ISSN : 2456-3307

KLE BCA
ADAPT | ADHERE | APPLY | ACHIEVE

KARNATAK LINGAYAT EDUCATION SOCIETY

IJSRCSEIT

National Conference on Communication Technology & Network Security (NCCTNS-2019)

Organised by
Bachelor of Computer Application
KLE Society's S.Nijalingappa College
Rajajinagar, Bengaluru, Karnataka, India

Scientific Journal Impact Factor Value 2017 = 4.032

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

Volume 4, Issue 7, September-October-2019

Email: editor@ijsrcseit.com

National Conference on Communication Technology & Network Security

(NCCTNS-2019)

11th Oct 2019

Organised by:

Bachelor of Computer Application, KLE Society's S.Nijalingappa College, Rajajinagar, Bengaluru, Karnataka, India

In Association with

International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

Volume 4, Issue 7, September-October-2019

International Peer Reviewed, Open Access Journal

Published By

Technoscience Academy

Website URL : www.technoscienceacademy.com

About SNC

KLE's S.Nijalingappa College, established in the year 1963,and has earned significant laurels for its services of more than half a century. Prominent among these are the rare distinction of having been re-accredited at A+ grade with CGPA 3.53 in the 3rd cycle of accreditation by NAAC. UGC has recognized KLE SNC as College with Potential for Excellence(CPE).

The college has always provided a platform to students with diverse needs for the evolving higher educational scenario at global level. Credit of having organized consistent and orderly sponsored seminars, conferences and workshops is an added feather to our crown.

About BCA

BCA @KLE started in the year 2000 with a vision to make students employable in IT industry wherein both human values and technology are well blended. "Smart classes and close mentoring relationships between students and faculty" is more than a tagline at KLE BCA; it's a long-standing hallmark and a true point of distinction.The course empowers the students by preparing them to adapt, adhere, apply and achieve balance and excellence in their career; thereby empowering them to add value to industry and society at large.

About Conference

In the age of universal digital connectivity of viruses, hackers, electronic eavesdropping and fraud, there is indeed no time at which security does not matter.

Two trends have come together to make the topic of this conference a matter of vital interest.

- First, the explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This, in turn, has led to an increase in awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of the same and to protect systems from network-based attacks.
- Second, the disciplines of network security has matured, leading to the development of practical, readily available applications to enforce network security.

The purpose of this Conference is to explore practical views and ideas of both the principles and practice of cryptography and network security. We at KLEBCA look forward to valuable ideas that would have important practical implications in future.

Objectives of Conference

- To empower participants with quality information on emerging techniques on Network Security
- To identify and analyze the impact of security for business which have legal obligations to keep client data secure
- To discover the tactics to maintain confidentiality, integrity and authenticity in Network Security
- To find approaches to curtail high – profile hacking cases
- To evolve different service models of software

Main theme - Communication Technology &Network Security

- Sub - themes
  1. Sensor/Ad-hoc Networks
  2. NextGeneration Networks and Services
  3. Wireless Security
  4. IT and Network Security
  5. Cloud Security

Advisory Committee

1. **Dr. G. Hemanth Kumar**
   Professor &Hon'ble Vice Chancellor,
   Mysore University.
2. **Dr. Hanumanthappa M**
   Professor & Chairman,
   Bangalore University.
3. **Dr. Siddu P Algur**
   Professor,
   RCUB.
4. **Dr. D. S. Guru**
   Professor,
   Mysore University.
5. **Dr. Arun Kumar T**
   Professor,
   VIT, Vellore.
6. **Dr. B. H. Shekar**
   Professor,
   Mangalore University.

Executive Committee

- **Chairperson**

  Dr. Arunkumar B Sonappanavar
  Principal, KLE's S.Nijalingappa College.

- **Organizing Secretary**

  Dr. Parvati N Angadi
  Co-Ordinator, Department of Computer Science.

Organizing Committee

- **Conveners**

  Mr. M. S. Kabbur
  Professor, Department of Computer Science.

  Mrs. Roopa. H. R
  Professor, Department of Computer Science.

- **Co-Ordinators**

  Mrs. DaneshwariAlur
  Assistant Professor, Department of Computer Science.
  Mrs. Priya D
  Assistant Professor, Department of Computer Science.
  Mr.Sagar D
  Assistant Professor, Department of Computer Science.

CONTENTS

National Conference on Communication Technology & Network Security In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Army Security Communication Network - An Review on Inter Tactical Mobile Ad Hoc Network Routing Protocol

Goutham S Tantri, Manjunatha M J
UG Scholar, Department of Electronics and communication, Jawaharlal Nehru National College, Shivammoga, Karnataka, India

ABSTRACT

Mission-critical military operations with dismounted soldiers are frequently characterized by high battlefield dynamics. In such scenarios a mobility model can manage soldiers' movements dynamically especially under enemy attacks. MOBILE armies need mobile communications. Those communications, though, must be secure—and not just from eavesdropping. They also need to be uninterruptible, The battlefield where these equipment are deployed includes a majority of coalition communication. Each group on the battleground may communicate with other members of the coalition and establish inter-MANETs links. Operational communications tend to provide tactical ad hoc networks some capacities. There is a better broadband radio in UHF band (ex: NATO - 225-400 MHz) and some heterogeneous services such as voice or video are provided. Several Network-layer protocols have been proposed in order to handle inter-domain routing for tactical MANETs. One key factor is the much more dynamic pattern of participation of individual nodes in a MANET. Today's operations can be much more ad hoc in terms of the use of unmanned vehicles, or airborne assets .This MANET communication networking comes handy in relocating operations, rescue operation and can even be applied in daily civilian usage

Keywords : Self-Organized Behavior, Mobility Models, Ad hoc Networks, Group mobility, Dismounted soldiers, Battlefield, MANET.

I. INTRODUCTION

Recently, the army has been interested in developing new skills and competencies such as making soldiers more connected in the battlefield based on modern electronic communication equipment and computer technologies by using mobile wireless ad hoc networks (MANETs) . Mobile ad hoc networks are useful in situations where there are no network infrastructures available and when there is a need for people to communicate using mobile devices. Since MANETS are based on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. The intrinsic nature of wireless ad hoc networks makes them very vulnerable to attacks ranging from passive spying to active interference. In mobile ad hoc networks, there is no central administration to take care of detection and prevention of anomalies. However, most of the existing key management schemes are not feasible in ad hoc networks because public key infrastructures with a centralized certification authority are hard and cost ineffective to deploy. Consequently mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to

cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficulties which includes the mobility of the nodes, a promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory. Attacks on ad hoc are classified into non disruptive passive attacks and disruptive active attacks. The active attacks are further classified into external attacks and internal one. External attacks are carried out by nodes that do not belong to network and can be prevented by firewalls and encryption techniques. Internal attacks are from internal nodes which are actually authorized nodes and part of the network , hence it is difficult to identify them. Lot of works had been done in the area of identifying and removal of adversaries in the network. The SMT protocol safeguards pair wise communication across an unknown frequently changing network, possibly in the presence of adversaries that may exhibit arbitrary behavior. Instead of transmitting in single path, the message will be transmitted in multiple paths to ensure reliability. Considering the benefits over the overhead involved in utilizing the multiple paths are increased security, reliability and reduced congestion that is mostly needed for MANETs in military.SMT protocol provides security based on the security association between the end nodes. It is not able to overcome the compromised nodes attacks. And to improve the security and reliability of data transmission in mobile ad hoc networks by providing secured routes. The Byzantine faults are identified and those links will be avoided in the data transmission phase. The current topological information will be gathered based on the network behavior such as transmission time, Probability of lost packets and correctly received – acknowledged packets and a threshold is set which is used in binary search probing.

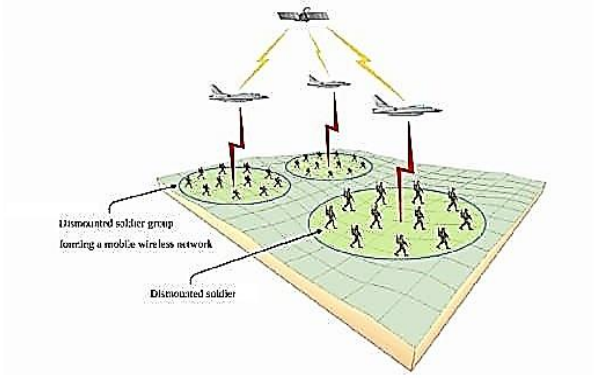


Fig. 1. Illustration of dismounted soldier group in military modern communications infrastructure.

History

We can characterized the life cycle of mobile ad hoc network into first, second and third generation. Present ad hoc network are considered the third generation .The first generation of ad hoc network can be traced back to 1970's. In 1970's, these are called Packet Radio Network (PRNET) .The Defence Advanced Research Project Agency (DARPA) initiated research of using packet- switched radio communication to provide reliable communication between computers and urbanized PRNET. Basically PRNET uses the combination of Areal Location of Hazardous Atmospheres (ALOHA) and Carrier Sense Multiple Access (CSMA) for multiple access and distance vector routing .The PRNET is then evolved into the Survivable Adaptive Radio Network (SURAN) in the early 1980's. SURAN provides some benefits by improving the radio performance (making them smaller, cheaper and power thrifty). This SURAN also provides resilience to electronic attacks.

Around the same time, United State Department of Defence (DOD) continued funding for programs such Globe Mobile Information System (GloMo) and Near Term Digital Radio (NTDR). GloMo make use of CSMA/CA and TDMA molds, and provides self-organizing and self-healing network (i.e. ATM over wireless, Satellite Communication Network). The NTDR make use of clustering and link state routing and organized an ad hoc network. NTDR is worn by

US Army. This is the only "real" ad hoc network in use. By the growing interest in the ad hoc networks, a various other great developments takes place in 1990's.

The functioning group of MANET is born in Internet Engineering Task Force (IETF) who worked to standardized routing protocols for MANET and gives rise to the development of various mobile devices like PDA's , palmtops, notebooks, etc . Meanwhile the Development of Standard IEEE 802.11 (i.e. WLAN's) benefited the ad hoc network. Some other standards are also developed that provide benefits to the MANET like Bluetooth and HIPERLAN.

II. METHODS AND MATERIAL

Manet Challenges

Unless the variety of applications and the long history of mobile ad hoc network, there are still some issues and design challenges that we have to overcome . This is the reason MANET is one of the elementary research field. MANET is a wireless network of mobile nodes, its a self organized network. Every device can communicate with every other device i.e. it is also multi hop network.

As it is a wireless network it inherits the traditional problem of wireless networking:

- The channel is unprotected from outside signal.
- The wireless media is unreliable as compared to the wired media.
- Hidden terminal and expose terminal phenomenon may occur.
- The channel has time varying and asymmetric propagation properties .

Along with these problems there are some other challenges and complexities MANET facing they are:

- The scalability is required in MANET as it is used in military communications, because the network grows according to the need , so each mobile device must be capable to handle the intensification of network and to accomplish the task.
- MANET is a infrastructure less network, there is no central administration. Each device can communicate with every other device, hence it becomes difficult to detect and manage the faults. In MANET, the mobile devices can move randomly. The use of this dynamic topology results in route changes, frequent network partitions and possibly packet losses .
- Each node in the network is autonomous; hence have the equipment for radio interface with different transmission/ receiving capabilities these results in asymmetric links. MANET uses no router in between.
- In network every node acts as a router and can forward packets of data to other nodes inorder to provide information partaking among the mobile nodes. Difficult chore to implement ad hoc addressing scheme, the MAC address of the device is used in the stand alone ad hoc network. However every application is based on TCP/IP and UDP/IP.

Areas Possible Scenarios

- **Military Scenarios** MANET supports tactical network for military communications and automated battle fields.
- **Rescue Operations** It provides Disaster recovery, means replacement of fixed infrastructure network in case of environmental disaster.
- **Data Networks** MANET provides support to the network for the exchange of data between mobile devices.
- **Device Networks** Device Networks supports the wireless connections between various mobile devices so that they can communicate.
- **Free Internet Connection Sharing** It also allow us

to share the internet with other mobile devices.

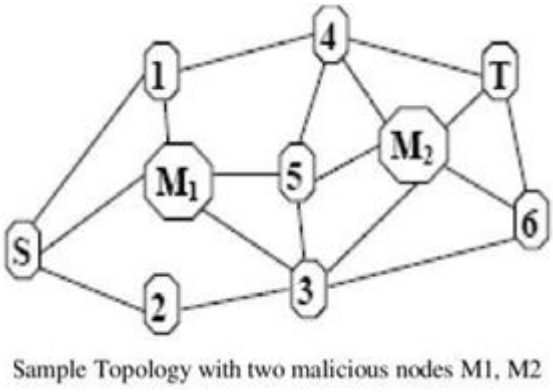
- **Sensor Network** It consist of devices that have capability of sensing, computation and wireless networking . Wireless sensor network combines the power of all three of them, like smoke detectors, electricity, gas and water meters

III. RESULTS AND DISCUSSION

A. Secure Communication Ways

Secure message Transmission

A.Secured Route Discovery by SMT Secured routes are provided by establishing an End-to-End security association between the source and the destination. This scheme won't consider the intermediate nodes that may exhibit arbitrary and malicious behavior. The source node S and destination node T negotiate a shared secret key- KS, T with the knowledge of each other's public key. A pair of identifiers - query sequence number and query identifier is generated and used for the construction of the route request packet. The identifiers along with source and destination and KS,T are used for the calculation of Message Authentication Code (MAC). The identities of the traversed intermediate nodes are added in the route request packet. The route request is denoted as a list {Q S, T: n1, n2 …nk}.The route reply is denoted as a list {RS, T : n1,n2 …nk}.



Sample Topology with two malicious nodes M1, M2

Figure 2

Security Provided by SMT under Various Attacks

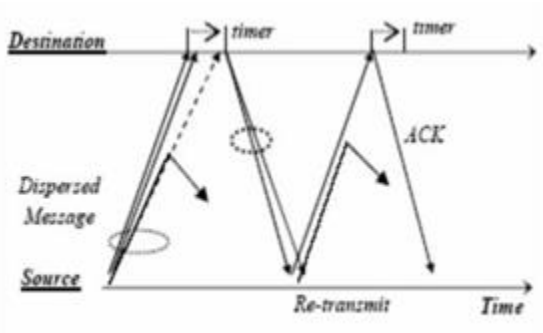
1) Fake Reply: If M1 receives the request by S and reply a fake route to S, that false reply will be discarded by the source since M1 doesn't know KS,T and not able to produce a valid MAC.

2) Tampering Route Reply: If the malicious nodes M1 or M2 changes the route reply send by T, S will discard it as the modified reply won't integrate with the expected MAC of T.

3) Resource Consumption Attack: If the adversaries want to exhaust the network resources then they will replay the requests. On receiving the replayed requests, the nodes will drop the requests based on query identifiers.

4) Fabricated Route Requests: Malicious nodes after observing for some time the requests generated by source, it will fabricate several queries with subsequent query identifiers. The goal is the intermediate nodes will store this numbers and drop out the legitimate requests sent by the source. This type of attack cannot be prevented by SMT.

5) Spoofing Attack: The nodes M1 and M2 may spoof an IP address and participate in the route requests. This attack cannot be identified and they can hide their location by masking.



Message Dispersion in SMT

Figure 3

Secured Data Communication of SMT

6) Active Path Sets(APS) and Message Transmission: A set of diverse, node disjoint multiple paths are selected by applying secured route discovery protocol. The set of paths used for current data transmission are known as Active Path Sets. The message is dispersed based on Robin's algorithm and is transmitted in multiple paths by dispersing it into pieces and after encoding. Redundancy ensures successful reconstruction of data even if some loss occurs due to malicious nodes or breakage of routes. Figure 2. Message Dispersion in SMT

7) Robust Feedback Mechanism: Each dispersed piece is transmitted in different route and carries a Message Authentication Code and by that the integrity of the message and authenticity of the source is verified. After validation, the destination acknowledges every successful receipt. The feedback mechanism is also cryptographically protected and dispersed.

8) APS Adaptation: Successful receipt of ACKS indicates operational routes while missing ACK implies that the route is either broken or compromised. The paths are rated based on short

term and long term rating. The routes are selected or discarded based on their rates. D. Byzantine Attacks Here, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, routing packets on non optimal paths, and selectively dropping packets. Byzantine failures are hard to detect. The network would seem to be operating normally in the viewpoint of nodes, though it may actually be exhibiting Byzantine behaviour . As discussed above, SMT is able to avoid only the rooting loops attacks caused by colluding nodes Secure Message Transmission movement in dynamic environment with near proximity is needed.

B. Byzantine Fault Detection

The detection scheme is based on using acknowledgements of the data packets. The destination has to return an acknowledgement to the source for every successfully received data packet. Timeouts are set for receiving the valid acknowledgements. The delay in receipt may be due to either malicious or non malicious causes. A threshold is set to a tolerable loss rate. A fault is defined as a loss rate greater than or equal to the threshold. The source keeps track of the number of recent losses. If the number of recent losses is greater than the acceptable threshold then a fault is registered and a binary search starts between the source and the destination in order to find the faulty link. The source controls the search by specifying a list of intermediate nodes on data packets. Each node in the list in addition to the destination must send an acknowledgement to the source. The list of nodes those have to send acknowledgements are known as probe nodes. Since the list of probed nodes is specified on legitimate traffic, an adversary is unable to drop traffic without also dropping the list of probed nodes and finally being detected. This scheme is able to detect all types of Byzantine attacks including network overlay attacks. Shared keys are used between the source and the probed nodes .This can be done by on demand Diffie-Hellmann key exchange algorithm. This key mechanism can be integrated into the route discovery protocol.

C. Binary Search Probing

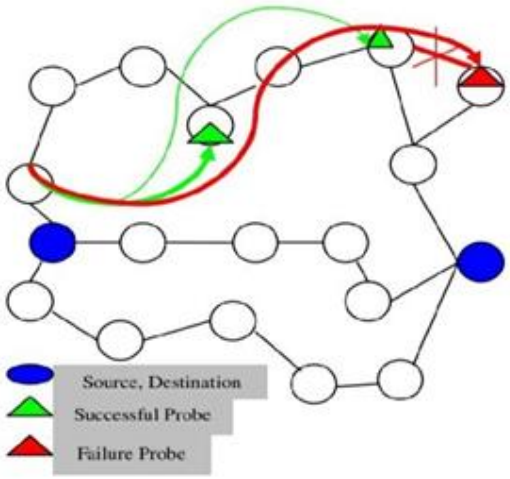


Figure 4. Binary Search Probing for Finding Faulty Links

The list of probes defines a set of non – overlapping intervals that covers the whole path where each interval covers the sub path between the consecutive probes that forms its end points as in Fig 4. When a fault is detected on an interval, the interval will be divided into two by inserting a new probe. This new probe is added to the list of probes appended to future packets. The process of subdivision continues until a fault is detected on the interval that corresponds to a single link. This result in finding log n faults where n is the length of the path.

D. Calculating the path metric

After a sender and a receiver start to exchange data packets, they build tables to keep traffic patterns. There is one table built by the sender and another one built by the receiver. The two tables have the same structure. Each table is composed of two fields: Packet identification number and time of action. Each time a packet is sent, the sender records the packet ID and the time. Each time a packet is received a receiver records the packet ID and the time. Every five (or t) seconds based on network environment, the receiver sends the sender a table. Upon receipt of the table from the receiver, the sender merges it with its own table into an anomaly detection table. The anomaly detection table contains packet identification, sending timestamp and receiving timestamp for each packet. Obviously, the sender gets the table refreshed every 5(or t) seconds. Using this information the sender can calculate the various values that will be mentioned in the following subsections and keep them in respective variables is received a receiver records the packet ID and the time.

