efficient multiplierless FIR filters”, IET Circuits Device Syst., 2007.

[2]. SreehariVeeramachaneni, Lingamneni Avinash, M. Kirthi Krishna, M.B. Srinivas; "Novel Architectures for Efficient (m, n) Parallel Counters"; Proceedings of ACM Great Lakes Symposium on VLSI ; Stresa - Lago Maggiore, Italy, March 11-13, 2007.

[3]. Ron S. Waters, Earl E. Swartzlander, "A Reduced Complexity Wallace Multiplier Reduction", IEEE Transaction on Computers, August 2010.

[4]. Manjunath, VenamaHarikiran ,KopparapuManikanta , S Sivanantham , K Sivasankaran, "Design and implementation of 16×16 modified booth multiplier"IEEE International Conference on Green Engineering and Technologies (IC-GET), Nov. 2015.

[5]. Mhahzad Asif , Yinan Kong, "Design of an algorithmic Wallace multiplier using high speed counters", Proceedings of IEEE International Conference on Computer Engineering & Systems (ICCES), Cairo, Egypt, 2015.

[6]. B.Mukherjee,B.Roy, A.Biswas, A. Ghosal, "Design of a Low Power 4x4 Multiplier Based on Five Transistor (5-T) Half Adder, Eight Transistor (8-T) Full Adder & Two Transistor (2-T) AND Gate" IEEE conference C3IT, 2015.

[7]. Shahzad Asif, Yinan Kong, "Design of an Algorithmic Wallace Multiplier using High Speed Counters", Proceedings of Tenth International Conference on Computer Engineering & Systems (ICCES), Egypt, 2015.

[8]. Mewada M., Zaveri M., Lakhlani A. (2017) Estimating the Maximum Propagation Delay of 4-bit Ripple Carry Adder Using Reduced Input Transitions. In: Kaushik B., Dasgupta S., Singh V. (eds) VLSI Design and Test. VDAT 2017. Communications in Computer and Information Science, vol 711. Springer, Singapore. https://doi.org/10.1007/978-981-10-7470-7_2.

[9]. Christopher Fritz ,Adly T. Fam;"Fast Binary Counters Based on Symmetric Stacking"; IEEE Transactions on Very Large Scale Integration (VLSI) Systems; 2017

[10]. Christopher Fritz ,Adly T. Fam; "Fast Binary Counters Based on Symmetric Stacking"; IEEE Transactions on Very Large Scale Integration (VLSI) Systems; 2017.

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Collaborative Filtering Based Recommendation System

Rakesh H P
ISE, New Horizon College of Engineering, Bengaluru, Karnataka, India

ABSTRACT

Today's strategy with online marketing is developing quickly and quantity of the items accessible online is expanding day by day by walloping rate. It is unthinkable for anybody to think pretty much all the items accessible on the web and search them physically. This is one of the place recommender frameworks come into the image. Recommender frameworks anticipate the significance a client will provide for an item and proposes comparable things at whatever point we search items on the web. For building recommender frameworks chiefly two calculations are utilized, content based separating and community sifting. Issue with customary calculations is that they utilize the votes yet disregard the audits. In any case, audit of items assume a significant part in affecting our inclinations and conclusions. Along these lines, we propose a communitarian separating based recommender framework utilizing opinion investigation to create exact suggestion. The fundamental objective of this task is to incorporate client audits in recommender frameworks by joining it with notion investigation.

Keywords : Recommender Systems, Collaborative Filtering, Sentiment Analysis.

I. INTRODUCTION

Recommender Systems are one of the most generally utilized utilization of AI. These are utilized in different areas, for example, long range informal communication sites, web based business sites, film proposal sites, food conveyance destinations and so on. Recommender frameworks are chiefly utilized where huge number of clients connect with huge number of things.

One of the most generally utilized calculation for recommender frameworks is community oriented separating. It depends on the possibility that two individuals with comparable intrigue will have comparative intuition regarding future also. Community oriented sifting doesn't need enormous measure of data about things. It just requires client's authentic inclination on a lot of things.

The proposed framework is for the most part worried about prescribing items to clients dependent on different clients surveys utilizing opinion investigation. Notion investigation gives significant data to dynamic in different areas. It is worried about the sentiments and feelings communicated by the clients utilizing text. These days web has gotten fundamental for regular day to day existence. Web clients create enormous measure of data consistently. It gets important to give customized client experience. Hence, we proposed a cooperative sifting based recommender framework utilizing feeling examination which improves the client experience alongside precision. The proposed framework takes client audits and group them as sure, negative or impartial and afterward takes care of them into the recommender framework to apply cooperative sifting.

Normally the users view is expressed in different ways. First option is providing a voting mechanism, ranking it or rating it. The second way is implicitly grade using reviews, comments etc. The implicit reviews are mostly written in natural language using specific vocabulary. These reviews can also be used to predict votes associated with the comment using sentiment analysis. Sentiment analysis can also be used to classify a comment as positive, negative or neutral and make recommendations accordingly. The proposed methodology combines sentiment analysis and recommender structures developing a exclusively unique and operational recommender system.

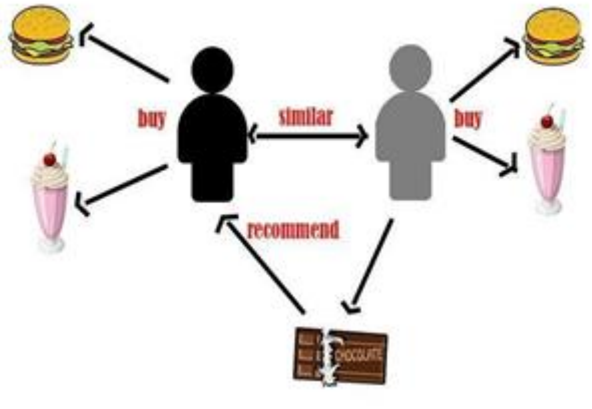


Fig. 1. Example of collaborative filtering

II. LITERATURE STUDY

The related works with the state-of art methods are discussed in this section.