1) Trip Time Variation: Trip time of each packet is the time a packet spends on the way, starting when it is transmitted, ending when it is received. That time is calculated using the sender's time stamp when a packet was sent and recipient's time stamps when a packet was received.
2) Change of packets frequency: The sender compares both the frequency at which packets were sent and the frequency at which packets were received, measured in packets per second. By comparing the two frequencies, delays of packets can be noticed.
3) Link Failures: Upon finding the link failure using binary search probes, all the paths containing that link will be discarded by decreasing the level of trust by half.
4) Trust Updation and Path Set Selection

An initial value is assigned to the variable of trust related to a path. A threshold is set based on expected behaviour of the network environment .Based on the observation the paths metrics are updated and are used as a parameter while selecting the active path set.

5) Emergency situation awareness<AN CASE STUDY>

A wireless network formed by the mobile devices can reduce lack of situation awareness in areas prone to emergencies, and support the management of emergency activities. The network nodes that are free to move and organize themselves can gather data from many sources and transmit them to the central dispatcher. In presented case study we focus on emergency situation at the airport The goal was to create the coherent IEEE 802.15.4 based wireless network for on-line monitoring of the arrival hall (90m×90m).

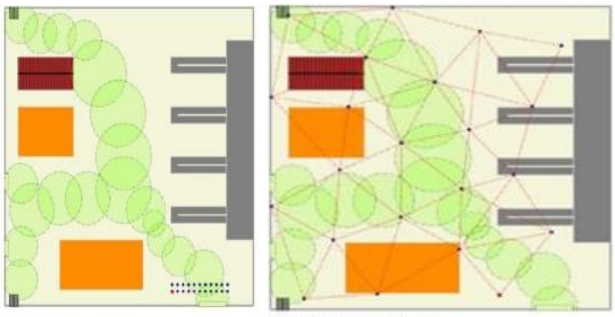


Fig. 14 The initial network topology

Fig. 15 The final network topology

The The initial network topology Mobile Netw Appl The final network topology plan of the arrival hall is presented. The network was composed of 22 mobile devices calculating their motion patterns due to the COHERENT NET algorithm. Fig. 14 presents the initial topology of the network. The results of the simulation of 200 seconds of network formation process are presented in Fig. 15 and in Table 1. From these results we can see that the final topology of the network is close to the expected one (most nodes reached their targets). However, the number of nodes assumed in this experiment was too small to create the optimal topology and satisfy all constraints.

IV.CONCLUSION

In this paper, we focused on mobility modeling in indoor and outdoor scenarios and proposed a novel approach to cooperative mobile network design. We mainly aimed to brief about the history application of MANET technologies basically in military applications rescue operations and many in a presice manner .Our approach combines techniques based on the potential field and the particle based scheme for the motion paths computation.

V. REFERENCES

[1]. Papadimitratos, P. Haas, Z.J , "Secure data communication in mobile adhoc networks" , This paper appears in: Selected Areas in Communications, IEEE Journal on Publication Date: Feb. 2006,Volume: 24, Issue: 2,On page(s): 343- 356.

[2]. Reza Curtmola Cristina Nita-Rotaru, " BSMR: Byzantine-Resilient Secure Multicast Routing in Multihop Wireless Networks" , IEEE Transactions on Mobile Computing, vol. 8,Issue. 4,pp. 445 - 459,February 2009.

[3]. A.Tsirigos and Z.J.Hass (2004) , "Analysis of mulitipath routing, Part 1: The effects on the packet delivery ratio" IEEETransactions on Wireless Communication., vol.3, no.2,pp:500-511

[4]. Banner, R. Orda, A , "Multipath Routing Algorithms for Congestion Minimization". This paper appears in: Networking,IEEE/ACM Transactions on Publication Date: April 2007 Volume: 15, Issue: 2,On page(s): 413-424.

[5]. P.Papadimitratos and Z.J.Hass, " Secure Routing For Mobile Ad-Hoc Networks", in proceeding of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS-2002).

[6]. Papadimitratos, P. Haas, Z.J and E.G.Sirer , " Path set selection in mobile ad hoc Networks" ,in Proc 3rd ACM MobiHoc , Lausanne, Switzerland, Jun 2002 ,pp 1-11.

[7]. C.Siva Ram Murthy and B.S Manoj.,(2004), "Ad Hoc Wireless Networks- Architecutres and Protocols" , Pearson Education.

[8]. Kołodziej J, Khan SU, Wang L, Min-Allah N, Madani SA, Ghani N, Li H (2011) An application of markov jump process model for activity-based indoor mobility prediction in wireless networks.In: 9th IEEE international conference on frontiers of information technology (FIT). Islamabad, pp 51–56 Mobile Netw Appl

[9]. Musolesi M, Mascolo C (2009) Mobility models for systems evaluation. A survey. State of the art on middleware for network eccentric and mobile applications (MINEMA).Springer

[10]. Mostafi Y (2011) Compressive sensing on mobile computing.IEEE Trans Mob Comput 10(10):1769– 1784

[11]. Niewiadomska-Szynkiewicz E, Sikora A (2011) Simulation-based design of self-organising and cooperative networks. Int J Space Based Situated Comput 1(1):68–75

[12]. A. Altay Yavuz, F. Alag¨oz , E. Anarım, A new satellite multicast security protocol based on elliptic curve signatures, IEEE International Conference on Information Communication Technologies (ICTTA) , April 2006, Syria.

[13]. A. Altay Yavuz, F. Alag¨oz, E. Anarım, Three-Tiers satellite multicast security protocol based on ECMQV and IMC methods, Computer-Aided Modeling, Analysis and Design of Communication Links and Networks (CAMAD'06),April 2006, Italy.

[14]. A. Altay Yavuz, F. Alag¨oz, E. Anarım, NAMEPS: N -Tier Satellite Multicast Security Protocol Based on Signcryption Schemes, IEEE Globecom Conference, San Francisco, November 2006.

[15]. W. Diffie, M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, Vol:.22, No.6, pp. 644–654, Nov. 1976.

Cite this article as :

Goutham S Tantri, Manjunatha M J, "Army Security Communication Network - An Review on Inter Tactical Mobile Ad Hoc Network Routing Protocol", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 01-08, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT19471

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

The Need For Quantum – Resistant Cyber Security : A Review

Subhashree K, Kavitha S, Sanjay K
M.Sc. Department of Mathematics (M.Sc.), Guru Nanak College, Chennai, Tamil Nadu, India

ABSTRACT

Conventional cyber security, especially public key cryptosystems depend upon the difficulty of solving large integer factorization and discrete log problems. The most straightforward way to solve these problems is to try all possible keys, which would be far too difficult for conventional computers. But the speed in which quantum computing is growing has posed a great threat to the conventional cryptosystems. This paper reviews how conventional public key cryptosystems might crumble under quantum computing and the need for quantum – safe cryptography.

Keywords : RSA, Shor's Algorithm, IFP, DLP, Quantum-resistant cryptography

I. INTRODUCTION

The two types of modern cryptography are symmetric and asymmetric key (Public key) cryptography. Secure Sockets Layer (SSL) and Transport Layer Security (TLS), cryptographic protocols that provide authentication and data encryption between servers, machines and applications operating over a network use combinations of symmetric and asymmetric cryptography. The most popular asymmetric cryptographic schemes used today are

- ✓ Rivest-Shamir-Adleman (RSA)
- ✓ Elliptic Curve Digital Signature Algorithm (ECDSA)
- ✓ Digital Signature Algorithm (DSA)
- ✓ Diffie-Hellman key agreement protocol

The use of these algorithms essentially depends upon the fact that the Integer Factorization Problem (IFP) and Discrete Logarithm Problem (DLP) are very hard to solve. But, the Shor's algorithm, created by Peter Shor, in the year 1994, can break these algorithms, if run on a quantum computer. Even though quantum computers are not commercial yet, they are speculated to be available for extensive use in a decade or so. Thus, security through the above mentioned algorithms, which are still in wide use today, will become obsolete after the advent of quantum computers. So, research is being carried out to create algorithms which are quantum resistant, to replace the conventional asymmetric cryptosystems.

II. INTEGER FACTORIZATION PROBLEM

Since the time of Euclid, it has been known that every positive integer n can be uniquely (up to order) factored into the product of primes.

Integer factorization, especially prime factorization is the problem of finding the prime factors of a given composite number. Factorizing large numbers is a very hard task for classical computers. It is computationally easy (polynomial time) to determine whether or not n is a prime or composite number. But if n is a product of two large prime numbers, then it is extremely hard to compute the factors of such n. This is the concept behind the RSA algorithm, which is the

most popular one in use now. Researchers have estimated that a 1024 bit RSA modulus (which is the bit size commonly used now), would take thousands of years to crack using classical computers.

III.DISCRETE LOG PROBLEM

If a is an arbitrary integer relatively prime to n and g is a primitive root of n, then there exists among the numbers 0, 1, 2, ..., Φ(n) - 1 , where Φ(n) is the totient function, exactly one number such that

$$a \equiv g^{\mu} \pmod{n}$$

The number μ is then called the discrete logarithm of a with respect to the base g modulo n and is denoted

$$\mu \equiv ind_g a \pmod{n}$$

It is very hard to find μ, given a and g. This concept is at the heart of Diffie-Hellman, Elliptic Curve Cryptography algorithms etc.

IV.SHOR'S ALGORITHM AND THE INTEGER FACTORIZATION PROBLEM

The Shor's algorithm tackles the integer factorization problem through the following steps: For a given integer n

Step 1: Determine if n is even, prime or a prime power. If so, we will not use Shor's algorithm as there are many effective classical methods to factorize such numbers.

Step 2: Pick a random integer $x < n$ and calculate $gcd(x,n)$. If this is not 1, then we have obtained a factor of n.

Step 3: This step is to be performed on a quantum computer. Pick q as the smallest power of 2 with $n^2 \leq q < 2n^2$. Find period r of $x^a \bmod n$. Measurement gives us a variable c which has the property $c/q \approx d/r$ where $d \in N$.

Step 4: Determine d ,r via continued fraction expansion algorithm. d,r only determined if $gcd(d,r) = 1$(reduced fraction).

Step 5: If r is odd, go back to *Step 2*. If $x^{r/2} \equiv -1 \bmod n$ go back to *Step 2*. Otherwise the factors p or $q = gcd(x^{r/2 \pm 1}, n)$. [15]

The best known algorithms (including probabilistic ones) which deliver a factor of n, all require a super-polynomial number of classical steps in n. For example, the Schnorr-Seysen- Lenstra probabilistic algorithm factorizes $n < 2^a$ in $exp(O((a \log a)^{1/2}))$ classical steps. In contrast, Shor's algorithm delivers (with positive probability) a factor of $n < 2^a$ in $O(n^2 \log n \log\log n)$ quantum steps [17].Thus, the Shor's algorithm, with the help quantum computers can break RSA and similar algorithms which rely on the difficulty of factorizing large numbers (1024 bit, 2048 bit etc.)

V. SHOR'S ALGORITHM AND THE DISCRETE LOG PROBLEM

The discrete logarithm problem in Z^*p, p prime as well as in the group of points of an elliptic curve over a finite field, is considered unbreakable by classical computers. The Shor's algorithm can solve the problem on n- bit inputs in $O(n^3)$ time, while the most efficient algorithm for this problem, for classical computers, called Gordon's algorithm will take as long as $exp(O((\log p)^{1/3} (\log \log p)^{2/3}))$ where p is the prime. [15]

VI. CONCLUSION

The monumental growth of quantum computing during the recent years has brought the need for quantum – resistant cryptography a bit closer. While many symmetric key algorithms are quantum safe, it is the asymmetric algorithms which would face a big blow in the quantum era. There have already been significant advances in research towards post –

quantum cryptography. On January 2019, National Institute of Standards and Technology has published 17 public-key encryption and key-establishment algorithms, which are considered strongest candidates for post-quantum cryptography standardization. They are BIKE, Classic McEliece, CRYSTALS-KYBER, FrodoKEM, HQC, LAC, LEDAcrypt (merger of LEDAkem/LEDApkc), New Hope, NTRU (merger of NTRU Encrypt/NTRU- HRSS-KEM), NTRU Prime, NTS-KEM, ROLLO (merger of LAKE/LOCKER/Ouroboros-R), Round5 (merger of Hila5/Round2), RQC, SABER, SIKE, and Three Bears. A continued analysis on the performance of the above mentioned algorithms will prove to be fruitful to get ready for the post- quantum era.

VII. REFERENCES

[1]. Weedbrook, C., Pirandola, S., Lloyd, S. and Ralph, T.C., 2010. Quantum cryptography approaching the classical limit. Physical review letters, 105(11), p.110501.

[2]. Gajbhiye, S., Karmakar, S., Sharma, M. and Sharma, S., 2017, December. Paradigm shift from classical cryptography to quantum cryptography. In 2017 International Conference on Intelligent Sustainable Systems (ICISS) (pp. 548-555). IEEE.

[3]. Farik, M. and Ali, S., 2016, December. The Need for Quantum-Resistant Cryptography in Classical Computers. In 2016 3rd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE) (pp. 98-105). IEEE.

[4]. Häner, T., Roetteler, M. and Svore, K.M., 2016. Factoring using 2n+ 2 qubits with Toffoli based modular multiplication. arXiv preprint arXiv:1611.07995..

[5]. Buchanan, W. and Woodward, A., 2017. Will quantum computers be the end of public key encryption?. Journal of Cyber Security Technology, 1(1), pp.1-22.

[6]. Amico, M., Saleem, Z.H. and Kumph, M., 2019. Experimental study of Shor's factoring algorithm using the IBM Q Experience. Physical Review A, 100(1), p.012305.

[7]. Coles, P.J., Eidenbenz, S., Pakin, S., Adedoyin, A., Ambrosiano, J., Anisimov, P., Casper, W., Chennupati, G., Coffrin, C., Djidjev, H. and Gunter, D., 2018. Quantum algorithm implementations for beginners. arXiv preprint arXiv:1804.03719.

[8]. Martín-López, E., Laing, A., Lawson, T., Alvarez, R., Zhou, X.Q. and O'brien, J.L., 2012. Experimental realization of Shor's quantum factoring algorithm using qubit recycling. Nature Photonics, 6(11), p.773.

[9]. Chen, L., Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R. and Smith- Tone, D., 2016. Report on post-quantum cryptography. US Department of Commerce, National Institute of Standards and Technology.

[10]. Brands, G., Roellgen, C.B. and Vogel, K.U., 2015. QRKE: Quantum-Resistant Public Key Exchange. arXiv preprint arXiv:1510.07456.

[11]. Ioannou, L.M. and Mosca, M., 2011, November. A new spin on quantum cryptography: Avoiding trapdoors and embracing public keys. In International Workshop on Post-Quantum Cryptography (pp. 255-274). Springer, Berlin, Heidelberg.

[12]. Chen, L., 2017. Cryptography Standards in Quantum Time: New wine in old wineskin?. IEEE security & privacy, 15(4), p.51.

[13]. Mavroeidis, V., Vishi, K., Zych, M.D. and Jøsang, A., 2018. The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200.

[14]. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing,26(5),1484-26. doi:http://dx.doi.org/10.1137/S0097539795293 1 72

[15]. Shor, Peter W. "Polynomial-time algorithms for prime factorization and discretelogarithms on a quantum computer."SIAM journal on computing26.5 (1997):1484-1509.

[16]. Ekera, M., 2016. Modifying Shor's algorithm to compute short discrete logarithms. IACR Cryptology ePrint Archive, 2016, p.1128.

[17]. Christophe Pittet. Mathematical aspects of Shor's algorithm. 3rd cycle. Shillong - Inde, 2013, pp.15.

Cite this article as :

Subhashree K, Kavitha S, Sanjay K, "The Need For Quantum - Resistant Cyber Security : A Review", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 09-12, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT19472

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

A Survey - Security and Privacy Issues In Cloud Computing

Sheela D V
Soundarya Institute of Management and Science, Bangalore University, Karnataka, India

ABSTRACT

Cloud Computing is inevitability as the number of connected devices are growing and also the computing and storage needs. Cloud computing converts the way Information Technology is encouraged and succeeded, cost worth, faster invention, faster time-to-market, and the capable to measure applications on demand. Security of the cloud is a major challenge today which has to be addressed. Several new technologies are emerging to keep the cloud services secure and efficient at the same time. This paper discusses the cloud services, risk associated with it and security measures in cloud computing.

Keywords : Public cloud, Private cloud, Hybrid cloud, Infrastructure as a service (Iaas), Software as a service (Saas), Platform as a service (Paas)

I. INTRODUCTION

Cloud Computing [1] is gaining importance in leaps and bounds and is expected to increase its usage in years to come. Cloud computing enables resources to be shared in a pool that can be rapidly provisioned and can be offered to the user with minimal interaction of the service provider. The main aim of the cloud computing is to provide secure, [2] quick and convenient data storage and computing service to the users. This paper discusses available types of cloud and various types of services offered to the end users in succeeding sections. The clouds which are accessible to the masses by internet wherein the user uses the service like application and storage are called public clouds.[10] The Clouds which are owned by a single company and are restricted to be used by its own set of people are called private cloud.[9] The Hybrid approach,[11] combines the above two types and is discussed in detail further in this paper. The highlight of the security issue on cloud computing is focused in the SPI model i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Internet as a service (IaaS) and id discussed in detail in this paper.

The Saas is the service provided to the user for using application running on the cloud. The PaaS[5] is the service offered by the service provider to install customer's own application on the service provider's cloud infrastructure without installing any additional tools and software on their local machines. The Iaas is the service provided to the user to utilize the facility of storage, processing and networking so that customer can run and deploy any software or tool on this platform. The paper then discusses and identifies the main vulnerabilities in these kinds of systems and also the threats related to these systems.

II. METHODS AND MATERIAL

2.1 TYPES OF CLOUDS

Cloud computing comes in basic three forms: public clouds, private clouds, and hybrids clouds. Virtual private clouds and Community clouds are few

modifications of the basic clouds. Depending on the type of data public, [10] private, and hybrid clouds, can be analyzed in terms of security and management requirement.

Fig.1 Types of cloud

2.2 PUBLIC CLOUDS

A public cloud [10] is basically the internet and is implemented using a shared data center infrastructure of hardware and software that is shared by multiple users. The data center is off-premises. Public Cloud service providers use the internet to provide resources, such as applications and storage to the general public, or on a 'public cloud. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google App Engine and Windows Azure Services Platform. The disadvantages of the public cloud is limited configuration, security, and specifications of SLA, making it unideal for services using delicate data that is subject to compliancy principles.

2.3 PRIVATE CLOUDS

Private clouds are data centers which are owned by a single company that provides flexibility, scalability, provisioning, automation and monitoring. A Private Cloud[9] is implemented using a dedicated infrastructure of hardware and software that is used privately by an organization. The data center can be on-premises or off-premises. It is not shared with another organization. The goal of a private cloud is to use the cloud "as- a-service" for its employees to gain the benefits of cloud architecture rather than offerings to external customers. Private clouds are quite expensive with typically uncertain economies of scale. This type of cloud can be an option for Small-to-Medium sized enterprises and is mostly used by large scale enterprises. Private clouds are focused on security and compliance, and keeping resources within the firewall.

2.4 HYBRID CLOUDS

A Hybrid Cloud [11] is any combination of Private cloud and public cloud. Similarly it is also a combination of Virtual Private Cloud and one or more Public Clouds. The resources are shared among the Clouds in Hybrid approach. By using a Hybrid approach, companies can maintain control of an internally managed private cloud while relying on the public cloud as and when needed. For example during peak times a single application, or portions of applications can be transferred to the Public Cloud. This will also be useful during expected disruption: floods, scheduled maintenance windows, power failure. Due to the cost, it is hard to maintain an off-premise disaster recovery site for most organizations. Though there are some lower cost solutions and alternatives that slow down the band an organization gets, at this times the recovery of the data quickly reduces. Cloud based

Disaster Recovery (DR)/Business Continuity (BC) services allow organizations to contract failover out to a Managed Services Provider that maintains multi-tenant infrastructure for DR/BC, and specializes in getting business back online quickly.

2.5 VIRTUAL PRIVATE CLOUDS

A Virtual Private Cloud is created using a shared data center infrastructure of hardware and software. The data center is most likely off-premises. It is shared with multiple organizations. If the data center is not shared then that is a Private Cloud. The topmost layers of the Cloud Computing Stack (PaaS and SaaS) in a Virtual Private Cloud is dedicated to the

organization. The lower layer of IaaS is shared among various users in a Virtual Private Cloud. A Virtual Private Cloud can join in a Hybrid Cloud also.

2.6 COMMUNITY CLOUDS

A Community Cloud acts as a Private Cloud, Virtual Private Cloud, Public Cloud, or Hybrid Cloud. The design of a Community Cloud meets the need of a community. Such communities involve people or organizations that have shared interests. The communities such as industrial community, research community, standards community, and so on. So, a Community Cloud is not considered to be a cloud since it looks like it. Only few member organization data center support the Community Cloud.

2.7 TYPES OF CLOUD SERVICES

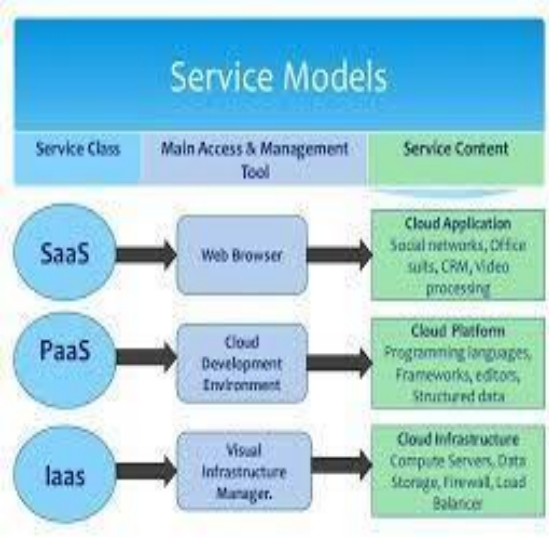


Fig.2 Types of Cloud Services

2.8 INFRASTRUCTURE AS A SERVICE (IaaS)

This service provides the customers with a collection of bare metal devices and software which are required to fulfill the computational and storage needs of the users. IaaS gives business access to web architecture, like storage space, servers, and connections, without purchasing and managing this infrastructure. It is economical to both service provider and user, in particular IaaS allows an internet business a way, to develop and grow on demand. Both PaaS [5] and SaaS clouds are a layer overlaid on IaaS clouds. The examples of IaaS are Amazon EC2 and Rack space Cloud.

2.9 PLATFORM AS A SERVICE (PaaS)

It is a layer over Iaas. PaaS has all flavors of operating environment to meet the various computational needs of the customer. The customer has the freedom to run any application without any additional expenditure of the operating environment and hardware requirements. Some examples of a PaaS [5] system include Mosso, Google App Engine, and Force.com. Main benefit of a PaaS is that it is an economical option for the user where the user can initiate application with no stress of the platform required for that application. A little porting may be required if you are dealing with an existing app. PaaS offers a lot of scalability by design because it is based on cloud computing. If you want a lean operations staff, PaaS is an option which will provide maximum output with limited staff.

2.10 SOFTWARE AS A SERVICE (SaaS)

SaaS is the topmost layer in the cloud stack which encompasses the software/applications [18] for the users. SaaS delivers the software services to the user over web. SaaS offers the users the advantage of not installing any software on their personal computers and neither the burden of maintenance of software which they use as per their computational needs. Examples of SaaS running on cloud are Gmail and Sales force, but it is not necessary that all SaaS has to be based on cloud computing.

III. THREATS RISKS OF CLOUD COMPUTING

There are a number of security risks [14] associated with cloud computing that must be adequately addressed:

1. LOSS OF GOVERNANCE.

While using public cloud, user have to surrender control to the cloud provider over a number of issues that may affect security. The service agreements provided by the service provider may not offer an assurance to solve such issues on the part of the cloud provider. This leaves a gap in security defense.

2. RESPONSIBILITY AMBIGUITY.

Responsibility of security issues may be split between the provider and the customer. This division of responsibility creates a critical vulnerability of unallocated responsibilities of critical security issues. This split is likely to vary depending on the cloud computing model used (e.g., IaaS vs. SaaS).

3. AUTHENTICATION AND AUTHORIZATION.

Cloud resources can be accessed from anywhere in the world on the Internet. This brings out a very important requirement of establishing with certainty the identity of a user especially if users now include employees, contractors, partners and customers. Authentication and authorization thus becomes a critical requirement to ensure security.

4. ISOLATION FAILURE.

Multi-tenancy and shared resources are main characteristics of public cloud computing. The isolation of storage, memory, routing and even reputation between tenants becomes a challenge which has to be dealt with for secure cloud operations (e.g. so-called guest- hopping attacks).

5. COMPLIANCE AND LEGAL RISKS.

It is very necessary for the service provider to prove that the services provided by the cloud comply with the industry standards for the customer to be completely satisfied before hiring the cloud service. The service provider must permit audits by the cloud customer. The customer must themselves verify that the cloud provider has appropriate certifications in place.

6. HANDLING OF SECURITY INCIDENTS.

he customer may hand over detection; reporting and successive management of security incidents to the cloud service provider, but these incidents affect the customer. Notification rules need to be discussed in the cloud service agreement so that customers are not caught unaware or informed with an unacceptable delay.

7. MANAGEMENT INTERFACE VULNERABILITY.

Interfaces to manage public cloud resources are usually accessible through the Internet. Since they allow access to larger number of resources than traditional hosting providers, they pose an increased risk, especially when combined with remote access and web browser vulnerabilities.

8. APPLICATION PROTECTION.

The defense-in-depth security approach is based on a clear demarcation of physical and virtual resources, and on trusted zones. In cloud computing the responsibility of infrastructure security is delegated to the cloud provider. The organizations now need to re plan perimeter security at the network level by incorporating more controls at the user, application and data level.

9. DATA PROTECTION.

Data Protection covers unauthorized exposure or leakage of sensitive data as well as the loss or unavailability of data. It is impossible for a customer (in the role of data controller) to keep a check on the data handling practices of the cloud provider. This problem increases greatly for cases of multiple transfers of data.

10. MALICIOUS BEHAVIOR OF INSIDERS.

Malicious actions of insiders within an organization can cause substantial damage, given the access and authorizations they enjoy. In the cloud computing environment this risk increases since such activity

might may occur within the customer organization or the provider organization.

11. BUSINESS FAILURE OF THE PROVIDER.
Such failures could render data and applications essential to the customer's business unavailable over an extended period.

12. SERVICE UNAVAILABILITY.
This could be caused by hardware, software or communication network failures.

13. VENDOR LOCK-IN.
Proprietary services of a specific cloud service provider could make the customer depend on that provider only. Absence of portability of applications and data among cloud service providers creates a chance of data and service unavailability in case of a change in providers; therefore it is an aspect of security issue. The absence of interoperability of interfaces associated with cloud services ties the customer to a particular provider and switching of provider becomes a difficult task.

14. INSECURE OR INCOMPLETE DATA DELETION.

After termination of a contract with a provider the data of the user may not be completely deleted. Backup copies of data usually exist, and there is a chance that this data may be mixed with other customers' data. The benefit of multi-tenancy thus posses a considerable risk to the customer than dedicated hardware.

IV. CLOUD SECURITY GUIDANCE

The applications and data which are critical for the customers to maintain are forwarded to the cloud to avail the cloud services. This section provides a recommended series of steps for cloud customers to estimate and manage the security of their use of cloud services, with the goal of mitigating risk and delivering an appropriate level of support.

1. Ensure effective governance, risk and compliance processes exist
2. Audit operational and business processes
3. Manage people, roles and identities
4. Ensure proper protection of data and information
5. Enforce privacy policies
6. Assess the security provisions for cloud applications
7. Ensure cloud networks and connections are secure
8. Evaluate security controls on physical infrastructure and facilities

PRESENT SECURITY SYSTEM IN CLOUD

There are mainly seven categories of the cloud security. The three major problems identified after referring to the various references are legal issues, compliance and loss of control over data.
Network Security Interfaces Data Security Virtualization Governance Legal Issues E- Discovery
Various sub security issues under these main categories which ensure a secure cloud system are:-

1. Network Security:-
The issue related to the communication of the networks and their configuration with respect to cloud computing setup.

Firewall: - One of the most efficient and successful protection can be achieved by installing firewall which will analyze and control communication of data and applications. It prevents the DoS attacks and any other abnormal instance on the cloud. Main advantages of a firewall are Secure Data Centre, Secure Remote Access, Identity and Management

Transit security: - Existing infrastructure of VPN (Virtual Private Network) model should be exercised

to protect the cloud from side channel attack spoofing, man in middle and sniffing.

2. Interfaces

All issues related to human and electronic interfaces like user interface, programming interface, administrative interface etc for accessing and controlling the cloud network are critical in securing the user's interest. Main interfaces which provide secure system are:

a. Application programming Interfaces (API)

b. Administrative Interface c. User Interface

c. Access authentication

3. Data Security:-

a. Confidentiality Integrity and Availability (CIA) protection must be ensured by all available means.

b. Redundancy: Mission critical data integrity and availability must be ensured while catering for redundant storage of data.

c. Data disposal: Deletion is the common technique used for the data disposal but in the parlance of cloud all the log reference, hidden backup, registers and complete destruction of data should be ensured.

4. Virtualization: - VMs (Virtual Machine) isolation and vulnerabilities of the third party virtual platform like hypervisor must be addressed to ensure the security of the user's data and application. a. Cross- VM attacks:- It calculates the providers traffic ingress and egress rate in order to steel cryptographies key and increase changes of VM placement attacks.

b. VM identification: - Lack of controls for identifying virtual machines that are being used for executing a specific process or for storing files.

c. Data leakage: - Exploitation of the hypervisor vulnerabilities in order to leak data from virtualized infrastructure.

5. Governance:-

Problems related to administrative and technical controls in cloud computing solutions are:-

a. Data control: - Moving data to the cloud means losing control over redundancy, location, file systems and other relevant configurations

b. Compliance: - Includes requirements related to service availability and audit capabilities. c. SLA: Mechanisms: - to ensure the required service availability and the basic security procedures to be adopted. Service Level Agreement between the Provider and the company should be ensured for frequent Audits and resolution of the critical issues.

d. Loss of service: - Very strong and robust disaster recovery policies and also customer side redundancy should be implemented to avoid service outages in the cloud environments.

e. Audit: - Helps security and availability assessments to be done by customers and third party participants. Fair methodology should be adopted for continuous analyzing service conditions.

6. Legal issues:- Issues related to judicial requirements and laws, like different data storage location and privilege escalation management.

a. Data storage location: - For the achievement of redundancy the data is stored in various multiple geographic locations. No common cyber laws across the globe directly or indirectly affect the law enforcement measures.

b. E-Discovery: - Confiscated hardware for investigation may also affect the stored data of other customers also. Data disclosure is critical in this case.

V. CONCLUSION

Cloud computing is the future of computing and storage technology. The exponential increase of connected devices and the need of small and portable devices for complex computation warrant

the growth of cloud computing technology. This paper has discussed the cloud technology, various security threats and prevention measures for ensuring a secure cloud system. The need for security is increasing along with the increasing demand of cloud computing services and the balance has to be maintained hand-in-hand.

VI. REFERENCES

[1]. Brian F. Cooper , Adam Silberstein , Erwin Tam , Raghu Ramakrishnan , Russell Sears, Benchmarking cloud serving systems with YCSB, Proceedings of the 1st ACM symposium on Cloud computing, June 10-11, 2010, Indianapolis, Indiana, USA [doi>10.1145/1807128.1807152]

[2]. "Security Guidance for Critical Areas of Focus in Cloud Computing", Cloud Security Alliance, Dec. 2009, [online] Available:

[3]. T. Ristenpart, "Hey You Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds", Proc. 16th ACM Conf. Computer and Communications Security (CCS 09)

[4]. "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22.

[5]. Boniface, M.; et al. (2010), Platform-as- a-Service Architecture for Real-Time Quality of Service Management in Clouds, 5th International Conference on Internet and Web Applications and Services (ICIW), Barcelona, Spain: IEEE, pp. 155– 160, doi:10.1109/ICIW.2010.91

[6]. Amies, Alex; Sluiman, Harm; Tong, Qiang Guo; Liu, Guo Ning (July 2012). "Infrastructure as a Service Cloud Concepts". Developing and Hosting Applications on the Cloud. IBM Press. ISBN 978-0-13-306684- 5.

[7]. Foley, John. "Private Clouds Take Shape". InformationWeek. Retrieved 2010- 08-22.

[8]. Jump up^ Haff, Gordon (2009-01-27). "Just don't call them private clouds". CNET News. Retrieved 2010-08-22.

[9]. "There's No Such Thing As A Private Cloud". InformationWeek. 2010-06-30. Retrieved 2010-08-22.

[10]. Jump up^ Rouse, Margaret. "What is public cloud?". Definition from Whatis.com. Retrieved 12 October 2014.

[11]. Jump up^ "Mind the Gap: Here Comes Hybrid Cloud – Thomas Bittman". Thomas Bittman. Retrieved 22 April 2015.

[12]. "Business Intelligence Takes to Cloud for Small Businesses". CIO.com. 2014-06- 04. Retrieved 2014-06-04.

[13]. Désiré Athow. "Hybrid cloud: is it right for your business?". TechRadar. Retrieved 22 April 2015.

[14]. Srinavasin, Madhan (2012). "'State-of- the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment". ACM ICACCI'.

[15]. "Swamp Computing a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010-01-25

[16]. "Top Threats to Cloud Computing v1.0" (PDF). Cloud Security Alliance. Retrieved 2014-10-20.

[17]. Winkler, Vic. "Cloud Computing: Virtual Cloud Security Concerns". Technet Magazine, Microsoft. Retrieved 12 February 2012.

[18]. "Software as a Service (SaaS)". Cloud Taxonomy. Open crowd. Retrieved 24 April 2011.

Cite this article as :

Sheela D V, "A Survey - Security and Privacy Issues In Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 13-19, September-October 2019.

Journal URL : http://ijsrcseit.com/CSEIT19473

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

A Survey On Sentiment Analysis

M. Janaki M.C.A, M.Phil, NET, SLET
Assistant Professor, Department of Computer Science, Sacred Heart Girls First Grade College, Bengaluru, Karnataka, India

ABSTRACT

Sentiment analysis is a technique to analyze people's opinion on given topics such as political, social, and economical or review on product etc.The techniques for sentiment analysis include machine learning (supervised and unsupervised), and lexical-based approaches. The most important focus of the realm of Sentiment analysis lies find the emotions indicate within the texts. Sentiment analysis allows us to extract reviews and present the summary which could be beneficial for market research and product enhancement.It helps business and organization because it's easy for them to know how people feel about their product or services so that they can make better decision or improve their services. For that purpose we have different sentiment analysis techniques like Naïve Bayes, Maximum Entropy, and Support Vector Machine which gives correctness of information or provides us accuracy. For sentiment we use machine learning because it train the computer to recognize the emoticon behind the sentence.

Keywords : Sentiment Analysis, Polarity classification, Techniques, Applications, Challenges.

I. INTRODUCTION

Sentiment analysis is a type of natural language processing for tracking the mood of the public about a particular product or topic. Sentiment Analysis has many names. It's often referred to as subjectivity analysis, opinion mining, and appraisal extraction, The purpose of sentiment analysis is to automatically determine the expressive direction of user reviews [6].Sentiment analysis, which is also called opinion mining, involves in building a system to collect and examine opinions about the product made in blog posts, comments, reviews or tweets. Two types of sentiment analysis are Subjectivity/Objectivity Identification and Feature /Aspect Based Sentiment Analysis.The users are now more interested to share their opinion on the internet using ratings, reviews, and a suggestion with diversified forms of user's expression.

The aim of Sentiment Analysis is to with strain this data in order to obtain critical information regarding public opinion, an emotions that help to make smarter business decisions, political campaigns and better product consumption.

To sentiment the data, here are some methodology like extract data from any site like twitter, amazon etc. Next step is cleaning process where irrelevant data is removed then on the pre-processed data apply feature selection which extract useful data from bag of words then give training and testing to it. Finally apply classifier algorithm which gives accuracy of that classifier.

Information available in textual format can be classified into two main things: Facts and Opinions. An objective expression made by user regarding

certain objects, entities or events and their attributes is known as facts. In the similar way, a subjective expression which describes emotions of a person, her sentiments and performance assessment about objects, entities and events and their characteristics is known as opinion.

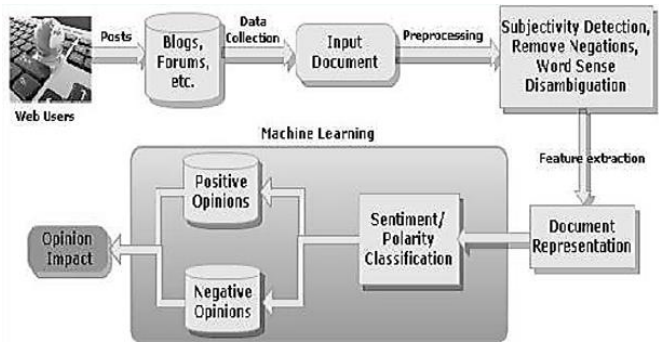


Fig 1 : Systematic Flow of Sentiment Analysis

1.1 Explicit Opinion and Implicit Opinion

Sentiment that appears in text comes in two flavours: explicit where the subjective sentence directly expresses an opinion ("It's a beautiful day"), and implicit where the text implies an opinion ("The earphone broke in two parts").Most of the work done so far focuses on the first kind of sentiment, since it is the easier one to analyse.