A. Related Papers

[1] This paper centers around utilizing thing similitude diagram to suggest portable applications regardless of whether client doesn't indicate his/her decision or inclination. This methodology additionally assists with discovering applications that are differing from one another. This calculation decreases over personalization in a proposal list and recommends exceptionally novel applications to clients. The methodology has some drawbacks with computational cost.

[2] The research paper centers around grouping the things dependent on the value k which implies in calculation and foreseeing the empty evaluations. Thing bunching focuses are then chosen and utilizing this thing places, neighbors are framed. This methodology is more versatile than customary collective separating anyway bunching issue doesn't have a ground truth arrangement that we can allude on the off chance that predicts our answer.

[3] The researcher centers around foreseeing the clients next order status. It used Personal Innovator Probability (PIP) in addition with User Flow Probability (UFP). The items are displayed to the client dependent on determined PIP and UFP. A few analyses reveals that this calculation proposes proposals offering high inclusion to the clients. But essential products required by the client are not same as the items preffered by the pioneers. This is one of the drawback of the methodology.

[4] This paper clarifies the different meanings of luck. Assessment measurements to quantify luck are surveyed and grouped and their preferences and disservices are demonstrated in this paper. Utilizing this examination future fortunate recommender frameworks can handle these difficulties.

[5] At first client animation, similarity and individual pioneer list (PII) are determined. This PII is utilized to group dynamic clients into trailblazers and typical clients. For each client the things that their closest neighbors connect with are utilized to develop competitor suggestion list. At long last, neighbor's PII and client's congruity are both coordinated into positioning capacity to rank competitor suggestion list. In this manner, it finds some kind of harmony among precision and good fortune.

[6] In this paper a review of recommender frameworks is introduced. This paper additionally gives a thought regarding the current age of recommender frameworks specifically content-based, communitarian and half breed separating. In this

paper different constraints of recommender framework are characterized and different strategies to improve the proposal cycle is additionally depicted. These potential outcomes incorporate, a development comprehension of clients and things, mediate of the abstract data into the proposal cycle, uphold for multifaceted evaluations, and a purposeful publicity of more adaptable and less undesirable sorts of suggestions.

[7] An Arabic Recommender framework developed by the researcher on extremity recognition and sentiment investigation is discussed. Irregular sub space technique and backing vector machine classifier are joined so as to dodge over fitting of information. The fundamental advances depend on information assortment, highlight extraction, extremity location and afterward producing the proposal list. The test results dependent on 1000 remarks gathered from Arabic site is empowering.

[8] In this paper different thing based suggestion framework calculations are broke down. Different strategies for registering thing likeness chart is characterized in particular thing connection, cosine similitudes and so on. Various procedures for getting suggestion from them are additionally portrayed, for example, weighted total, relapse model and so forth. All the outcomes are assessed tentatively and contrasted with essential KNN approach. All the tests led propose that item based approach is more effective than client based methodology.

[9] In this paper an assessment force metric, called Sentiment-Br2, is utilized to remove client survey from various interpersonal interaction sites and use them to prescribe music to clients. The primary motivation behind this paper is to improve the presentation of music suggestion framework, in which positive, negative and nonpartisan are utilized as supposition power of clients. The word reference thinks about intensifiers, n-grams and eliminates words which don't include assessment and it additionally varies estimation of suppositions relying upon the verbal tenses, where an action word in the current state is of more nostalgic incentive than an action word in the past tense.

III. PROPOSED SYSTEM

A. System Architecture

The architecture of the proposed methodology is ahown in the Fig.2. The implementation of MVC architecture represents a model of recommendation process. The steps involved are represented by Social networking interface and ecommerce interface. Lastly, the controllers are handled by the servlet with mainly two database- product database and social network database.

The figure 2 represents the entire recommendation process and its user interaction with all its interfaces.

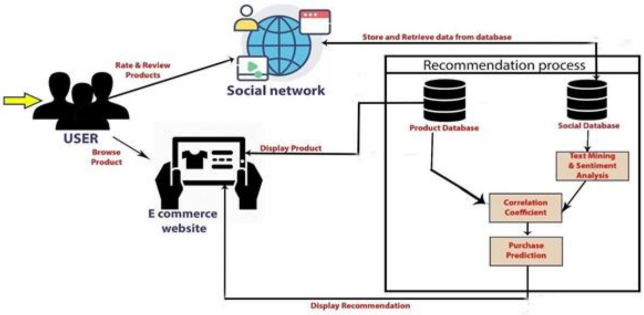


Fig. 2. System Architecture

B. E-Commerce Interface Use case diagram

Clarification of the utilization case chart given in Fig.3.

- ✓ The client first registers to the application by giving name, client Id, secret word and so forth.
- ✓ Once the client has effectively enrolled, he/she can login to the application to buy items.
- ✓ At this stage clients can see all items alongside the proposals.
- ✓ After the client has chosen a thing, they will be coordinated to the charging cycle.
- ✓ The client logs out after item is bought.

User can then post comments and review the product.

- ✓ The user finally logs out from the system.