1.2 Feature Selection in Sentiment Classification

Feature extraction phase deals with feature types (which identifies the type of features used for opinion mining), feature selection (used to select good features for opinion classification), feature weighting mechanism (weights each feature for good recommendation) reduction mechanisms (features for optimizing the classification process). [11]

Types of features used for Sentiment analysis could be:

1) Term frequency (The presence of the term in a document carries a weight age).
2) Term co-occurrence (features which occurs together like uni-gram, bi-gram or n-gram),
3) Part of speech information (POS tagger is used to separate POS tokens).
4) Opinion words (Opinion words are words which express positive (good) or negative (bad) emotions)
5) Negations (Negation words (not, not only)
6) Syntactic dependency (It is represented as a parse tree and it contains word dependency based features)

Term (T) and Term Frequency (TF) The feature considered as individual word or word n-grams is called as term and its occurrence count in the document is known as term frequency. [8]

Part of Speech Tags (POS) It is the method used to assign a Part-of- Speech to every word present in the sentence. Every word in the sentence is assigned a tag like, verb, noun, prepositions and adjective etc. In English language, mainly adjectives are used to identify subjectivity and opinions. So, the earlier researchers used these adjectives as significant indicators of either subjectivities or opinions and counted these adjectives as the special features in the field of opinion mining.

Opinion Words and Opinion Phrases In the opinionated text positive or negative sentiments which are commonly used to express emotions of the opinion holder are called as opinion words. We can consider the beautiful, good, amazing, etc. as positive opinion words and negative opinion words like, bad, weak, poor, etc. Moreover, instead of such individual opinion words, there are also idioms and phrases which can be used to indicate opinions. Consider an example, "These opera tickets cost us an arm and a leg". Here, 'cost someone an arm and a leg' is a phrase which means having a negative impact of something. Therefore, opinion phrases and opinion words play a vital role in performing sentiment analysis.

1.3 Preprocessing Task into Several Sub phases:
Pre-processing the text is a process of cleaning the text and prepare them for text classification. Usually the online product reviews contain some noisy and

irrelevant information such as tags, scripts and advertisements.

There are some predefined steps used for pre-processing of texts [19]. They are online text cleaning, White space removal, Abbreviation expansion, Stemming, Removal of Stop words, Negation handling and finally feature selection. Fig. 1 illustrates the steps involved in processing of sentiment analysis. Online text cleaning involves in clean up line breaks, HTML tags and word formatting. Removing the empty spaces from the document is called white

space removal. In abbreviation expansion, the abbreviations such as TV, AC are expanded as Television and Air Conditioner by using pattern recognition and regular expression techniques. Stemming attempts to remove the inflected forms of a word, in order to reduce each word to its root form. Stop words such as 'the', 'of', 'a'are removed in next step [20]. But it should be deliberated for the opinion words which are expressed as phrasal words. In negation handling the negative terms are considered for polarity. For feature selection(remove noisy features), Point- wise Mutual Information (PMI), Chi- Square and Latent Semantic Indexing (LSI) methods are used [21].

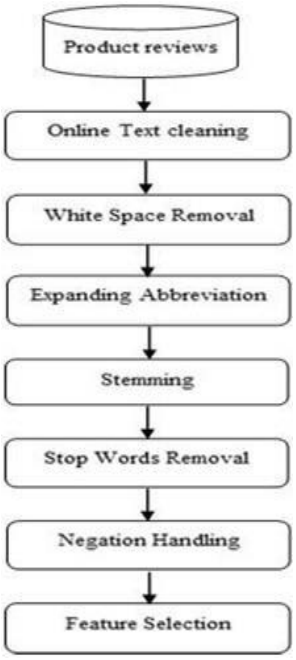


Figure 1. Processing steps in Sentiment Analysis

DIFFERENT LEVELS OF SENTIMENT ANALYSIS

Different three levels in sentiment analysis which is document level, sentence level and aspect level. In document level i.e. identified that is the review is positive or negative. In sentence level i.e., identified every sentence is positive or negative and in aspect level entities and their features/aspects sentiments is positive and negative. [2]

Document level

In Document level analysis task is characterize whether an entire opinion of document level communicates a positive or negative supposition For instance, given thing audit, the framework figures out if the survey communicates a general positive or negative decision about anything. This undertaking is regularly known as document level sentiment classification

Sentence level

In Sentence level the fundamental undertaking is goes to the Sentence and makes sense of if every sentence communicated a positive, negative, or neutral sentiment. Neutral means no opinion about any sentence. This level of investigation is immovably related to the subjectivity arrangement. Which is recognizes sentences (called target sentences) [2] that is express genuine information from the sentences (called subjective sentences) that express subjective perspectives and opinions.

Aspect level

In Aspect Level both the document level and the sentence level analyses do not discover what exactly people liked and didn't like. Aspect level performs better- grained investigation. Aspect level is directly looks at the opinion itself. In the Aspect level is depend on the possibility that an opinion consists of a sentiment positive, negative or neutral or an objective of sentiment

For e.g. Sentence is "The Redmi phone's call quality is amazing, yet its battery life is short" assesses two focuses first is call quality second is battery life, of Redmi (component). The conclusion on Redmi's call quality is certain in sentence however the opinion on its battery life is negative. Redmi phone's call quality and battery life of Phone are the feeling targets. In this level of investigation, an organized of assessments about elements and their viewpoints can be created, which turns unstructured content to organized.

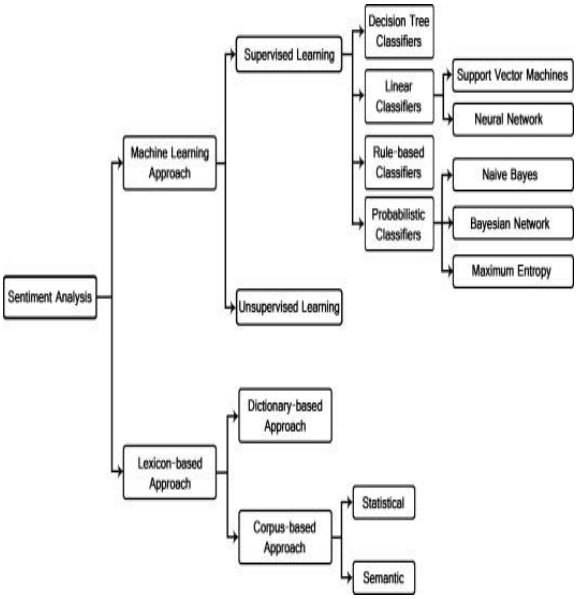
NEGATION:

Negation is a very common linguistic construction that affects polarity and, therefore, needs to be taken into consideration in sentiment analysis. When treating negation, one must be able to correctly determine what part of the meaning expressed is modified by the presence of the negation. Most of the times, its expression is far from being simple , and does not only contain obvious negation words, such as not, neither or nor. Research in the field has shown that there are many other words that invert the polarity of an opinion expressed [16],

SENTIMENT ANALYSIS TECHNIQUES:

Sentiment Classification techniques are separated into two different techniques which is ML and Lexicon based Approaches. [3]

Machine learning methods are based on training an algorithm. It mostly based on classification on a set of selected features for a specific purpose and then test on another set whether it is able to detect the right features and give the right classification. A lexicon based method depends on a predefined list or corpus of words with a certain polarity. There are wide variety of machine learning methods such as Naïve Bayes Classifier, Support Vector Machine and Maximum Entropy Classifier .Various lexicon based sentiment methods such as Senticnet.



II. LITERATURE REVIEW

In the G. Vinodhini[12] research paper, Naïve Bayes, a commonly used algorithm for document categorization is used to compute the probabilities by using the collective probabilities of topics and words. Support Vector Machine is a text categorization which outperforms the Naïve Bayes technique.

It searches for a decision surface to split the training data points into two categories and makes decisions based on the given support vectors.

It is observed in Liu [15] that, the opinion contents which are available online on internet as well as off line are containing mostly textual information used by the customer to provide relevant product feedback. The information available in textual format can be generally classified as either facts or opinions.

The research paper the survey gives an overview of the efficient techniques, recent advancements and the future research directions in the field of Sentiment Analysis[11].This research paper describes some of the considerable challenges in sentiment analysis and the techniques use to analyse, the main challenge in the opinion mining is to identify the sentiment expressed

by the text and the significant approaches of enhancing the performance of sentiment analysis are through i) N-Gram model,

ii) subjective lexicon, and iii) machine learning[5]

This study ensures an overall survey about sentiment analysis related to product reviews, and classification algorithms used for sentiment classification. It is a system thatidentifies and classifies opinion/sentiment as represented in electronic text [1].Sentiment Analysis is also investigated on Indian Language, Chinese language, Arabic Language [22] apart from the English language. At present, existing techniques towards sentiment analysis is focused on using lexicon generation in text-based processing [23], subjectivity detection [24], sentiment polarity detection [25], sentiment structurization [26], summarization-visualization tracking [27], etc. Apart from this, adopt of sentiment analysis is very much frequent for analyzing social network data from Facebook, Twitter, and Google [28].

Current Trends and Techniques some novel approaches:

1. Document level sentiment classification: This technique, identifies whether the given document contains positive or negative sentiment about any topic. Generally classification techniques are used to solve these issues. The general features used in these techniques are: (1) terms and their occurrence frequency (for example the use of Tf- Idf), (2) POS taggers, (3) Opinion words and phrases, (4) Syntactic dependencies and (5) negative & Positive words.

2. Using unsupervised learning: For example, the use of POS tagger to identify two word phrases. It estimates the orientation of the extracted phrases using the Pointwise mutual information (PMI).

3. Sentiment analysis at sentence level: Techniques using this approach, considers the sentences as the source of single opinion. For a given a sentence s, it applies two sub-tasks: (a) Subjectivity classification: Determine whether s is a subjective sentence or an objective sentence, and (b) Sentence-level sentiment classification: If s is subjective, determine whether it expresses a positive or negative opinion.

III.APPLICATIONS

1) It is mostly used in E-commerce activities. When any customer buys any item or service from the e-commerce websites, then it permits them to submit their opinions about qualities of shopping services and products. A summary for the product and various features of the product is provided by assigning ratings.
2) It is used in Entertainment by helping people to choose which movie or series to watch.
3) It is also used in Marketing. Nowadays, each company makes available the facility to its users to provide opinions about its products and services. Hence, it is helpful for businesses to save money as well as time because there is no need any more to conduct surveys as the feedbacks related to all the products are available on their sites.
4) It is also used in education domain, to help students to determine which university is good for studies

IV.RESEARCH CHALLENGES

There are various challenges in Sentiment analysis. A few of them are discussed in this paper.
1) The very first challenge is “opinion word” which can be considered to be positive in one way but may be considered negative in another way.
2) Second challenge is that sometimes user may convey their sentiments in an unusual way. The text in a sentence can be difficult to identify as ironic or sarcastic and this can lead to faulty polarization and misleading sentiment analysis. Reference [8] discusses this problem.

3) The third challenge is the language i.e, the majority of the work done in opinion mining is focused on two languages: English and Chinese and other languages needs to be explored.

4) Now, the fourth challenge is the sentiment given on twitter is difficult to comprehend as it consists of poor abbreviations, lack of capital letters, spelling mistakes, no proper punctuations, and grammatical errors and so on.

5) Sixth challenge is in "detection of spam and fake comments, mainly through the recognition of duplicates, the association of qualitative with summary feedbacks, the recognition of outliers, and also the reputation of the reviewers".

V. CONCLUSION

Sentiment Analysis is one of the important research areas as it summarizes opinions and reviews of public. This survey highlights the main idea behind Sentiment Analysis and explains literature review, Sentiment Classification, challenges in detail. Sentiment analysis is one of the active research areas and several interesting works have been done in this field. Still, a fully useful and highly efficient system has not been introduced till now. But business organizations and academics are working hard to find the best system for sentiment analysis. Sentiment analysis helps in decision making and knowing people review by analyzing or giving rating to their views such as product reviews. By making use of this system, user can get suggestion for product to buy.Naive Bayes and Support Vector Machines are the most frequently used ML algorithms for solving SC problem.

VI. REFERENCES

[1]. Sentiment Analysis: A Survey of Current Research and Techniques

[2]. Jeevanandam Jotheeswaran, Dr. S. Koteeswaran International Journal of Innovative Research in Computer and Communication Engineering

[3]. Xing Fang and Justin Zhan "sentiment analysis using product Review data" Department of computer science, North Carolina a&T State University Greensboro, NC, USA, 2015 Springer journal.

[4]. WalaaMeddhat , Ahmed Hassan ,Hoda Korashy "Sentiment analysis algorithms and applications: A survey, Ain Sham University, Faculty of Engineering, Computer & Systems Department, Egypt 19 April 2014.

[5]. Ayesha Rashid et al, "A Survey Paper: Areas, Techniques and Challenges of Opinion Mining", International Journal of Computer Science (IJCSI), Vol 10 Issue 6 No 2, Nov 2013.

[6]. 5A Survey On Challenges In Sentiment Analysis Lincy W and Naveen kumar M International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 21 Issue 3 – APRIL 2016.

[7]. F. Luo, C. Li, and Z. Cao, Affective- feature-based sentiment analysisusing SVM classifier, 2016 IEEE 20th Int. Conf. Comput. Support. Coop.Work Des., pp. 276281, 2016.

[8]. Eirinaki, M., Pisal, S., Singh, J.: Feature-based opinion mining and ranking. J. Comput. Syst. Sci. 1175–1184 (2012)

[9]. Aggarwal Charu C, Zhai Cheng Xiang. Mining Text Data. Springer New York Dordrecht Heidelberg London: _ Springer Science+Business Media, LLC'12; 2012.

[10]. Pang, B., Lee, L., and Vaithyanathan, S. (2002). Thumbs up? Sentiment Classification using Machine Learning Techniques. In Proc. of EMNLP, pages 79–86.

[11]. E. Marrese-Taylor, J. D. Velasquez, F. Bravo-Marquez, "Opinion Zoom: A Modular Tool to Explore Tourism Opinions on the Web", In the Proceedings of the 2013 IEEE/WIC/ACM International Conferences on Web Intelligence (WI) and Intelligent Agent Technology (IAT), CA, pp. 261–264, 2013.

[12]. S ChandrakalaAnd C Sindhu: Opinion Mining And Sentiment Classification: A SURVEY DOI: 10.21917/ijsc.2012.0065 12.G.Vinodhini, RM.Chandrasekaran "Sentiment Analysis and Opinion Mining: A Survey", Volume 2 Issue 6, June 2012.

[13]. S. ChandraKala, C. Sindhu2 "OPINION MINING AND SENTIMENT CLASSIFICATION: A SURVEY", ICTACT Journal on soft computing, Volume: 03, Issue: 01, October 2012

[14]. BakhtawarSeerat, FarouqueAzam "Opinion Mining: Issues and Challenges (A survey)", International Journal of Computer Applications (0975 – 8887)Volume 49– No.9, July 2012

[15]. Liu, B.: Sentiment analysis: a multi- faceted problem. In: IEEE Intelligent Systems, pp. 1–5 (2010)

[16]. Michael Wiegand and Alexandra Balahur, "A Survey on the Role of Negation in Sentiment Analysis", Proceedings of the Workshop on Negation and Speculation in Natural Language Processing, 2010.

[17]. Adam L. Berger, Stephen A. Della Pietra and Vincent J. Della Pietra, "A maximum entropy approach to natural language processing", Computational Linguistics, Vol. 22, No. 1, pp. 39–71, 1996.

[18]. Thorsten Joachims. "Text categorization with support vector machines: Learning with many relevant features", Proceedings of the European Conference on Machine Learning, pp. 137–142, 1998.

[19]. Subhabrata Mukherjee, —Sentiment Analysis : A Literature Survey —,Indian Institute of Technology, Bombay. Department of Computer Science and Engineering, June 29, 2012.

[20]. Ms. KrantiVithalGhag, Dr.Ketan Shah, —Comparative Analysis of Effect of StopwordsRemoval on Sentiment Classification‖, IEEE International Conference on Computer, Communication and Control (IC4-2015). 21.ZohrehMadhoushi, AR Hamdon, S Zainudin, —Sentiment Analysis Techniques in Recent Works‖, Science and Information Conference 2015 July 28-30, 2015.

[21]. M. Biltawi, W. Etaiwi, S. Tedmori, Hudaib, and A. Awajan, "Sentiment Classification Techniques for Arabic Language: A survey," In Information and Communication Systems (ICICS), 7th International Conference, pp. 339- 346, 2016.

[22]. O. Kolchyna, T.TP. Souza, P.Treleaven, and T. Aste, "Twitter Sentiment Analysis: Lexicon Method, Machine Learning Method and Their Combination," arXiv preprint arXiv: 1507.00955, 2015

[23]. M.Graña, C. Toro, "Advances in Knowledge-based and Intelligent Information and Engineering Systems," Volume 1", IOS Press, pp. 2273, 2012

[24]. "Sentiment analysis", https://en.wikipedia.org/wiki/Sentiment_ analysis, Retrieved, 16-Feb-2017

[25]. W. Medhat, A. Hassan, and H. Korashy, "Sentiment Analysis Algorithms and Applications: A Survey," Ain Shams Engineering Journal, Vol.5, No. 4, pp.1093-1113, 2014

[26]. A. Das, S. Banyopadhyay and B. Gambäck, "The 5W Structure for Sentiment Summarization Visualization-Tracking," ERCIM, Retrived, 16-Feb- 2017

[27]. A. Selamat, H. Fujita, H. Haron, "New Trends in Software Methodologies, Tools and Techniques: Proceedings of the Thirteenth SoMeT_14," IOS Press, pp. 1128, 2014

Cite this article as :

M. Janaki, "A Survey On Sentiment Analysis", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 20-26, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT19474

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Brief Study on Cloud Security

Harlin Sheeba. M
Department of Computer Science, Darshan college R.V College Post, Mysore Road, Kengeri, Bangalore, Bangalore University, Karnataka, India

ABSTRACT

Cloud security is a protection of data, application, and network into the cloud environment (whether it's a public, private or hybrid cloud). In the cloud environment resources are shared among servers, users and individuals since the data centre of cloud provider is spread all over. We can access the data from any corner of the world. Even though cloud computing is becoming popular, security concerns start to arise. While using the cloud infrastructure the client gives up the control to the cloud provider on many issues which may affect security. The most critical one is when the owner starts to lose the control of information which is spread into the cloud.
This article briefly explains about how to get the advantages and benefits of cloud computing technology while getting rid of disadvantages like data, network and application attacks. It describes the security issues associated with cloud and cloud security providers like AWS (amazon web service) platform.
Keywords : Issues related with cloud Security, Cloud security attacks, Encryption and Security, Cloud Security control, AWS platform.

I. INTRODUCTION

Cloud security means keeping your data stored online safe. According to the recent study the average cost of a data breach worldwide now equals $ 3.86 million. However, the number vary greatly from country to country.

When it comes to security, timing is everything. The earlier you detect and fix the problem, the safe you are.The cloud technology is facing many technological challenges in different aspect of data and information handling and storage.

As you can see, knowing about the possible dangers are being ready to react to them fast can be a real lifesaver so, in this paper you will study about the security issues in the cloud you should be ready to face.

Cloud security issues

Virtualization:

It refers to the creation of a virtual resources such as server, file, storage, network. virtualization changes the definition of what the real resources is, so security is no longer trying to protect the privacy. The lack of

visibility and control over virtual networks is the main issue in the cloud security.

1. Access control and identity management:

Access control in the cloud security is a system with which the owner can regulate and monitor permission to access the data by formulating various policies. The owner should control unauthorized user access.

Identity management has to check whether it is a valid user, what does the user wantto do and what access does the user need to do his job.

2. Weaker authentication:

A lack of proper authentication is responsible for data breach multi-factor authentication system, like one-time password and phone-based authentication, protect cloud services by making it harder for attackers to steal the password. This isa preventative discussion that every business that has a online presence should have to ensure the safety of its customers.

1) Cloud security attacks:

- Data Attack
- Application Attack
- Network Attack

Data attack

1.a. Data breach:

A data breach is possibly the most important cloud security concern. When unauthorized user or program gains access over confidential data and can view, copy or transmit it leads to attack.

1.b. Data loss:

Data loss often happens due to physical destruction or it can also be a result of a target attack. It may also lead to permanent loss of data without backup.

1.c. Data removal:

Both the data of an individual or a company will be removed from the cloud. Unauthorized disclosure of data is dangerous if the cloud contains sensitive data.

1.d. Data Theft:

Data theft is the illegal transfer or storage of any information that is confidential, personal or password. The data can be theft by portable hard drive, memory cards, remote sharing and by USB drive.

1.e. Data integrity:

When a data is on a cloud anyone from any location can access those data. Then cloud does not differentiate between a sensitive and a common data thus enabling anyone to access those sensitive data's. Thus, there is lack of integrity.

1.f. **Data location:**

When the user uses the cloud, user probably won't know exactly where the data is hosted and where it will be stored.

2. Application attack:

2.a. Cloud Malware Injection:

This attack focuses on injecting a service implementation or evil virtual machines to the cloud environment. The main goal of this type of attack is to take control over the victim's data in the cloud, so the attacker uploads a crafted and tricks the image to be a part of the victim's cloud environment. After the user request will start forwarding to it causing the vulnerable code.

2.b. Cookie Poisoning:

Cookies stored on your computer's hard drive maintain a bit of information on that allows website you visit to authenticate your identity. Cookie poisoning is the modification of a cookie personal information in a web user's computer byan attacker. To gain unauthorized information about user for purposes such as identity theft. The attacker may

use the information to open a new account or to gain access to the user's existing accounts.

2.c. backdoor:

Another threat on a virtual environment empowered by cloud computing is the use of backdoor virtual machines that leak sensitive information and can destroy data privacy.

2.d. Hidden File Manipulation:

A developer working on the application could possibly assume the information will stay unharmed in the hidden field. However, a hacker can subsequently alter that using a common HTML editor.

3. Network level attack

3.a. Network Sniffing:

Sniffing involves inspecting, capturing, decoding and interpreting the information inside a network. The sole purpose behind this is to steal information which is very usual in the form of user id, password, network detail. This attack can be silent or invisible on the network.

3.b. IP Spoofing:

Sending and receiving the internet protocols(IP) packets is a primary way in which networked computers and other dives communicate.it consist a header and important routing information including the source address. If the packet has been spoofed, the source address will be forged.

3.c. Man in the middle:

It occurs when the third-party places itself in the middle of a connection and intercept or modify communication between the two

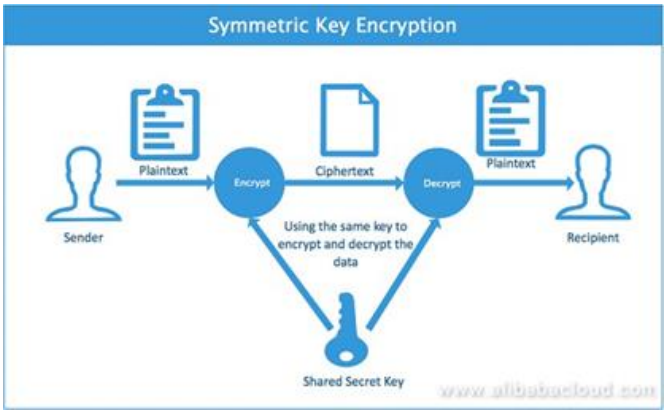
Encryption and security

When the data and information is shared through a network that data can be hacked so, encryption is used to make the data safe and secure.

There are two types of encryption:

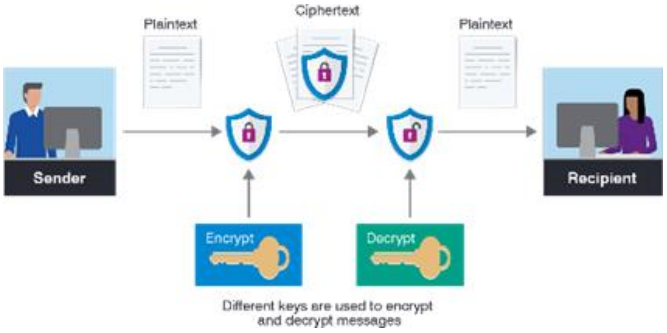
- Symmetric encryption
- Asymmetric encryption

1. Symmetric



When the same key is used for both encryption and decryption it is known as symmetric and it is also known as secret key cryptography

2. Asymmetric:



It uses public key for encryption and private key for decryption, it is also called as public key cryptography.

Encryption is regarded as one of the most effective approaches to data security.

Scrambling the content of any system, database, or a file in such a way that it's impossible to decipher without a decryption key. By applying encryption and practicing secure encryption key management, companies can ensure that only authorized users have access to sensitive data.

Even if lost, stolen, or accessed without authorization encrypted data is unreadable and essentially meaningless without its key.

Security

1. Data security:
It focuses on protecting the software and hardware associated with the cloud. It should secure from physical attack and external treats avoiding unauthorized access.

2. Application Security:
The measures taken to improve the security of an application often by finding, fixing, and preventing security vulnerabilities.

3. Network security:
Protecting the network over which cloud is running from various attacks like IP spoofing. Attack on data affects a single user whereas a successful attack on the network has the potential to affect multiple users, therefore network security is of foremost important.

Cloud security controls

1. Detective Control:
It helps to address the issues to detect and react instantly and appropriately to any attack.

2. Deterrent Control:
It means to reduce the purposeful attack on the cloud system, it reduces the threat level by giving a warning sign.

3. Preventive Control:
It is the strength of the system against any attack from vulnerabilities. It reduces the extent of potential damages and reduces the chances of attack.

4. Corrective Control:
It reduces the consequence of an attack by controlling/limiting the damage.

2) AWS platform

Amazon web Service(AWS) is the world's most broadly adopted cloud platforms. Millions of customers trust AWS to their power infrastructure.

Cloud security at AWs is the highest priority. As an AWS custom will benefit from a data centre and networkarchitecture built to meet the requirements of the most security of sensitive information.

3) Benefits:

1. **Keeps your data safe**: The Aws infrastructure puts storing safeguards in the place to help and protect privacy. All the data are stored in highly secure AS data centres.
2. **Saves money:** Cut cost by using Aws data centres, maintain the highest standards of security without having to manage yourown facility.
3. **Scale quality**: Security scales with your Aws cloud usage. No matter the size of your business the Aws

infrastructure is designed to keep your data safe.

4. **Cloud directory**: It enables you to build flexible, cloud directories for organizing hierarchies of data.
5. **Organizations**: It helps you to create group of AWS accounts that can use to more easily manage security and automation setting.
6. **Guard duty**: Provides intelligent threat detection to protect your AWS accounts

Amazon web service is a secure cloud service platform, offering compute power, database storage, content delivery and other functionality to help every organization.

In simple AWS allows you to do the following:

1. Running web and application server in the cloud to host dynamic website.

2. Securely store all your files on the cloud so you can access them from anywhere.

3. Using managed database like MySQL, oracle or SQL server to store information.

2. Adjust cloud access policies as a new service come up.

3. Remove malware from a cloud server.

4. Deliver static and dynamic files quickly around the world using a content delivery network(CDN).

Measures for cloud security

- Understand cloud usage and risk:
- Protect your cloud:

1. Data protection

2. Encrypt sensitive data

3. Set limitation on shared data.

4. Stop data from moving to unmanaged devices you don't know about.

5. Apply advance cloud provider.

• Respond to cloud security issues:

6. Require additional verification.

II. CONCLUSION

This paper gives a complete understanding about how the cloud security is attacked and it is clear that cloud security issues are increasing. To achieve complete security a organization or an individual should check their cloud infrastructure every time (not only if something happens) and to make sure to keep it up to date. Also, choose reliable cloud security provider with advanced version.

III. REFERENCES

[1]. www.skyhighnetworks.com
[2]. www.veracode.com
[3]. www.cloudcomputing-news.net
[4]. www.w3schools.in
[5]. www.techopedia.com
[6]. www.sciencedirect.com
[7]. http://www2.gemalto.com/cloud- security/
[8]. http://zerotoprotraining.com

Cite this article as :

Harlin Sheeba. M, "Brief Study on Cloud Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 27-31, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT19475

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

A Study on Intrusion Prevention/Detection

Dr. Vinay Ranganathan[1], Ravikant S. B.[2]
[1]Professor, Charan's Degree College, Ulsoor, Bangalore, Karnataka, India
[2]Assistant Professor, Charan's Degree College, Ulsoor, Bangalore, Karnataka, India

ABSTRACT

Today one of the most important challenges in communication is securities interior network. Understanding the basics of any technology is significant if ever aiming to totally perceive that technology. A good security answer not solely solves the protection perplexity, but also reduces the total cost of implementation and operation of the network. This paper highlights all the treads that have an effect on network security like legal problems, privacy concerns and people shortages. The eminent use of recent technologies needs associate hyperbolic have to be compelled to defend valuable data and network resources from corruption and intrusion. Now a day's anybody with a PC and an internet connection can download attacking tool and start attacking. These tools are commonly referred to as kiddle-scripts. Hackers are people who play around with software code in order to understand how it works. They might discover holes with in the systems and can oftenbe veryaltruistic. A crackeris one who breaks into or otherwise violates the system integrity of remote machines with malicious intent. As a result he gain unauthorized access and destroys very important data. There are many threats to port and protocols. Each attack has its characteristic and totally different handling to forestall system from them. There are several network security tools to facilitate network security like firewalls, proxy server, web contents filters and others. The paper gives all emphasis on the key elements of network security and its weaknesses.

Keywords : Network security, Data privacy, Security trends, Security goals, Hackers, Crackers.

I. INTRODUCTION

For several years now, society has been dependent on information technology (IT).With the rise of internet and e-commerce this is more applicable now than ever. People rely on computer networks to provide them with news, stock prices, e-mail and online shopping. People's credit card details, medical records and other personal information are stored on computer systems. Many companies have a web presence as an essential part of their business. The research community uses computer systems to undertake research and to disseminate findings. Computers control national infrastructure components such as the power grid. The integrity and availability of all these system shave to be protected against a number of threats. Amateur hackers, rival corporations, terrorists and even foreign governments have the motive and capability to carry out sophisticated attacks against computer systems. Therefore, the field of information and communication security has become vitally important to the safety and economic wellbeing of society as a whole. Moreover, to expose privacy breaches, security needs powerful intrusion detection and prevention systems (ID/PSs).This paper focuses on providing an up-to-date comprehensive state of the art of ID/PSs based on risk analysis. In Section 1.1, we present a background introduction to ID/PSs. In Section 2, we briefly outline the definition of risk management and its importance in developing well- managed security

systems. In Section 3, we provide a brief overview of ID/PSs, including a description of what ID/PSs are, the functions they serve, the two primary types of detection and prevention systems and different methods of ID that may be employed. Finally, in Section 4, we present the main goal of this work when we discuss in detail, with examples of some threat incidents occurred during the years 2018 and 2019, the requirements driving the necessity of developing anew detection mechanism to detect known and unknown threats based on intelligent techniques such as machine learning and autonomic computing.

II. METHODS AND MATERIAL

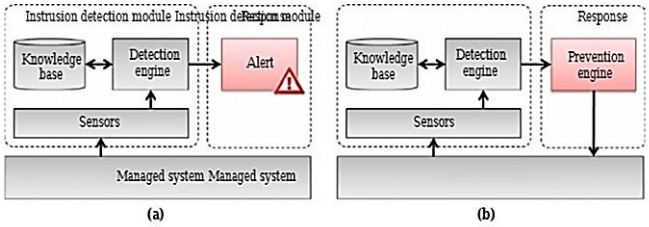
Background

In order to understand the ID/PSs, first one must understand the nature of the event they attempt to detect. An intrusion is a type of attack on information assets in which the instigator attempts to gain entry into a system or disrupt the normal operations of a system. In Brown's et al. (2002) view, intrusions are actions that attempt to bypass security mechanisms of computer systems. They are any set of actions that threaten s the integrity, availability or confidentiality of the information and the information system, where integrity means that data have not been altered or destroyed in an unauthorized manner and where confidentiality means that information is not made available or disclosed to unauthorized individuals, entities or processes. Availability means that system that has the required data ensures that it is accessible and usable upon demand by an authorized system user. Occasionally, an intrusion is caused by an attacker accessing the system from the internet or the network, or from the operating system of the infected machine, or exploits any security flaw of third party (middleware) applications that manages the information system. Attacks that come from these external origins are called outsider attacks. Insider attacks, involve unauthorized internal users attempting to gain and misuse non-authorized access privileges.ID is the process of monitoring computers or networks for unauthorized entry, activity or file modification. An intrusion detection system (IDS) is a software or hardware device that automates the ID process. IDSs can respond to suspicious events in one of several ways, which includes displaying an alert, logging the event or even paging an administrator. Intrusion prevention is the act of intercepting detected system threats in real time by preventing them from continuing to their intended destinations. It is useful against denial of services, floods and brute force attacks (Martin, 2009). An intrusion prevention system (IPS) is a software or hardware device that has all the capabilities of IDS and can also attempt to stop possible incidents. An IPS can respond to a detected threat in several ways: It can reconfigure other security controls in systems such as a firewall or router to block future attacks; It can remove malicious content of an attack in network traffic to filter out the threatening packets; or.it can (re-)configure other security and privacy controls in browser settings to prevent future attacks. Usually, disable prevention features in IPS products cause them to function as IDSs. IPSs are considered to be an extension of IDSs, although IPS and IDS both examine network traffic searching for attacks, there are critical differences. IPS and IDS both detect malicious or unwanted traffic. They both do so as completely and accurately as possible, but they differ in the type of response provided by each. As shown in Figure 1, the main function of an IDS product is to warn of suspicious activity taking place whiles is designed and developed for more active protection to improve upon the IDS other traditional security solutions, which can react in real time to block or prevent those activities. An effective risk management process is an important component of a successful IT security system. Organizations should use risk management techniques to identify the security controls necessary to mitigate risk to an acceptable level. To design an effective

ID/PS, proper requirements capture based on risk management is essential.

Importance of risk management

It is expected that all computer and communication systems, including all the applications, system software's and infrastructure and networking services, are protected from accidents and abuse by a set of safety measures composed from security, privacy, trust, audit, digital forensics and fault- tolerance functions, in order that they areto be available, reliable, trusted, safe, identifiable and auditable. Equally, these functions must provide the necessary facilities to end-users, make them feel safe and trusted in the complex world of information communication technology driven by the web, the internet, mobile and ad hoc wireless networks where today everything from business to leisure has become e-everything. These safety measures are vital in economic terms. Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. It is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions (Chichakli, 2009). A strong security program reduces levels of threat to reputation, operational effectiveness, legal and strategic risk by limiting an organization's vulnerability to attempted intrusion, thereby maintaining confidence and trust in the institution. Security concerns can quickly erode customer confidence and potentially decrease the adoption rate and rate of return on investment for strategically important products or services. An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should beta protect the organization and its ability to achieve its mission, rather than simply its IT assets. Therefore, the risk management process should not be treated as merely a technical function carried out by the IT experts who operate and manage the IT system, but as an essential mission-critical management function of the organization. Risk-based protection strategies are characterized by identifying, understanding, mitigating as appropriate and explicitly accepting the residual risks associated with the operation and use of information systems. To help protect organizations from the adverse effects of on-going, serious and increasingly sophisticated threats to information systems, organizations should employ a risk-based protection strategy along with ID/PSs, as a complete system of protection to ensure the integrity, availability and confidentiality of the information and the information systems.



Notes: (a) IDS; (b) IPS

Figure 1. Typical intrusion detection and intrusion prevention systems

Intrusion detection and prevention systems

Whitman and Mattered (2005) defined ID as the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies or standard security practices. An ID is a device or software application that monitors network and/or information system for malicious activities or policy violations and responds to that suspicious activity by warning the system administrator by one of several ways, including displaying an alert, logging the event or even paging the administrator. Intrusion prevention is the process of performing ID and attempting to stop detected

possible incidents. The IPS is a device or software application that has all the capabilities of IDS and can also attempt to stop possible incidents. IPS is designed and developed for more active protection to improve upon the IDS and other traditional security solutions. An IPS is definitely the next level of security technology with its capability to provide security at all system levels from the operating system kernel to network data packets (Martin, 2009). IPSs are designed to protect information systems from unauthorized access, damage or disruption, IDS informs of a potential attack, whereas IPS makes attempts to stop it. IPS has another benefit or advantage over IDS in that it has the ability to prevent known intrusion detected signatures, besides the unknown attacks originating from the database of generic attack behaviors (Beal, 2005).Modern ID/PSs are comprised two basically different approaches, network- based and host-based. A relatively recent addition of special IDS called application-based is a refinement of the host-based ID (Brown et al., 2002). Both servers and workstations are protected by host-based intrusion detection/prevention systems (HID/PSs) through secure and controlled software communication channels between system's applications and operating system kernel. The software is preconfigured to determine the protection rules based on intrusion and attack signatures. The HID/PS will catch suspicious activity on the system and then, depending on the predefined rules, it will either block or allow the event to happen. HID/PS monitors activities such as application or data requests, network connection attempts and read or write attempts to name a few. One potential disadvantage with this approach is that, given the necessarily tight integration with the host operating system, future operating system upgrades could cause problems. Network-based intrusion detection/prevention system (NID/PS) is software or dedicated hardware system that connects directly to a network segment and protects all of the systems attached to the same or downstream network segments. Network ID/PS devices are deployed in-line with the network segment being protected (Martin, 2009). All data that flows between the protected segment and the rest of the network must pass through the network ID/PS device. As the traffic passes through the device, it is inspected for the presence of an attack. When an attack is identified, the network ID/PS discards or blocks the offending data from passing through the system to the intended victim thus blocking the attack. NID/PS will intercept all network traffic and monitor it for suspicious activity and events, either blocking g the requests or passing it along should it be deemed legitimate traffic. One interesting aspect of network intrusion prevention system is that if the system finds an offending packet of information, it can rewrite the packet so the hack attempt will fail, but it means the organization can mark this event together evidence against the would be intruder, without the intruder's knowledge. Regardless of whether they operate at the network, host or application level, all ID/PSs use one of two detection methods; signature-based or anomaly-based (Whitman animator, 2005).