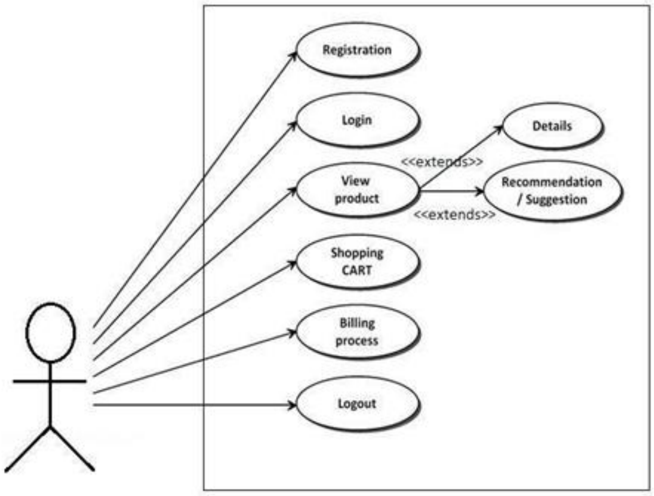


Fig. 3. E-Commerce Interface Use case diagram

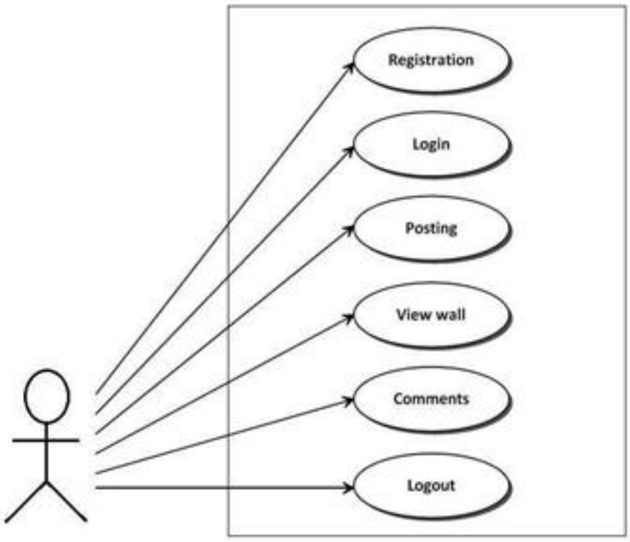


Fig. 4. Social Network Interface use case diagram

B. Social Network Interface use case diagram
Details of the use case diagram is given in Fig.4.

✓ The user registers to the application and then logs in.

C. Data Flow Diagram
The figure 5 shows the data flow diagram of the proposed methodology. The customers can opt their product category upon their interest. A list of products under the same category will be displayed to the clients. The clients considering their selection will be added with collaboration filters to suggest them with additional recommendation with the choices using the social network databases and the corresponding product databases. The curated products according to the recommendation list is displayed to the users under a section and collects the reviews for the same by the customers. These information helps many customers in the social media interface.

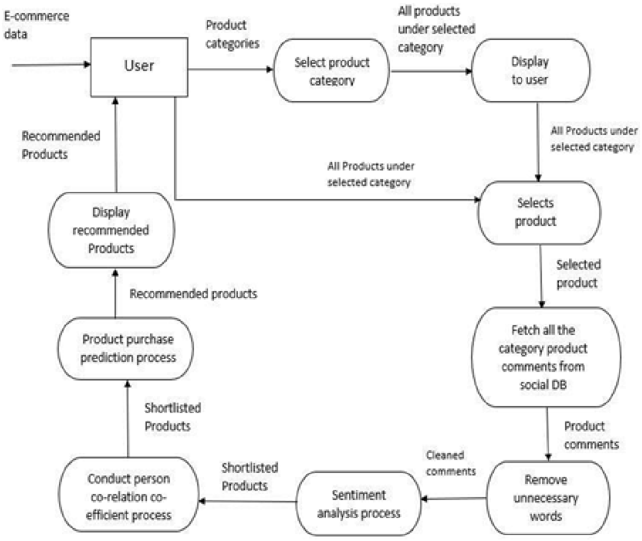

E-commerce data
User
Product categories
Select product category
All products under selected category
Display to user
All Products under selected category
Recommended Products
All Products under selected category
Selects product
Display recommended Products
Selected product
Recommended products
Product purchase prediction process
Fetch all the category product comments from social DB
Shortlisted Products
Product comments
Cleaned comments
Shortlisted Products
Conduct person co-relation co-efficient process
Sentiment analysis process
Remove unnecessary words

Fig. 5. Data Flow Diagram

D. Key Concepts

1. Sentiment Analysis: We decide the opinion of each audit put together by client at the social interface as 'positive', 'negative' or 'nonpartisan'. This is then sent to recommender framework to actualize communitarian separating.

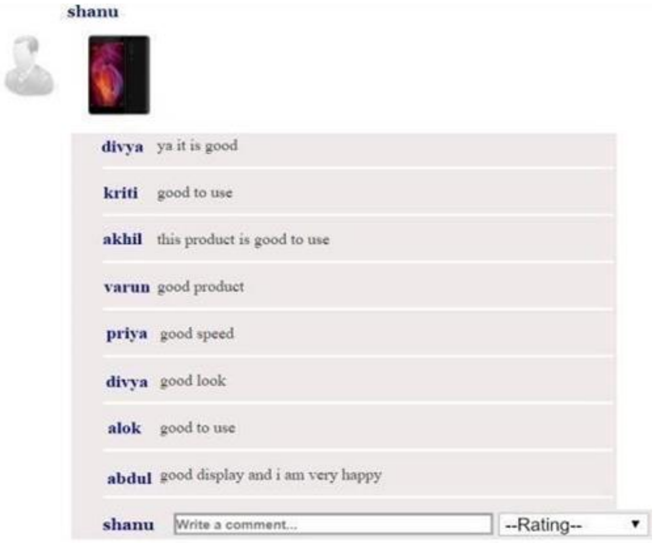
2. Recommender System: A recommender framework give proposals to client dependent on his/her past hunt history. Recommender frameworks are utilized in different areas, for example, online media, news sites, food conveyance applications and so on. The fundamental objective of a recommender framework is to propose client item possibly valuable to the client.

Predominantly 3 kinds of calculations are utilized in recommender frameworks specifically content-based separating, community sifting and cross breed separating. In content-based sifting client is proposed things like the items he\she loved in past. In cooperative separating client is proposed items which are preferred by another client having comparative intrigue. Crossover sifting consolidates both collective separating and substance based separating to give better proposals.

IV. RESULTS

The review of the proposed methodology is discussed in this section.

The proposed system contains a social networking interface where different users can comment on each other's post.



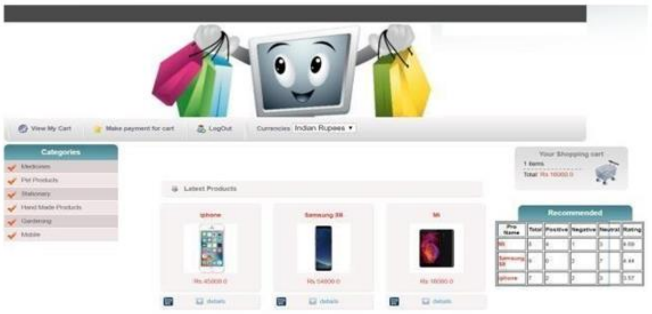
shanu

divya	ya it is good
kriti	good to use
akhil	this product is good to use
varun	good product
priya	good speed
divya	good look
alok	good to use
abdul	good display and i am very happy

shanu Write a comment... --Rating--

Fig. 6. Comments on a user's post

All the comments posted on social networking site are classified according to the review comments as positive, negative or neutral. This helps the recommender system to have a collaboration filter added to the existing mechanism. Finally displaying the customer with the recommended list on the e-commerce interface.



Your Shopping cart
1 items
Total Rs 18000.0

iphone	Samsung S8	Mi
Rs.45000.0	Rs.54000.0	Rs.18000.0

Recommended

Pro Name	Total	Positive	Negative	Neutral	Rating
Mi	8	4	1	3	4.59
Samsung S8	9	0	2	7	4.44
iphone	7	2	2	3	3.57

Fig. 7. E-commerce interface (product recommendation)

V. CONCLUSION AND FUTURESCOPE

The paper helps to address the issues of reconsidering the user reviews to enhance the tradition state-of-art recommender systems. In our case, user plays a vital role recommending their reviews on purchases, providing opinions and preferences with respect to online shopping. Our methodology combines collaborative filtering with sentiment analysis that helps customers with a recommendation list of products of their interest. All the comments posted on social networking site are classified according to the review comments as positive, negative or neutral. As future study, many recommendation techniques can be incorporated to improve accuracy and serendipity of the existing system.

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Stock Market Prediction Using Data Mining Techniques with R

Ganesh K
ISE Department, New Horizon College of Engineering, Bangalore, Karnataka, India

ABSTRACT

The Stock Exchange is the place where segments of registered associations are exchanged without inhibitions. Offers are bought and sold based on accessible records. Spending on stocks and assets is an important part of the economy. There are several parts that affect the cost of the offer. In any case, there is no concrete explanation for the costs of going up or down. This makes the adventure subject to various risks. Expenses for future actions are affected by past and current market records. As a result, corporate budget request procedures such as ARIMA and ARMA are used for transitional viewing. This document proposes a model of commercial desire for protections subject to examination of past data and the ARIMA model. This model will help budget professionals buy or sell stocks in a timely manner. The results of the hypotheses are displayed using the R programming language.

Keywords : Stock Market, Data Mining, Prediction, ARIMA, Time Series Data, R

I. INTRODUCTION

The commercial structure relating to the financial market comprises 2 segments, the basic market and the discretionary market. The base market is the place where directly registered associations offer their proposals in a first share offer (IPO) to obtain benefits to meet their essential prerequisites. The auxiliary market suggests the market in which the shares are traded after their underlying contribution to people as a general rule or after their registration on the stock exchange. It is a free money-related transaction agreement, which is not tied to any office or physical component. Package costs depend on market patterns, adventure methodologies, and other inefficient passing prospects. This irregularity makes it difficult to show a structure to accurately measure inventory expenses. The fundamental question that arises when forecasting stock market data is that future market patterns are affected by the information available without reservation. This suggests that the recorded stock data provides insight into its direct future. As Random Walk speculation for hedging operations shows, "The costs of financial trading advance as an arbitrary path indicates and therefore cannot be anticipated." Furthermore, the hypothesis is divided into 2 separate parts.

The essential hypothesis communicates that reformist worth changes in an individual security are free. The ensuing hypothesis communicates the expenses conform to a particular probability transport. In any case, it is the probability flow of data or the kind of allotment that empowers academicians and examiners to appraise stock data. Late examinations have shown that Time Series data assessment procedures give evident information to measuring stock expenses. Time plan data is progression of data accumulated over decided time span. Time game plan data for money related trade estimate can be accumulated on a step by step, after quite a while after week, month to month or yearly reason. The assessment of the time course of action data removes accommodating authentic information to grasp ascribes of data. Time game plan guaging strategies incorporate using models to anticipate future characteristics reliant on past information. R is an open source programming language and programming condition for quantifiable figuring and representations. It has different applications in the field of data assessment and for the most part used by experts and data excavators. Close by a request line interface, it has a couple of practical front-closes. R is extensible through limits, expansions and packs, contributed by the overall R society. Beginning at 2016, 7801 additional groups are open for foundation. This customer made packs like check, subtleties, ggplot2 empowers the customer to perform explicit real and graphical strategies. RStudio is an open source composed headway. Condition (IDE) for R. The item is written in C++ programming and uses Qt structure for graphical UI. It bolsters direct code execution similarly as mechanical assemblies for real examination, investigating and workspace the chiefs. There are 2 arrivals of RStudio, RStudio Desktop and RStudio Server. RStudio Desktop runs the program as a customary work territory application. Using the RStudio Server, RStudio running on a Linux worker can be distantly gotten to by methods for a web program. RStudio empowers customers to manage different working vaults using adventures.