Anomaly detection is designed to uncover abnormal patterns that deviate from what is considered to be normal behavior, whereas ID/PS establishes a baseline of normal usage patterns and anything that widely deviates from it gets flagged as a possible intrusion. Anomaly detection can also vary but one should be aware that if any incident occurs more or less than two standard deviations from the statistical norm would raise an alarm. An example of this would be if a user logs on and off of a machine eight times a day instead of the normal one or two. Also, if a computer is used at 2:00 AM when normally no one outside of business hours should have access, this should raise some suspicions. At another level, anomaly detection can investigate user patterns, such as profiling the programs executed daily. Once again, if a user in an IT department suddenly starts to access accounting programs or recompiles them, then the system must immediately raise an alarm or alert its administrators

(Minnelli and McMillan, 2001).The major benefit of anomaly based detection methods is that they can be very effective at detecting previously unknown threats (Scarf one and Mel, 2007).Usually, in the first stage of a deployment of an anomaly-based ID/PS, the system learns what a normal behavior is. The controlled system is running as usual under the assumption that there is no abnormal behavior. During the learning stage, no attack must occur in the controlled system so that the ID/PS does not learn to ignore the attacks. The learning process can be addressed by variety of means such as machine learning or building statistical behavioral profiles. In the second stage of the deployment, in which the system possibly faces attacks, the ID/PS monitors the activities in the controlled system and compares them to the learned normal behavioral patterns. If a mismatch occurs, a level of "suspicion" is raised and when the suspicion, in turn, trespasses a given threshold, the system triggers an alarm. The main advantage of anomaly detection is that it does not require prior knowledge of intrusion and can thus detect new intrusions. The main disadvantage is that it may not be able to describe what an attack is and may have high false positive rate. Unauthorized behavior is normally detected by their misuse and is also commonly referred as signature detection. However, this method uses known patterns of unauthorized behavior to predict and detect subsequent similar attempts. These specific patterns are called signatures. For host-based intrusion detection/prevention, one example of a signature is "three failed logins." For network intrusion detection/prevention, a signature can be as simple as a specific pattern that matches a portion of a network packet (Whitman and Mattered, 2005). For instance, packet content signatures and/or header content signatures can indicate unauthorized actions. The occurrence of signature might not signify an actual attempted unauthorized access (for example, it can be an honest mistake), but it is a good idea to take each alert seriously. Depending on the robustness and seriousness of a signature that is triggered, some alarm, response or notification should be sent to the proper authorities. The concept behind misuse detection schemes is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. This means that these systems are not unlike virus detection systems, they can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods. An interesting point to note is that anomaly detection systems try to detect the complement of "bad" behavior. Misuse detection systems try to recognize known "bad" behavior. The main issues in misuse detection systems are how to write a signature that encompasses all possible variations of the pertinent attack, and how to write signatures that do not also match non-intrusive activity (Newman et al., 2004).The main advantage of misuse detection paradigm is that it can accurately and efficiently detect instances of known attacks. The main disadvantage of misuse detection method is that it lacks the ability to detect the newly invented attacks. Signature databases must be constantly updated, and IDSs must be able to compare and match activities against large collections of attack signatures.

III. CONCLUSION AND FUTURE RECOMMENDATIONS

Today's interrelated computer network is a dangerous realm, filled with people that have millions of man-hours available to employ against the strongest of security strategies. The only way to beat them is to know when they are attempting an attack and counter their attempts. Strategy is the key and selecting the right ID or prevention system will be instrumental in ensuring that an enterprise's networks and systems remain secure. As security incidents become more numerous, ID/PS and supporting tools are becoming increasingly necessary. These intelligent ID/PSs and tools should use a combination of several intelligent techniques from the subject areas of autonomic

computing, machine learning, artificial intelligence and data mining to assist them to determine what qualifies as an intrusion, versus normal activity, by building acknowledge base which grows as and when new facts or knowledge come to light.ID/PSs are still a fledgling field of research. However, it is beginning to assume enormous importance in today's computing environment. The combination of facts such as the unbridled growth of the internet, the vast financial possibilities opening up in electronic trade and the lack of truly secure systems make it an important and pertinent field of research and development. Future research and development trends seem to be converging towards a model that is based on multi-agent ID/PSs based on and managed by autonomic computing paradigm together with advanced techniques from natural language processing, artificial intelligence and data mining to help improve anomaly ID, based on itself-managed properties such as self-configuration, self-optimization, self-healing and self-protection. These autonomic computing properties have to be extended to include self-detection and self-prevention. The results from these techniques will aid an analyst to clearly distinguish malicious attack activities from normal everyday on-attack activities. They will make ID/PSs smart and a formidable part of security management system with a rich but simplified alarm handling and presentation of security violation activities for easy human consumption.

IV. REFERENCES

[1]. https://en.wikipedia.org/wiki/Intrusion_detection_system
[2]. Data Protection Technical Guidance Note: (PET) Privacy enhancing technologies (ICO)
[3]. https://searchsecurity.techtarget.com/definition/intrusion-detection-system
[4]. http://www.legalserviceindia.com/articles/articles.html

Cite this article as :

Dr. Vinay Ranganathan, Ravikant S. B., "A Study on Intrusion Prevention/Detection", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 32-37, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT19476

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Cloud Security Ecosystem for Data Security and Privacy

Divyashree D, Santhosh Kumar
Department of Computer Science, Soundarya Institute, Bangalore, Karnataka, India

ABSTRACT

In the past couple of years Cloud Computing has become an eminent part of the IT industry. Because of its economic benefits more and more people are heading towards Cloud adoption. In present times there are numerous Cloud Service providers (CSP) allowing customers to host their applications and data onto Cloud. However, Cloud Security continues to be the biggest obstacle in Cloud adoption and thereby prevents customers from accessing its services. Various techniques have been implemented by provides to mitigate risks pertaining to Cloud security. In this paper, we present a Hybrid Cryptographic System (HCS) that combines the benefits of both symmetric and asymmetric encryption thus resulting in a secure Cloud environment. The paper focuses on creating a secure Cloud ecosystem wherein we make use of multifactor authentication along with multiple levels of hashing and encryption. The proposed system along with the algorithm are simulated using the Cloud simulator. To this end, we illustrate the working of our proposed system along with the simulated results.

Keywords : Cloud Security, Data Security, Data Privacy, Cloud Simulator

I. INTRODUCTION

In today's times Cloud computing has a significant impact on the IT industry. With growing popularity more and more organizations are making use of cloud services [1]. Although cloud services have a widespread acceptance but the fear pertaining to security and privacy of these services continue to be an open challenge. With rapid technological advancements these services could be easily accessed through smart phones thus allowing users to share pictures, video, documents and other important data across various platforms on a real time basis [2].

However, a security breach in their cloud account could lead to stolen data which would indeed result in huge losses.

Security has always been a concern in the domain of information technology. With Cloud services handling critical data which can be accessed from anywhere through the internet makes security a prominent concern [3]. The pervasive nature of Cloud and its disbursal of data across various geographical locations amounts to high security risks. While talking of Cloud Security there are many aspects which one needs to consider such as, trusted authentication, appropriate authorization, data security and privacy. These are some of the basic security goals which are extremely essential for every cloud provider to incorporate [4]. Since security has been seen as an attribute for information technology, data encryption has been one of its key measures in ensuring data security protection. Many algorithms in the past have been proposed for conducting efficient data encryption. These algorithms range from DiffieHellman, RSA, DES to AES, RC4 and 3DES. Each of these algorithms have their own advantages along with their demerits. These algorithms are broadly classified as being symmetric or asymmetric in nature.

Our focus here would be to create a Secure Cloud Ecosystem that leverages from the benefits of both symmetric and asymmetric encryption. We make use of RSA (Asymmetric) and AES (Symmetric) algorithms for carrying out data encryption. We aim at creating a comprehensive Cloud Environment that has security measures at all levels from creating and storing username and password, multifactor authentication, transmission of user data and data encryption.

The rest of the paper is categorized as follows: Section II talks about security concerns pertaining to Cloud Computing.

Section III elucidates the proposed work wherein the proposed system and its working are explained. Section IV discusses the algorithm that depicts the workflow of the entire system, whereas its successful simulation and its results are discussed in Section V. Finally, Section VI concludes the paper.

II. SECURITY CONCERNS IN CLOUD

Security in cloud plays an important role in creating a sense of belief and confidence between the customer and Cloud Service Provider (CSP). Since, all the user data is stored, managed and processed at the cloud end thus it is the duty of the CSP to mitigate any kind of risk pertaining data security and privacy. Following are certain Cloud security which a CSP needs to keep in mind while dealing with user data.

- Data Protection: Cloud computing poses several data protection risks for cloud users, providers and brokers. There are different kinds of SLAs involved between the cloud user, provider and broker leading to certain kinds of data leaks. Many of times it is seen that it becomes difficult for the cloud user to have a check on the data handling practices of the cloud provider [5]. Further there can be challenges due to the complex network topology between cloud and the end user that gives scope to many network related attacks.

- Loss of Data: Mission critical applications involving the use of crucial data are not preferred to be offloaded to cloud. Due to the presence of common resource pools, applications run on the same platform that could lead to disclosure of user's information through its application. In many cases proper encryption schemes for secure processing are not adopted for data transfer and its storage by the cloud vendor.
- Traffic hijacking: is also one of the prominent threats that end users face while leveraging form cloud computing. In 2013 Cloud Security Alliance ranked it as the third most extreme threat to cloud security. In such kind of an attack, hackers tend to obtain a user's security credentials and proclaim unauthorized access to its data. After which all the activities of a user including its confidential transactions happening on the cloud are now open to a hacker [6]. The hacker can easily tamer the users data along with have access to its applications running on cloud. A similar kind of an attack was faced by Amazon in 2010 when the hackers had stolen the session IDs and had access to client's credentials.
- Isolation of Resources: In present times the two main characteristics of cloud computing are multi-tenancy and shared resources. This risk category caters to processes that work and manage resources like storage, memory, bandwidth and even reputation between different tenants. Cloud provides a shared platform for different kind of applications from different users. This common resource pool adds problems relating to security thus making the user data more vulnerable to data breaches.
- Malicious Insider: Usually, the damage which may be caused by malicious insiders is often far

greater than expected. Such type of attackers uses their own device as a medium to inject the unsecure code to the cloud. This code behaves maliciously when properly injected and the control of which lies in hands of the user operating it [7]. This code can provide access of information to the malicious user, criticality of which depends on the capability of the designed code and the level of security measures taken by the cloud.

III.PROPOSED WORK

Over the years, many security models have been presented about Cloud computing but most of them had their focus on a particular security threat rather than catering to the entire system. In this section we, discuss our proposed Secure Cloud Ecosystem which intends to provide security measures on a pan Cloud basis. The aim of our system is to ensure data security and privacy right from the process of user authentication to data being stored on Cloud. We make use of multiple algorithms for ensuring the efficiency of our system. Our primary focus in this section would be to illustrate upon our encryption & decryption process along with describing our system architecture.

A. Data Encryption

In this sub section, we would be talking about the ways in which data encryption takes place at the Cloud end. The following is a flow chart which clearly depicts the working of our proposed system.

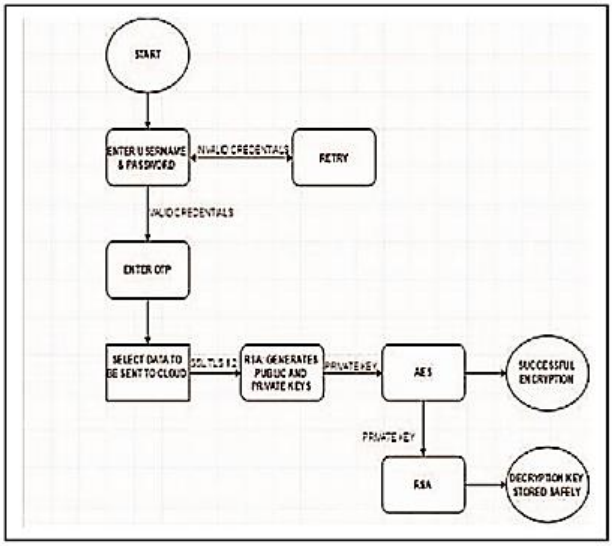


Fig. 1. Encryption Process Flowchart

As it can be seen in the figure, no unauthorized user will have access to and kind of user data. This is ensured by making use of multifactor authentication in form of One Time Password (OTP). Once a legitimate user enters its login credentials an OTP is sent to its registered mail which one needs to enter to make certain successful login. Upon successful login the user can anytime send or retrieve data from Cloud. If a user wishes to store its data onto the Cloud, in this case the data can pass through a secure network channel to protect it from any kind of hackers residing over the network. Once the data reaches the Cloud end it undergoes encryption through our Hybrid Cryptographic System. At first the RSA generates Public and Private Keys which are later used by the AES to commence data encryption. The Private Key of the AES again undergoes encryption through RSA and is saved in the data base after adding salt to it. In this way the user data is stored in an encrypted form at the Cloud end and whenever the user wishes to access it will be available after successful decryption.

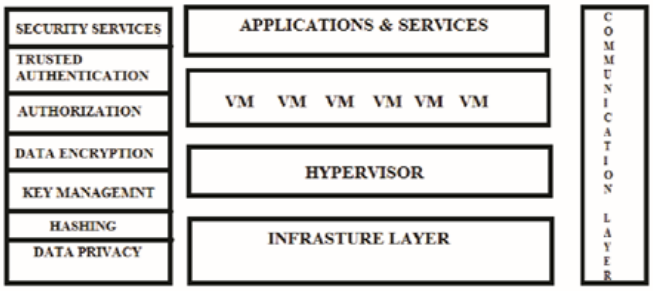


Fig. 2. System Architecture

The list of security services which our Secure Cloud Ecosystem ensure are:

B. System Architecture

In this sub section, we would be discussing the system architecture of our proposed Secure Cloud Ecosystem. The system architecture comprises of various physical entities that constitute the entire ecosystem. Here we would be talking about all different actors that constitute the Cloud, their roles, basic functionalities and the security services which our system provides. The following figure exemplifies our system architecture.

- **Trusted Authentication**: Only a legitimate user will be allowed to access services and data being hosted on Cloud.
- **Authorization**: The system ensures proper authorization by only allowing system admin to have access to decryption keys. It is only the Cloud admin who is aware of the salted value added to every user password and Decryption Key before being saved in the database.
- **Data Encryption**: The system makes use of Hybrid Encryption by allowing RSA and AES algorithms to encrypt user data. The proposed system leverages the benefits of both symmetric and asymmetric data encryption. We make use of RSA2048 and AES256 for our encryption process.
- **Hashing**: SHA512 and bcrypt functions are used for securing user password.
- **Key Management**: The Private Key of AES is encrypted and salted and safely stored into the database. The decryption keys are also saved soon after the encryption gets over. The SHA512 key is protected using keyed-hash message authentication code (HMAC).

IV. ALGORITHM

The working of our proposed system is explained through the illustration of the algorithm that forms the core for it. The algorithm depicts the functioning of the system by representing the entire process from user authentication to storage and retrieval of user data from Cloud.

STEP 1: Create Username and Password

STEP 2: Password creation using CSPRNG

STEP 3: SHA512 and bcrypt function used for password protection

STEP 4: SHA512 key is protected using HMAC algorithm

STEP 5: Enter login credentials

STEP 6: Make use of OTP for multifactor authentication.

Validity of OTP is 5 minutes.

STEP 7: User stores data on Cloud

STEP 8: SSL and TLS 1.2 are used for conducting transfer user data over the network

STEP 9: RSA algorithm is used for Public Private Key generation

STEP 10: AES algorithm encrypts data using RSA Private Key

STEP 11: Private Key encrypted using RSA

STEP 12: User request to access data

STEP 13: RSA generates Decryption Keys

STEP 14: Decryption process takes place

STEP 1 to STEP 6 depict the authentication process wherein trusted authentication takes place through

the use of original user credentials. Multifactor authentication has also been performed by making use of One Time Password (OTP), which is sent to the registered email-id of the user. In STEP 2, we make use of CSPRNG (Cryptographically Secure Pseudo-Random Number Generator) which is a salting technique used for protecting passwords in case there is an attack on credential database. In STEP 3, hashing functions such as SHA512 and decrypt have been used for ensuring password protection. STEP 9 to STEP 11 illustrate the process of data encryption that happens at the Cloud end. STEP 12 to STEP 14 demonstrate the decryption process in case the user needs to access its data.

V. CONCLUSION

In this paper, we present a Hybrid Cryptographic System (HCS) that combines the benefits of both symmetric and asymmetric encryption. The Secure Cloud Ecosystem which we propose ensures data security and privacy by implementing different encryption techniques at various levels. The system also makes use of certain hashing and salting techniques which even strengthens the entire encryption process. During the design of our system we also made sure of trusted authentication thereby allowing the feature of One Time Password (OTP). In future we wish to incorporate definite steps that would enhance the efficiency and generality of our system. This could be in form of extending our system to work for a multi cloud environment and add certain backup and recovery features which would prevent data loss in case of an attack.

VI. REFERENCES

[1]. Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.

[2]. Pawar, Pramod S., et al. "Security-as-a-service in multi- cloud and federated cloud environments." IFIP International Conference on Trust Management. Springer International Publishing, 2015.

[3]. Nair, Nikhitha K., K. S. Navin, and Soya Chandra. "Digital Signature and Advanced Encryption Standard for Enhancing Data Security and Authentication in Cloud Computing." (2015).

[4]. Wang, Cong, et al. "Privacy-preserving public auditing for data storage security in cloud computing." INFOCOM, 2010 Proceedings IEEE. Ieee, 2010.

[5]. Hendre, Amit, and Karuna Pande Joshi. "A semantic approach to cloud security and compliance." 2015 IEEE 8th International Conference on Cloud Computing. IEEE, 2015.

[6]. Khanna, Abhirup, Sarishma. (2015). Mobile Cloud Computing: Principles and Paradigms. IK International.

[7]. Khanna, Abhirup. "RAS: A novel approach for dynamic resource allocation." Next Generation Computing Technologies (NGCT), 2015 1st International Conference on. IEEE, 2015.

[8]. Calheiros, Rodrigo N., et al. "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms." Software: Practice and Experience 41.1 (2011): 23-50.

[9]. Huang, Wei, et al. "The State of Public Infrastructureas- a-Service Cloud Security." ACM Computing Surveys (CSUR) 47.4 (2015): 68.

[10]. Aich, Asish, Alo Sen, and Satya Ranjan Dash. "A Survey on Cloud Environment Security Risk and Remedy." Computational Intelligence and Networks (CINE), 2015 International Conference on. IEEE, 2015.

[11]. Singh, Aarti, and Manisha Malhotra. "Security Concerns at Various Levels of Cloud Computing Paradigm: A Review." International Journal

Cite this article as : Divyashree D, Santhosh Kumar , "Cloud Security Ecosystem for Data Security and Privacy", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 38-42, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT19477

National Conference on Communication Technology & Network Security In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Communication Technology and Network Security

Prof. Ganapathi A
M.Tech(CNE), MSc(IT), B.Tech(CS), DCS &E, Triveni Institute of Commerce & Management, Bangalore, Karnataka, India

ABSTRACT

Security is a fundamental component in the Communication Technology and network Security. The first and foremost thing of every network planning, designing, building, and operating a network is the importance of a strong security policy. Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern. The internet structure itself allowed for many security threats to occur. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. There are different kinds of attack that can be when sent across the network. By knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide and all of these required different security mechanisms. In this paper, I am trying to discuss current communication technology different kinds of attacks along with various different kinds of security mechanism that can be applied according to the need and architecture of the network.

Keywords : Information and Communication Technology, Intrusion, Confidentiality, Firewall, Spoofing, Byzantine attack.