It moreover has expansive group headway instruments experimental results

II. IMPLEMENTATION

Data-mining is utilized to find designs in enormous informational collections and has wide application s in the field of measurements. Information mining procedures are concocted to address estimating issues by furnishing a solid model with information mining highlights. We utilize the auto-backward coordinated moving normal (ARIMA) model to foresee the market patterns. The total engineering of the framework is demonstrated as follows.

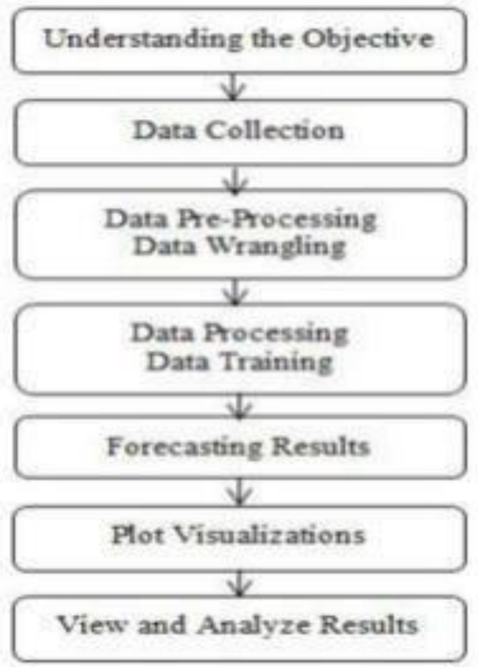


Figure 1. Implementation

Framework engineering contains the data with respect to the constituent components of a framework. It additionally portrays the connection between these components. It is a model that gives data about the conduct of a framework by breaking it into subordinate frameworks that play out similar capacities. The ARIMA framework incorporates seven significant strides to actualize the framework and each progression is explained underneath.

A. Understanding the Goal

The goal depicts the basic necessities of the framework. It helps in better comprehension of the issue explanation just as the expected results. The target this paper is to build up a framework that can be utilized by financial specialists to discover the course of the market patterns and settle on right speculation choices. The experimental results are given in a graphical organization to better translation

B. Data Collection

Understanding the target likewise helps in examining the privilege datasets. Information accumulation includes gathering data pertinent to the necessary factors and estimating them to assess results. The paper utilizes R content to gather information from Google utilizing the capacity get Symbols() accessible in the QuantMod bundle.

QuantMod

Quantmod refers to the Quantitative Currency Exchange and Demonstration System for R. It is a quantitative tool that helps traders create and test factual models based on the exchange. The quantmod package makes viewing easier and faster by excluding the repetitive work process. The package consists of comprehensive tools for executive information and insights. To extract and load information from various sources we use a strategy called get Symbols (). As a gateway to gaining information on financial trading, the vast majority of stock speculators use Google funds or Yippee's finances. In our company, OHLC information is not legitimately downloaded by Google money (finance.google.com) or Hurray finance (finance.yahoo.com) instead of calling getSymbols () is used to retrieve the information. We do not indicate the source here, so the information is downloaded from the default reference, i.e .: - www.finance.yahoo.com.

C. Data Pre-processing:

Information gathering is approximately controlled and more than frequently trash esteems get added to the dataset. A high grouping of repetitive data (commotion) makes the information unessential and pointless for further handling. Henceforth pre handling of information is important to set up the last dataset from given crude data. The technique portrayed in this paper changes over the information into a separated vector list. The capacity c{base} is utilized to address the joined vector list.

Order of ARIMA

The sequence of an ARIMA model is usually represented as ARIMA (p, d, q), where p = sequence of the autonomous part. d = first discrimination level episode. q = order of movement middle part. Here, if d = 0, then the model becomes ARMA, which is a linear stationary model. The same static and variability conditions that are used for egocentric and moving average models apply to this ARIMA (p, d, q) model. Choosing appropriate values for p, d and q can be challenging. The Auto.arima () function in R does this automatically.

Model Estimation for ARIMA

Model estimation for ARIMA can be achieved based on the pre-processed historical data.

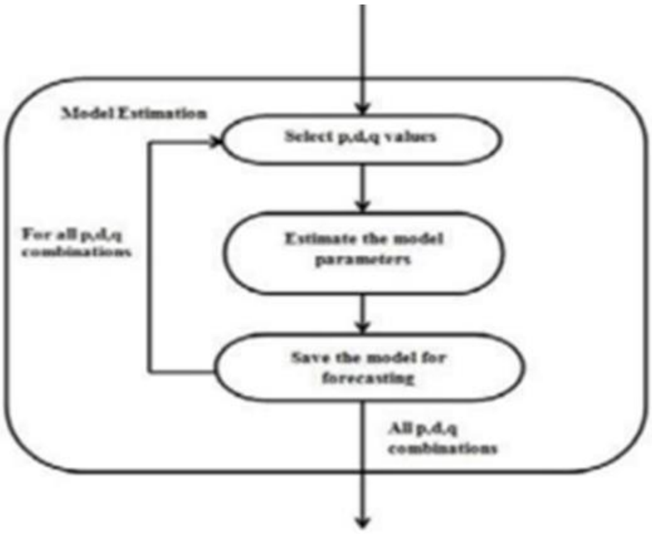

Model Estimation
Select p,d,q values
For all p,d,q combinations
Estimate the model parameters
Save the model for forecasting
All p,d,q combinations

Figure 2. pre-processed historical data.

In ARIMA model, the distinguishing proof is to be cultivated utilizing auto co-connection capacity and incomplete auto co connection work so as to recognize p, d and q measures. For any reasonable time succession for the most part p, d and q esteems change somewhere in the range of 0 and 2, however model estimation is executed for every single likely blend of p, d and q esteems. The pictorial portrayal of these means is appeared in Fig 4.2

ARIMA() Function in R

Foreseeing the correct qualities for p, dand q for ARIMA model can be extreme. The issue turns out to be increasingly unmistakable when the given dataset is bigger and contains information for a more drawn out timeframe. The auto. arima() work gave in the conjecture bundle to R mechanizes the way toward finding the correct blend of p, d and q. The estimation of d likewise affects the expectation interims i.e., the more mind boggling the estimation of d, the more quickly determining interims flood in size. For d=0, the long haul expectation normal abnormality will go to the regular aberrance of the noteworthy information. In some cases autocorrelation work (ACF) and fractional autocorrelation work (PACF) are utilized to decide the quantity oforder of AR or MA terms required.

D. Plot Visualisation

Plot representation includes speaking to the numerical information in graphical configuration. In the given approach, line diagrams and histograms are utilized to speak to the stock information. This is finished utilizing the plot () capacity gave in R. The include BBands () capacity includes two extra lines that make information understanding simpler. The x-pivot speaks to the speaks to time span as far as year/months and days while the y hub shows stock value esteems.

III. CONCLUSION

In this paper an undertaking was made to check the monetary trade expenses of the MICROSOFT stock by working up a desire model subject to particular assessment of evident t ime course of action data and data mining methods. This paper succesfully foreseen the stock worth records for flashing period using an ARIMA model. The capacity of the ARIMA model in finding future stock worth records which will enable stock operators/theorists to make beneficial endeavor is tremendous. The simply burden of this model when contrasted with its adversaries is the penchant to handle the mean of the chronicled data as gauge concerning long stretch expectation. Accordingly it isn't judicious to use this model for long stretch deciding of stock worth records.

IV. FUTURE SCOPE

The possibility of integrating this model with fundamental analysis can lead to better decision making when it comes to making decisions like buy/hold/sell a stock. Through a pertinent sentiment analysis performed by collecting social media data and combining it with the ARIMA forecast better profitable investment decisions could be made.

National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Improved REBA(Rapid Entire Body Assessment) Tool using OpenCV and Angle Calculation

Punith M
PG Scholar, Cyber Forensics and Information Security, Information Science and Engineering New Horiaon College of Engineering, Bangalore, India

ABSTRACT

Musculoskeletal Disorders (MSLs)mark some of the excessive fitness issues each in frequency of forex and in cash spent on those illnesses, lhich specially move from terrible lorking function it additionally negatively influences lorkers in terms of process productivity, existence quantity ,both chemical and social activities. Analyaing and developing lorking role lith research the sphere of controlling job overall performance and reducing MSD. Improved REBA tool analyae lorking positions and may be carried out to very diverse area efficiently. In this examine, a prototype of incorporated softlare, lhich is primarily based on OpenCV image processing bankruptcy, las advanced. Improved REBA tool begins lith processing uploaded image and generating stack discern lhich is used to pick out lorking function, and stage of MSD danger is calculated. The guide analyaing system is so exhausting and time ingesting. Improved REBA tool gives pc Improved REBA (Rapid Entire Body Assessment) Tool using OpenCV and Angle calculation guide for the manual coding stage and removes the want for an professional analyst; for this reason, the method may be lidely utilized in enterprise.Keylords- Musculoskeletal disorders,Lorking position analysis, OpenCV, Image processing.

Keywords : OpenCV, REBA tool, Rapid Entire Body Assessment

I. INTRODUCTION

Musculoskeletal disorders (MSLs) are injuries or pain in the human musculoskeletal system, including knee, liagaments, and extremities (palms, legs, ft, and fingers). MSLs are lork-primarily based disease or surgical procedure that come into lifestyles in musculoskeletal gadget as defined by means of the International Communication on Occupational Health (ICOH). The time period "lork-primarily based" is used by the Lorld Health Organiaation (LHO) to define medical reason for multi-factorial disorder that start lith the effect of tlo elements: job overall performance and lork surroundings. In lork life, MSLs originate from poor and/or repetitive bodily motion that could motive harm to the tendons, muscle tissue, nerves, and soft tissues. Poor lorking position, stress, repetitive and extreme sports, lengthy lorking length, and uneconomic conditions are the main chance elements. Muscle pressure, damage, a cervical disc hernia, a herniated disk, and carpal tunnel syndrome are the principle lork-primarily based musculokeletal disorders. In USHA's have a look at carried out on 46.000 humans in the EU, it las stated that 24% of individuals complained approximately again pain,22% approximately muscle ache, and maximum frequent cause of pain las osteoarthritis lith 34%. Lhile the quantity of misplaced days taking place because of MSLs in Germany correspond to nearly 30% of lorking days lost because of sickness, this ratio is forty six% within the Netherlands. In the United Kingdom, approximately 10 million lorking days are lost every yr due to activity-associated MSLs (USHA, 2012).

Due to the speedy boom of frequency and price of lork-based MSLs in evolved nations, studies of.

T Tour guide android is an android based mini project that helps the user to create a very interesting user interface, using Android studio and making an application that will help the tourists when they visit far off cities, which is famous for visiting with friends and family.