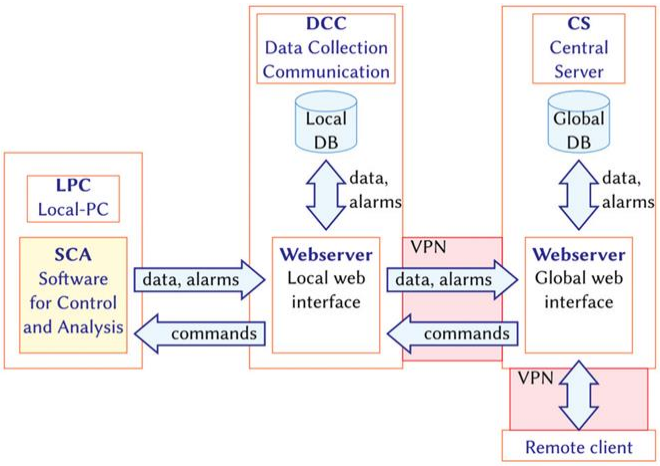
I. INTRODUCTION

Information and communications technology (ICT) is an extended term for information technology (IT) which stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), computers as well as necessary software, its storage and the audio-visual systems, which enable all users to access, store, transmit, and manipulate information. The term ICT is also used to refer to the combining of audio-visual and telephone networks with computer networks through a single cabling or link system. There are large economic incentives (huge cost savings due to elimination of the telephone network) to merge the telephone network with the computer network system using a single unified system of cabling, signal distribution and management. However, ICT has no universal definition, as "the concepts, methods and applications involved in ICT are constantly evolving on an almost daily basis. "The broadness of ICT covers any product that will store, retrieve, manipulate, transmit or receive information electronically in a digital form e.g. personal computers, digital television, email and even the modern day robots. The last few decades have witnessed a tremendous & phenomenal growth in the field of Information & Communication Technology (ICT) in education also which has influenced life of people especially students in some way or the other. ICT is arguably the technology area that has had the strongest impact on society during the past 60 years. The technology is visibly present in our use of computers, smart phones, information search, robotics and intelligent agents, but, has an even

greater impact as an enabling technology for a large number of application areas, such as medicine and healthcare, energy production and distribution, finance, public management and transport logistics to name a few. This progress has enabled to get prompt access to any required information. In these modern times of technological advancements, children are more interested in trying out; hence, a teacher should act as a facilitator and should encourage a child / student to advance technologically and in the right direction. In the field of education, ICT can be used to enhance quality and value of education especially through integration.

The massive global infrastructure has no fundamental security mechanisms built in to protect itself. It is thus set for unbelievable information sharing on both levels of unimportance and extreme necessity and so the need for network security is paramount to prevent against countless threats. Network Security is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. Security has become important issue for large computing organizations [1]. Computer network security is concerned with preventing the intrusion of an unauthorised person into a computer network. As computer connectivity increases, computer network security becomes more complex. Intrusion [2] is any set of actions that attempt to compromise the integrity, confidentiality or availability of a computer system resource (for example, unauthorised distribution of sensitive material over the Internet).

A Typical ICT Model



II. Types of Security Attacks

Here we are presenting some basic class of attacks which can be a cause for slow network performance, uncontrolled traffic, viruses etc. Attacks to network from malicious nodes. Attacks can be categories in three: "Passive Attacks" when a network intruder intercepts data travelling through the network, and "Active Attacks" in which an intruder initiates commands to disrupt the network's normal operation. An advanced persistent threat (APT) is a prolonged and targeted cyberattack in

which an intruder gains access to a network and remains undetected for a period of time. The intention of an APT attack is usually to monitor network activity and steal data rather than to cause damage to the network or organization.

2.1 Active attack

Some active attacks are spoofing attack, Wormhole attack, Modification, Denial of services, Sinkhole, and Sybil attack.

a. Spoofing

When a malicious node miss- present his identity, so that the sender change the topology.

b. Modification

When malicious node performs some modification in the routing route, so that sender sends the message through the long route. This attack cause communication delay occurred between sender and receiver.

c. Wormhole

This attack is also called the tunnelling attack. In this attack an attacker receives a packet at one point and tunnels it to another malicious node in the network. So that a beginner assumes that he found the shortest path in the network [1].

d. Fabrication

A malicious node generates the false routing message. This means it generate the incorrect information about the route between devices [2].

e. Denial of services

In denial of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy the network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response.

f. Sinkhole

Sinkhole is a service attack that prevents the base station from obtaining complete and correct information. In this attack, a node tries to attract the data to it from his all neighbouring node. Selective modification, forwarding or dropping of data can be done by using this attack [1].

g. Sybil

This attack related to the multiple copies of malicious nodes. The Sybil attack can be happen due to malicious node shares its secret key with other malicious nodes. In this way the number of malicious node is increased in the network and the probability of the attack is also increases. If we used the multipath routing, then the possibility of selecting a path malicious node will be increased in the network [1, 2, and 3].

2.2 Passive attack

The names of some passive attacks are traffic analysis, Eavesdropping, and Monitoring [1, 2, and 3].

a. Traffic analysis

In the traffic analysis attack, an attacker tries to sense the communication path between the sender and receiver. An attacker can found the amount of data which is travel from the route of sender and receiver. There is no modification in data by the traffic analysis.

b. Eavesdropping

This is a passive attack, which occurred in the mobile ad-hoc network. The main aim of this attack is to find out some secret or confidential information from communication. This secrete information may be private or public key of sender or receiver or any secrete data.

c. Monitoring

In this attack in which attacker can read the confidential data, but he cannot edit the data or cannot modify the data.

2.3 Advance attacks

a. Black hole attack

Black hole attack is one of the advance attacking which attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. An hacker use the flooding based protocol for listing the request for a route from the initiator, then hacker create a reply message he has the shortest path to the receiver . As this message from the hacker reached to the initiator before the reply from the actual node, then initiator will consider that, it is the shortest path to the receiver.

b. Rushing attack

In rushing attack, when sender send packet to the receiver, then attacker alter the packet and forward to receiver. Attacker performs duplicate sends the duplicate to the receiver again and again. Receiver assumes that packets come from sender so the receiver becomes busy continuously.

c. Replay attack

It this attack a malicious node may repeat the data or delayed the data. This can be done by originator who

intercept the data and retransmit it. At that time, an attacker can intercept the password.

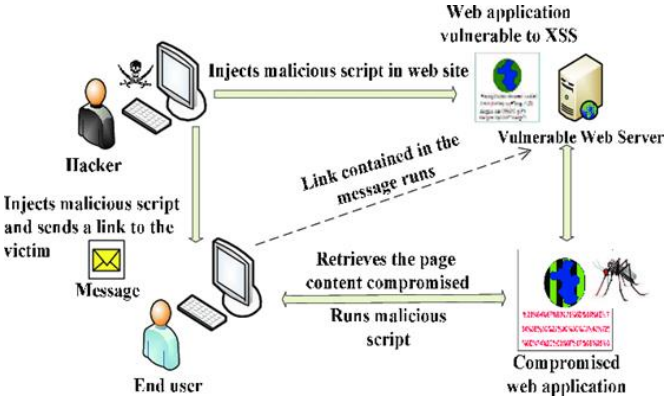
d. Byzantine attack

A set of intermediate node works between the sender and receiver and perform some changes such as creating routing loops, sending packet through non optimal path or selectively dropping packet, which result in disruption or degradation of routing services.

e. Location disclosure attack

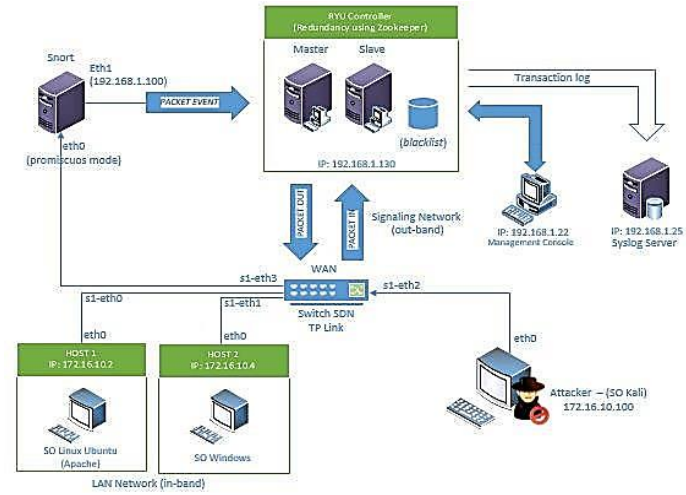
Malicious node collects the information about the node and about the route by computing and monitoring the traffic. So malicious node may perform more attack on the network.

Overview of Security Attacks



III. Internet Security Technology

Open Flow Network Security Architecture



With the rapid growth of interest in the Internet, network security has become a major concern to companies throughout the world. The fact that the information and tools needed to penetrate the security of corporate networks are widely available has increased that concern. Internet security tools typically provide authentication, encryption, identify attacks, and block and filter packets. There are two different access control approach used, the Discretionary Access Control (DAC) and the Mandatory Access Control (MAC). Commercial systems are based on DACs which indicates that the resources' owner specifies who may access and who may not access the resources. MAC on the other hand, works as a security officer that decides who is allowed and who is disallowed access to a particular resource.

3.1 Cryptographic systems

Cryptography originally denotes the art of keeping information secret by the use of codes and ciphers. It is a prevalent tool for security engineering today since one can notice that the computer industry has extensively utilized cryptography as a basic standard in secured software development. The main process of cryptography is to encrypt or scramble an input message called 'plain text' with cryptography algorithm, which results in an output message called 'cipher text or cryptogram'. At the receiver side, in order to change cipher text into a readable format, a cryptographic key must be used for decryption. A cryptographic key is created from a string of digits. If the same key is used for both encryption and decryption, it is called a symmetric key. Another kind of key is an asymmetric key, which simply means the encryption key differs from the decryption key. At the present time, a strong cryptography is considerably powerful security technology. The strong cryptography algorithm is based on reliability of mathematical calculation. The calculation of cryptographic key is so complicated that it could not be cracked within a short time. Anyone, who wants to crack it, is supposed to take several years to achieve his goal.

As long as people rely on mathematical complexity, the strong cryptography is still the most efficient tool to safeguard computer security. The immediate or significant arguments against this idea have not yet come forward.

3.2 Firewall

A firewall is a typical border control mechanism or perimeter defence. The purpose of a firewall is to the front line defence mechanism against intruders. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. There are basically two different types of firewalls packet filters and proxies. Packet filtering firewalls are those designed to filter IP addresses, MAC addresses, TCP or UDP ports, and subnets, among others. A packet filter is, in principle, a router with the ability to filter or block traffic to and from a network. Packets to a specific service can also be blocked. IP packets to a computer on an internal network with certain options turned on or off could also be screened. Information on the TCP/IP level is used to decide whether to allow or disallow a particular type of traffic. Packet filtering firewalls look at each packet header entering or leaving the network and accept or reject a particular packet based on specific rules defined by the user/network administrator. Packet filtering is fairly effective and transparent to users. They, however, are difficult to configure and are also susceptible to IP spoofing a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. Proxy servers, on the other hand, intercept all the messages entering and leaving the network but it differs in that the proxy hides IP addresses of the clients in the internal network.

3.3 Intrusion Detection Systems

An Intrusion Detection System (IDS) is an additional protection measure to firewalls, virus scanners, and encryption that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. Attacks can take many forms, as previously discussed. Attack can occur through applications such as Netscape, Internet Explorer, Eudora, or Microsoft Outlook and also via the operating system, regardless of whether it is UNIX, Windows or Mac-based. You also can be attacked via the network through Denial of Service (DoS) attacks or attacks against protocols. IDS products are used to monitor connection in determining whether attacks are been launched. Everything from a simple port scan to a full attack against your Web server can be detected by the IDS system. A flag is raised when an attack is suspected. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack. Software and hardware designed to detect attackers can pick up many levels of intrusions. IDSs will not be capable of detecting certain things, such as information about ISP and IP address range. Public information doesn't really affect the system until the attackers begin to ping the system to see if it is alive. These techniques are used for reconnaissance and mapping out potential targets.

3.4 Anti-Malware Software and scanners

Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so called anti- Malware tools are used to detect them and cure an infected system. This type of tool acts as an internal defence mechanism. The most common type of anti-Malware software is virus scanners. These tools often consist of two different but related parts: a scanner (or verifier) and a disinfector. Vulnerability scanners are special tools designed to automatically find vulnerabilities in systems.

3.5 Internet Protocol Security (IPSec)

The technology that brings secure communications to the Internet Protocol (IP) is called Internet Protocol Security (IPSec). IPSec as a framework that provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithms(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. IPSec is a point-to-point protocol, one side encrypts, the other decrypts and both sides share key or keys. IPSec can be used in two modes, namely transport mode and tunnel modes. IPSec is a collection of open standards that work together to establish data confidentiality, data integrity and authentication between peer devices.

3.6 Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) is a suite of protocols that actually uses many different standards of key exchange, authentication and encryption to get its job done. The server typically provides regular web service http on port 80, and SSL- encrypted web traffic https over port 443. SSL is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL is a good choice for adding end-to-end protection to applications, it protects against eavesdropping, session hijacking and Trojan servers. SSL can be applied to online security and privacy that provide authentication, integrity, confidentiality and Non-repudiation. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity

3.7 Data Encryption Technology

Data encryption technology categories can be divided in data storage, data transfer, data integrity, authentication and key management techniques. Data encryption is stored in the memory in order to prevent data loss and destruction. The transmission process in the information encrypted is commonly in the form of circuit encryption and port encryption. Data integrity identification technology is to protect information transfer, storage, access, identification and confidential treatment of people and data. In this process, the system is characterized by the parameter value judgment on whether the input is in line with the set value. Data are subject to validation, and encryption enhanced the protection. Key management is a common encryption in many cases. Key management techniques include key generation, distribution, storage, and destruction, etc.

3.8 Intrusion detection technology

Intrusion detection technology is to ensure the safety of the design and the rational allocation. Intrusion detection technology can quickly find anomalies in the system and the authorized condition in the report. It can address and resolve system vulnerabilities in a timely manner. Technologies that are not in line with security policies are frequently used.

IV. CONCLUSION

Security is a very difficult and vital important topic. Everyone has a different idea regarding security' policies, and what levels of risk are acceptable. The key for building a secure network is to define what security means to your need of the time and use. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system around him but Users who find security policies and systems too restrictive will find ways around them. There are different kinds of attacks on the security policies and also growing with the advancement and the growing use of internet. In this

paper, I have mentioned different kinds of attacks that penetrates our system. As the threats are increasing, so for secure use of our systems and internet there are various different security policies are also developing. I have mentioned some of the security policies that can be used mostly by number of users and some new advance qualities that fits to the todays more penetrating environments like Trend micro security mechanism, use of big data qualities in providing security, etc. Security is everybody's business, and only with everyone's cooperation, an intelligent policy, and consistent practices, it is achievable.

V. REFERENCES

[1]. Importance of Network Security, found at http://www.content4reprint.com/computers/security/importance-of-networksecurity-system.htm

[2]. R. Heady, G. Luger, A. Maccabe, and M. Servilla(1990). The Architecture of a Network Level Intrusion Detection System. Technical Report Dept. of Computer Science, University of New Mexico, New Mexico, August.

[3]. Neha Khandelwal, Prabhakar.M. Kuldeep Sharma, “An Overview Of security Problems in MANET”. [4]. Anupam Joshi and Wenjia Li. “Security Issues in Mobile Ad Hoc Networks- A Survey”.

[4]. Ali Ghaffari, “Vulnerability and Security of Mobile Ad hoc Networks”

[5]. Predictions and Trends for Information, Computer and Network Security [Online] available: http://www.sans.edu/research/security-laboratory/article/2140

[6]. A White Paper, —Securing the Intelligent Network‖, powered by Intel corporation.

[7]. Network Security [Online] available: http://en.wikipedia.org/wiki/Network_security.

[8]. Network Security: History, Importance, and Future‖, University of Florida Department of Electrical and Computer Engineering, Bhavya Daya.

[9]. Ateeq Ahmad, Type of Security Threats and its Prevention”, Ateeq Ahmad, Int.J.Computer Technology & Applications, Vol 3 (2), 750-752.

[10]. Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257

Cite this article as :

Prof. Ganapathi A, "Communication Technology and Network Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 43-49, September-October 2019.

Journal URL : http://ijsrcseit.com/CSEIT19478

National Conference on Communication Technology & Network Security In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Artificial Intelligence and Its Review

Nayana S Shankar, Mahalakshmi, Dr. Kavitha
Department of Computer Applications, Dayananda Sagar College of Arts, Science and Commerce, Bangalore, Karnataka, India

ABSTRACT

In the current period artificial intelligence is the wide concept that all humans are curiously preparing algorithms to establish it everywhere. The work we have done is based on Artificial Intelligence . Artificial intelligence is very much important because that can reduce stress of human beings and do the work automatically according to the human knowledge and it will think how the humans thinks, where it is programmed by humans .The researchers studied about Artificial intelligence to help human in many ways. The algorithms are built and came out in such a way that humans will get accurate solution to their problems. in this research paper we done about AI and defined AI ,its advantages, and also mentioned applications of AI . we have researched some points about the use of AI in healthcare. we have taken the example of robots that works by artificial intelligence and where it is implemented and also how it works .

I. INTRODUCTION

In today's computing world, technology is growing very fast and wide, and we people are exploring new engrossing technologies for our convenience, also getting in touch with different new soft-wares day by day.

Here one of the intensifying technologies in computer science is ARTIFICIAL INTELLIGENCE[1] which is ready to create a new revolutionizing world by making intelligent machines which does magical things over the world. The artificial intelligence occupied all around us. It is currently dealing with a variety of subfields, ranging from general to specific such as self-driving cars, playing chess, proving theorems, playing music, painting, etc.

AI is one of the most fascinating and universal fields of computer science which has a great scope in the present and future. AI holds a tendency to make a machine to work as a human, which means it acts the same as a human does but behind the background, it's all developed by humans itself.

Artificial intelligence

It is an approach to make a computer or a robot or a product to think that how human thinks. AI will learn, decide, develop, analyze and work and repeat the process. when it tries to solve problems it analyses and finally this study outputs intelligent software systems. **[2]**The ambition of AI is to improve computer functions which are related to human knowledge it is composed of Reasoning, learning, problem-solving, precision, linguistic intelligence.

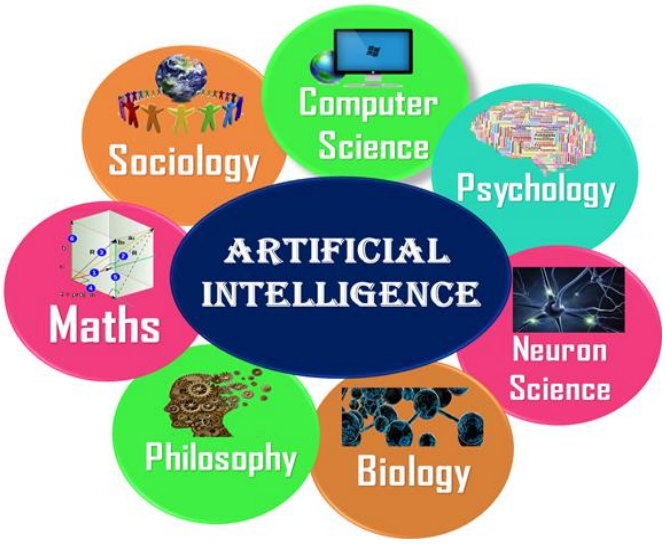


Fig.1.artificial intelligence

AI is a combination of two words artificial and intelligence, where artificial defines "human-made", and intelligence defines "assuming power", hence AI means "a human-made assuming power ".