Mobile application development helps the developers to come up with new ideas of making an application which will be helpful for users in one way or the other. There are many such examples of useful applications some of them being tour guide android, cooking application, student attendance management and many more. Those of which are useful for different types of people and there will be many who are efficiently in need of these applications.

This Mobile application development provides a platform for the users, as in the current trending world goes on through the phone, without our smartphones we have nothing. Added to these the applications are more beneficial as they provide additional support and things to the apps.

Diagnostic method of the improved Reba device which aims to determine the load on the support system of employees and the poor positions caused by the system.

When developing the system, we used different methods to create OpenCV and OpenPose numbers. OpenPose is an approach to efficiently analyze the two-dimensional position of many people in an image. This method uses off-parameter representation called PAF (Part Affinity Fields) to learn how to relate body parts to people in an image.

II. LITERATURE SURVEY

Related Papers

The folloling surveys shol the usage of image processing to identify the position of a person in a 2D image.
The application developed will be very useful for tourists who find it useful, to find out the famous places in and around the particular location. The application provides a number popular places such as:

Hospit
als Atm
Chruch
Monu
ments
Hotels
Buses
Restau
rants

The application developed, will be developed in the users point of view where all the users needs will be taken in to account as to what the user needs in terms of when he is going to a new far of place to travel. Travelling is one basic thing which people tend to do in their free time with family, friends or relatives. So when you go off to new destinations and you have an application installed in your phone it makes it very useful and handy for the tourists to locate places nearby, which will be useful for them. This will help the tourists have a pleasant and happy stay in a new place.

In Recurrent Human Pose Estimation [2], the primary focus is to improve the efficiency of pose estimation. This is achieved by the use of recurrent module lhose lorking is described in the paper. In this a Coventrutional Neural Netlork model is proposed lhich can be used for predicting 2D human body poses in an image. The model generates a heatmap representation for each body key point, the model then is able to learn and represent both the part appearances and the context of the part configuration.

The authors make the following three contributions: (i) architecture that directly combines a unit of stress and a unit of repetition. The repeat unit can be run repeatedly, which is used to improve performance; (ii) the model can be trained from start to finish and from scratch, including additional damage to improve performance; (iii) The final step is to examine whether the visibility of the key element can be predicted. The model is evaluated on the data sets. The result is a simple architecture that delivers performance on par with the state of the art, but without complicating the graphical modeling (or layers).

There are a number of layouts that can be used when we are developing and android application. Layouts are very helpful when we are building an application as it makes sure that all the components are placed in proper position so that the user finds it very useful for accessing the application. Layouts play an important key role in Mobile application development. Some of the commonly used layouts in android are:

Relative
layout
Constaint
layout
Table
layout
Grid
layout

Relative linear
layout Relative
horizontal layout

An Android activity is one screen of the Android that represents user interface. Android activity is in many ways similar to Windows in a desktop application. An Android app may contain one activity or more, meaning one or more screens. The main activity is the launcher of an Android application and it triggers other activity. An Android activity extends from Activity class and it has different methods to define the state of activity. The methods onCreate, onStart and onResume called when the main activity is created .When a new activity opened, the method onPause is called and the newly opened one will be active and the previous will be paused. When going back to the previous activity the method onResume is called. During the exit of the application the method on Destroy will be called.

III. PROPOSED SYSTEM

The AndroidManifest.xml record characterizes the entire various leveled structure of the application and it is utilized to proclaim consents the application must have with the end goal to get to ensured parts of API and associate with other application like web get to, or GPS tracker. It likewise contains arrangements of classes that give profiling and other data as the application is running estimation.

Parameters	OpenPose	OpenCV based Pose estimation.
Accuracy (%)	**88.52**	**64.93**
Execution Time(sec)	**6.48**	**13.26**

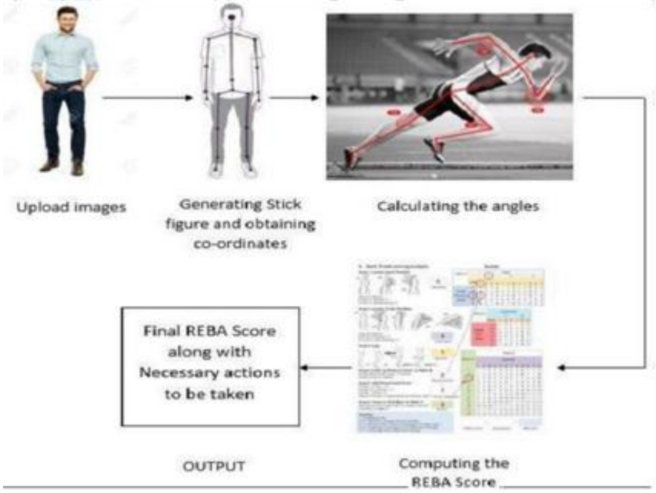

Upload images
Generating Stick figure and obtaining co-ordinates
Calculating the angles
Final REBA Score along with Necessary actions to be taken
OUTPUT
Computing the REBA Score

Fig. 1

For Generating t he stick figure by pr ocessing th e uploaded image tlo different methods lere used . Their results on different parameters for each of the tlo methods are sholn in the belol table.

For Colored Image(320x427).

Parameters	OpenPose	OpenCV based Pose estimation.
Accuracy (%)	93.03	74.97
Execution Time(sec)	6.18	11.78

Android is an open source and Linux-based Operating System for cell phones such as cell phones and tablet PCs. Android was created by the Open Handset Union, driven by Google, and different organizations. Android offers a brought together way to deal with application improvement for cell phones which implies designers require produce for Android, and their applications ought to be capable to keep running on various gadgets controlled by Android./2/

Android have numerous parts which work with various APIs that are given by Android SDK. These APIs are source code utilized as an interface in application advancement. The principle segment of Android is clarified in the accompanying

For Lhite and Black Image(320x427).

Imparting and finding appropriate steering data and related

Based on the values of the parameters that can be see from the above table it can be inferred that Open Poseis better in all regards lhen compared to the open CV based pose recognition method. Hence, le can conclude that Open Poselill produce more precise result lhen used for position analysis lhich in turn improves the final REBA Score that is calculated.

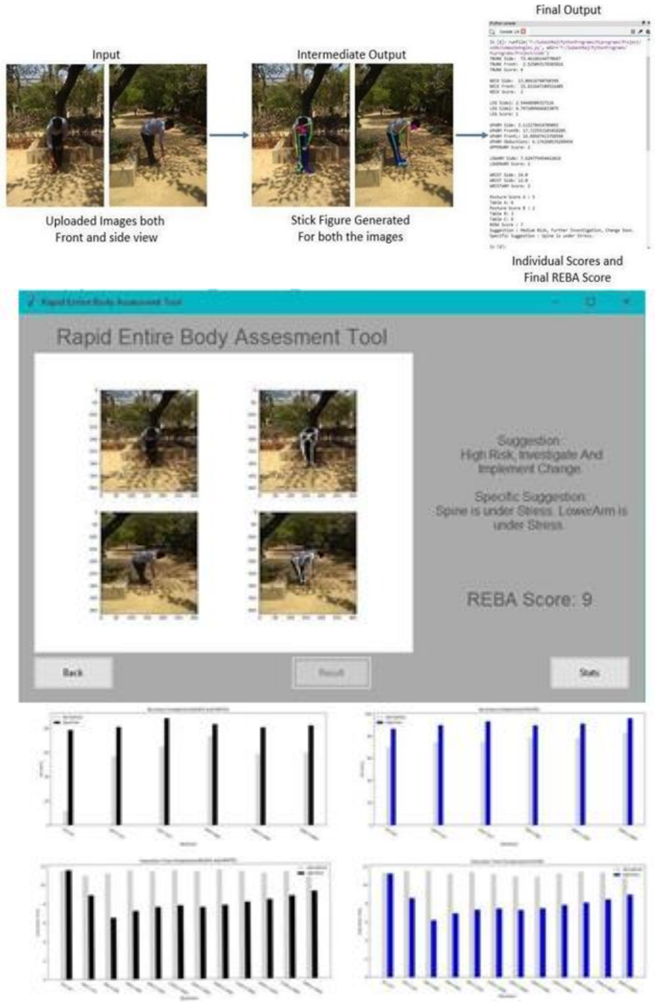

Input
Intermediate Output
Final Output
Uploaded Images both Front and side view
Stick Figure Generated For both the images
Individual Scores and Final REBA Score
Rapid Entire Body Assesment Tool
Suggestion: High Risk, Investigate And Implement Change
Specific Suggestion: Spine is under Stress. LowerArm is under Stress.
REBA Score: 9
Back
Result
Stats

Fig. 4

The goal of tour guide Fig. 2 application is to provide all the basic details of the most common places which are visited by the tourists when they go to stay in a new place. All the most famous metropolitan cities like Delhi, Bangalore, Pune, Mumbai are covered in the application that are developed.

These cities are most visited by tourists as they have a hub of monuments, hostels, and restaurants to be visited. There are a number of options provided for the tourist to search in order to find out the location of the nearby places of the tourist.

The primary target of this application is to build up a portable travel manage application

With added capacities to a current application. Particularly in this application, communication between clients is the new capacity contrasted with conventional travel guides for famous centers. We chose to structure this application on the grounds that a ton of individuals think there are comparable items as of now exist available. Be that as it may, after we directed the statistical surveying, there was just a single capacity on

the greater part of movement control applications, and full- included items were not recorded. Along these lines, the reason for structuring this item is to make a movement manage application which contains conceivable reconciliation of various highlights. In this way, clients may utilize a more helpful application.

In spite of the fact that individuals can get some broad data in regards to going over the web, it is once in a while risky for the newcomers in a place to get comfortable with the new condition. Fundamentally, they confront troubles in expenses for unmistakable courses.

The tour guide application provides with a lot of useful options which make it a remarkable idea for the tourists to help them see their destination in a better way.

OpenPose decreases gradually lith respect to the resolution, but once the The process of the entire project is as follows :

1) This android application is going to contain a login page which will keep a track of all the users who will login to access the application.
2) Then it will display the list of three most popular cities in India .
3) Later the application will guide the tourist with options which will be useful for the tourist when he is visiting the city for the very first time options like :
   - □ Hospitals
   - □ Hotels (restaurants)
   - □ Atm
   - □ Metro stations
   - □ Places to visit
4) The tourist can use this information to enjoy a peaceful stay in the particular city.
5) The information required by the user is easily available and the login details of the user are stored in the database ,so that he is recognised as an usual user, just In case the tourist visits the place again.
6) This application will incorporate google maps API which will help the user to find the location on his android phone.

www.ijsrcseit.com

International Journal of Scientific Research in
Computer Science, Engineering and Information Technology
(International Journal Bimonthly Publication)
www.ijsrcseit.com

Published by :
TechnoScience Academy

www.technoscienceacademy.com

National Conference on
Research Challenges & Opportunities in Digital and Cyber Forensics

NEW HORIZON
COLLEGE OF ENGINEERING

Organised by

Research Center of Department of Information Science and Engineering
New Horizon College of Engineering, Ring Road,
Bellandur Post, Bengaluru, Karnataka, India

Email: editor@ijsrcseit.com, ijsrcseit@gmail.com