Before grabbing information about artificial intelligence, we should know that what is the importance of AI and why should we learn and make it a resource to overcome our problems

Definition : It refers to software functions that replace human intelligence in the performance of certain works. it is truly a wonderful topic in computer science set to become a strong foundation of all the latest software over the upcoming periods and quadrants. **[4]** Artificial intelligence, the skill of an electronic computer or system-controlled robot to execute tasks that are generated by human intelligence and process the project by developing the characteristics of human beings.

These are some reasons to learn about AI : With the help of AI, you can create such software or device which can solve real-world problems very easily and gives accurate solutions in no time such as health issues, marketing, traffic issues, google typing, auto-correction, etc.**,[3]** you can create your personal assistant, such as Google Assistant, Siri, Alexa, etc. AI opens a way for other new technologies, new software devices, Similar to human intelligence, gives exact news related to real-world problems

Goals of AI

Replicate human intelligence, solve knowledge intensive tasks an intelligent connection of perception and action , creating some system which can exhibit intelligent behaviour , learn new things by itself ,demonstrate , explain ,and can advise to its user .

There are some of the advantages

High accuracy with errors:-AI machines or systems are prone to less errors and high accuracy as it takes decisions as per pre-experience information

High speed :-AI system can be of very high-speed and fast-decision making , because of that**[5]** AI systems can beat a chess champion in the chess game

High reliability:- AI machines can be highly reliable and can perform the same action multiple time with high accuracy and also useful for risky areas ,digital assistant, useful as a public utility.

APPLICATIONS OF ARTIFICIAL INTELLIGENCE

Artificial intelligence can modify various aspects of healthcare. It decreases annual expenses, in case of any diseases, it detects early and suggests the proper way to get rid of it.

Artificial intelligence can help patients in many ways if, in case of any disease which couldn't identify by doctors, it will recognize early before the doctors.**[5]** Also, that helps doctors, administrators, staff members such as maintaining records of patients, consulting patients, general check-ups, etc.

Fig 2. Artificial Intelligence

a. Medical records: -

Every two years, the amount of available data in the world doubles. So the workload will be more, also it requires more staff members to do different works with highly qualified medical personals for the organization to maintain such records. fortunately, this **[8]**AI is doing wonderful job in spite of humans to overcome from this problem.

b. clinical decision making: -

It helps in the decision of cost for the particular treatment and tells the patients before get admitted.**[10]** And also it decides that what exact treatment should be guided in preferences to the patients.

c.AI powered health assistants

instead of bugging information about symptoms that a person is suffering from you can ask virtual assistants which is powered by **[11]** AI will be available 24/7 whenever you want to know you can ask as many questions as you can it gives proper information instead of coming and waiting to get an appointment, you can sit at home and take appointment from particular doctors from particular location.

Robots and Artificial Intelligence

The feature of AI is one of the interesting and promising technology in the field of robotics. which helps in hospitality, traveling, hotel industries.**[13]** It mimics the human's intelligence and performs tasks. Some tasks are autonomous and some are semi-autonomous. *examples from around the world.*

When discussing robots and their uses, it is important to first establish what they actually are. In simple terms, a robot is a machine, which has been built to carry out complex actions or tasks automatically. Some robots are designed to resemble humans and these are called androids, but many robots do not take such a form.

Modern robots can be either autonomous or semi-autonomous and may make use of artificial intelligence (AI) and speech recognition technology. With that being said, most robots are programmed to perform specific tasks with great precision, with an example being the industrial robots seen in factories or production lines.

Robots and Artificial Intelligence

The use of artificial intelligence within the field of robotics is one of the most exciting and promising applications for individuals and businesses operating within the hotel or hospitality industry. Nevertheless, this is another complex area, where a clearer understanding is necessary.

Essentially, artificial intelligence refers to the performance of seemingly intelligent tasks, which mimic human cognitive functions. Although there is no precise definition of what constitutes artificial intelligence, problem solving, reasoning, understanding human speech and autonomous navigation are typically viewed as examples of AI.
Therefore, references to artificially intelligent robots will usually be describing robots that have been designed to be able to achieve some of these *'intelligent'* tasks or functions.

10. Robots in the Hospitality Industry

Part of the reason why robots have emerged as a popular technology trend within the hospitality industry is because ideas of automation and self-service are playing an increasingly vital role in

the customer experience. The use of robots can lead to improvements in terms of speed, cost-effectiveness and even accuracy.

For example, chatbots allow a hotel or travel company to provide 24/7 support through online chat or instant messaging services, even when staff would be unavailable, delivering extremely swift response times. Meanwhile, a robot used during the check-in process can speed up the entire process, reducing congestion.

Examples of the Use of Robots within the hospitality industry

Below, you will find a list of eight current uses of robots within the hospitality industry.

a. A Tour of the World's First Robot-Staffed Hotel

Situated in Nagasaki, Japan, Henn-na Hotel became the first hotel in the world to be entirely staffed by robots. Throughout the hotel, robots are deployed to provide information, front desk services, storage services, as well as check in and check out services, with technology including voice and facial recognition.

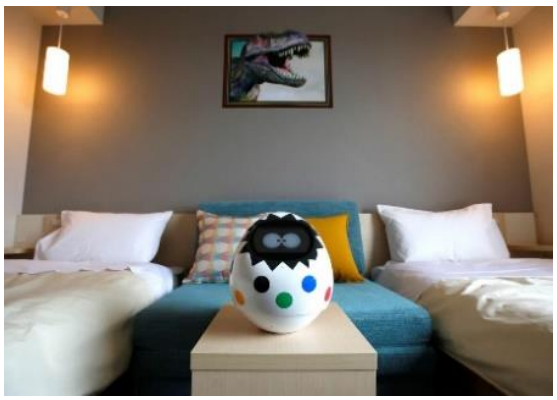


Fig.3.artificial intelligence

Fig.4.artificial intelligence

b. Meet Connie, the Hilton Robot Concierge

Connie is a robot concierge, used by Hilton. The robot makes use of an artificial intelligence platform developed by IBM, and is able to interact with guests and respond to their questions, thanks to its speech recognition capabilities. The system also learns and adapts with each interaction, improving the answers it provides.

Fig.6.artificial intelligence

c. A Robot Suitcase Called Travel mate

Away from the hotel industry, Travel mate is an example of robotics being used for luggage purposes. Essentially, it is an autonomous suitcase, which is able to follow you on its own. It makes use of anti-collision technology, has 360 degree turning capabilities and eliminates the need for carrying, pulling or pushing a suitcase around.

Fig.5.artificial intelligence

d. A Robot Assistant for Airports and Hotels

Airports and hotels are increasingly making use of robotic assistants, transforming the entire hospitality industry. These assistants are capable of carrying out various tasks, including room service and information provision. A key advantage is the ability for robots to offer support for a variety of different languages.

e. A Robot for Travel Agencies

Some travel agents are also looking into the use of robots, especially as a means of pre-qualifying customers. For example, Amadeus have experimented with a robot called 1A-TA, which is powered by artificial intelligence. Rather than forcing customers to wait during busy periods, the robot is able to immediately get to work, finding out about their needs and preferences and passing the information on when they actually speak to a human travel agent.

e. A Chatbot to Make Your Flight or Hotel Booking

To date, chatbots have been one of the most common uses of robots within the hospitality sector and these can be used to deliver basic customer service, or for more complex tasks, like hotel or flight bookings. A great example of this is the SnatchBot Booking Travel Template, which intelligently guides customers through the booking process.

f. Security Robots for Airports

Airport security is one of the most important areas where new technology is deployed and robots are in use here too. One particularly strong example of this is the Knightscope robots that are increasingly being used to autonomously detect concealed weapons, helping to keep passengers safe during their flights.

Fig.7.artificial intelligence

g.More Examples of Robots in the Hospitality Industry

There are a number of additional uses for robots, especially within the hotel industry. For instance, as the following video will show, there are examples of robot butlers and robot luggage porters, which make use of a variety of technologies, including collision detection, Wi-Fi and AI, in order to navigate hotels and provide services.

II. REFERENCES

[1]. https://www.javatpoint.com
[2]. https://becominghuman.ai
[3]. http://www.internetsociety.org
[4]. www.cigionline.org
[5]. www.thersa.org
[6]. www.theconversation.com
[7]. Rreferred by google photos
[8]. https://disruptionhub.com
[9]. https://becominghuman.ai
[10]. refered by https://www.revfine.com
[11]. referred by google photos
[12]. https://www.aldersonloop.com/ai-vs-ml/

Cite this article as : Nayana S Shankar, Mahalakshmi, Dr. Kavitha, "Artificial Intelligence and Its Review", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 50-54, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT19479

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Case Study on Block Chain for Current Era

V. Prushotam, Vibha. B. G, Dr. Kavitha

Department of Computer Applications, Dayananda Sagar College of Arts Science & commerce, Bangalore, Karnataka, India

ABSTRACT

In the current era blockchain is new technology used to record transaction between two parties. It is a public ledger in which everyone is able to have access without central authority having control. This technology is very much essential for the finance sector, banking sector, government sector. In our research we have focused on the applications of the block chain, what all are the major technology used in the bockchain and comparative study on the various technology used in blockchain. The blockchain technology is 30% used in banking and finance sector,13% for government and public goods,8% for media and music.

Keywords : Blockchain,

I. INTRODUCTION

Blockchain is the main technology for the digital cryptocurrency bitcoin. It is a distributed database which records all the transaction that has been done and shared among two parties. Each block in block chain contains a single transaction of amount between the two parties. Bitcoin is the most popular cryptocurrency an example is blockchain. The first existence of blockchain came in to when "a group of people named SantoshiNakamoto first time published about the bitcoin". This was the first time when blockchain came into existence. This technology is used to record all the transaction in the format of digital ledger which is distributed all over the world by the networks. We can record any transaction what we did for ex, from buying of assets till paying money to the seller. The most important use of blockchain is the bitcoin. It is a cryptocurrency which is used to do all the transaction online. In this paper we are going to study about what is block chain, what all are the places where blockchain is used, what all technology involved in the block chain, comparison of blockchain technology. At last we will summarise This paper and elaborate upon future trends in this research field.

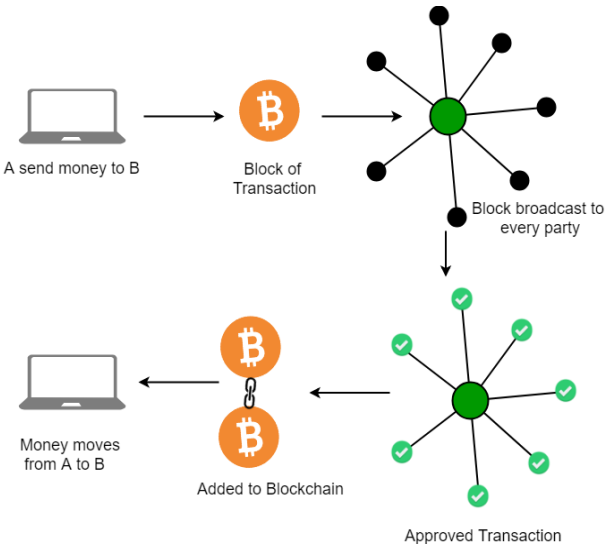


Fig 1.Blockchain Transaction

II. DEFINATION OF BLOCK CHAIN

A blockchain is a growing list of records that are increasing day by day. Every blockchain contains blocks. Each block contains a single transaction that is done by the two parties and it also contains a cryptographic hash of the previous block, and a timestamp. Once the transaction between the two

parties is recorded then it is difficult to alter. This is why blockchains are considered as secure design.

This blockchain was firstly invented by a group of people using the name of sasntoshinakamoto in 2008 to serve the public transaction through the use of cryptocurrencies (bit coin). This blockchain also solved the problem of double spending without the need of a trusted authority or central server.

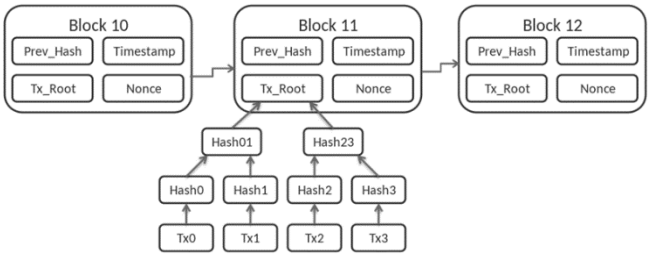


Fig 2. Blockchain diagram

III. MAJOR APPLICATION OF BLOCKCHAIN AND ITS USES

FINANCIAL SERVICES:

Block chain technology in finance:

In financial services blockchains can be used in an efficient way as there are transaction between two parties in the financial service. Financial sector activities ranges from backend clearing and settlement, to global capital markets architecture. So in this sector we can introduce digital ledgers system so that what all transaction done between the two parties are secure. This is how we can introduce blockchains in financial services.

Fig. 3. Blockchain Technology in finance

GOVERNEMENT:

In government sector also we can introduce block chain system which is Distributed Ledger Technology (DLT)). If we introduce this system in the government sector we can improve govt services and there will be faster communication between government and the citizen .this system is more efficient and secure for data sharing.

Fig.4. Blockchain technology in government

HEALTHCARE:

In healthcare sector we can introduce block chain system or we can just use Distributed Ledger Technology (DLT)) to record the patients transaction. Which patents are coming at what time and how much they are spending. We can record all these transaction through DLT ledger system. In now days we use pen paper to record the transaction instead we can use DLT ledger system so that the data is more secure and efficient.

INSURANCE:

In insurance sector we can use block chains to record the data between two parties. If we use block chain system then we can overcome from the problem of data sharing, data security which comes in recording the transaction through pen and paper. This is why nowadays many are changing to Distributed Ledger Technology (DLT).

Fig.5.Blockchain technology in healthcare

MONEY

In transferring of money between two parties the block chain technology is used. Block chains are more secure to use. And blockchains also provide a permanent record for the transaction that has been done between two parties. We cannot delete the transaction what is done. This system shows that how secure is the blockchain technology is. If we transfer the money through bank then there will be 3 parties involved in the transaction. This system involves peer to peer transaction means person to person. In this system only 2 parties are involved. This is why this technology is more secure and safe.

Fig.6.Blockchain technology in money

IV. BLOCKCHAIN ALGORITHM

Blockchain is growing rapidly and it is collections of records linked to the powerful cryptography. Cryptography has written code that will require which has authorized decoding and encryption. Cryptocurrency uses cryptography for security reasons and to record transaction using blockchain technology which is discussed further. Adding the collections of records for validation of transaction is completely referred to as a blockchain algorithm.

TYPES OF BLOCKCHAIN ALGORITHM

From the introduction of blockchain and bitcoin and cryptocurrency in 2009 by Satoshi Nakamoto, many other algorithms have been accepted. Several such algorithms are continuously developed which also has main aim for solving the errors in the already existing algorithms such has PoW. Both Proof of Work and Proof of Stake are both present in consensus algorithm. They all the nodes of blockchain to and prevent from double spending, it also prevents from an attack which always attempts to spend the same coin repeatedly.

CONSENSUS ALGORITHMS

The introduction to blockchain bought the acceptance of consensus algorithms; even several more algorithmshave been accepted. These algorithms are very complex but it assists when the coins are purchased or while a node is running. It achieves the constant growth which contains multiple nodes, and also it makes sure all nodes are proper to the said rule or action.

Nodes tell the consensus is a bitcoin, but not the minors. Consensus is always told as chain with most of the work. Nodes present in consensus accept the transactions, blocks with validations, blocks replication, block serving, last but not least storage of blockchain. Nodes also define PoW(Proof of Work) algorithms that has been employed by minors.

COMPARISON OF THE FIVE CONSENSUS ALGORITHMS

characteristics	consensus algorithms				
	PoW	*PoS*	*DPoS*	*PBFT*	*RAFT*
Byzantine fault tolerance	50%	50%	50%	33%	N/A
crash fault tolerance	50%	50%	50%	33%	50%
verification speed	>100s	<100s	<100s	<10s	<10s
throughput(TPS)	<100	<1000	<1000	<2000	>10k
scalability	strong	strong	strong	weak	weak

Fig.8.Comparison of five consensus algorithms

MINING ALGORITHM

In mining algorithm the data mining has three main components they are

- Clustering or Classification
- Association rules
- Sequence analysis
- Clustering or Classification: It is examination of a group of data and also to generate a group of grouping rules which is used to keep the order of future data.
- Association Rules: It is a rule which has a specific alliance relationship between the group of objects in database.
- Sequence Analysis: It is the complete analysis of patterns that will come in sequence.

There are many more of such algorithms which has given the ides to implement like those aspects in data mining.

In blockchain, the data miners use their computer to repeatedly and also to guess the answers to the puzzle among a group until one of them in the group wins. More importantly the data miners use the blocks unique header metadata using a hash function in it which will also return a secure length of random string numbers, it uses the hash value to modify the nonce value in the data.

If a miner recognizes the hash functions that has the similarities of that of the target then the miner will be rewarded in cryptocurrency and also the blocks will be emitted across the networks for each of the nodes to also validate and add their own ledger copy. If miner B finds the hash before minor A, minor A will stop its process and process the remaining blocks.

V. TRACEBILITY CHAIN ALGORITMS

Traceability demonstrates the origin & practices the transaction when it is collecting extra information to improve the internal performance process and activity of each node in the supply chain. The major aim in traceability chain algorithms is to grab the decisions quickly and in speed. Accordingly, such as operation which produces the irrelevant information problems and it also optimizes the traceability in blockchain poorly. The AI(artificial intelligence) of a mining blockchain algorithm, it runs more faster than consensus algorithms because of inference mechanism.

Nowadays the companies are not able to trace items repeatedly because of data in silos which is corresponding with repetitive points. Using block chain we can repeatedly trace the journey of the transactions. A new approach called Takagi Sugeno Fuzzy cognitive maps applies this traceability chain algorithm. Biased functions for optimized decision compute are described as the participant node constraint method. Thus definition succeeds in meeting the less mining efforts when the traceability chain is process in done.

To grow a fully traceability system, there should be motion of a transactions on the blockchain, giving the each item that will link to the transactions a virtual identity. For that objects have to be linked with all sensors that will store data about items and transfers them to a particular platform. For ex: QR codes, RFID, or wireless sensor networks. A traceability algorithm consists of three main sub-processes:

1. Identifying and naming of products to facilitate the product name.

2. Data capturing and recording: Scans the capacity with electronic data flow to optimise retrieval of information.
3. Linkage & communication is needed to optimize the information sharing which happens between supply chain partners and protocols.

The cooperation between the traditional traceability tools and blockchain guarantees monitoring of transaction without any interruptions the supply chain acts as a major shield against markets performing poorly.

VI. WHAT ALL TECHNOLOGIES USED IN THE BLOCK CHAIN

The basic and most important technologies used in blockchain are:

- Decentralisation
- Tranparency
- Immutability

DECENTRAILISATION:

Earlier centrailized services were more used commonly used. But in now days tradition hass changed a lot. With the brought up of the new technology bitcoins and the bittorrents technology has changed a lot. Earlier in centralised system we used to depend a lot on a particular entity for example earlier if we want to send money to someone we used to depend on t he entity named bank if we want to transfer money . If bank is not there then we cant do the transaction part in the centralised system. But in these days trend has changed .bit coins and bit torrents are the example of the decentralised system. In decentralised system what we do is that we don't depend on any type of entity so the transaction is in the very easy manner.

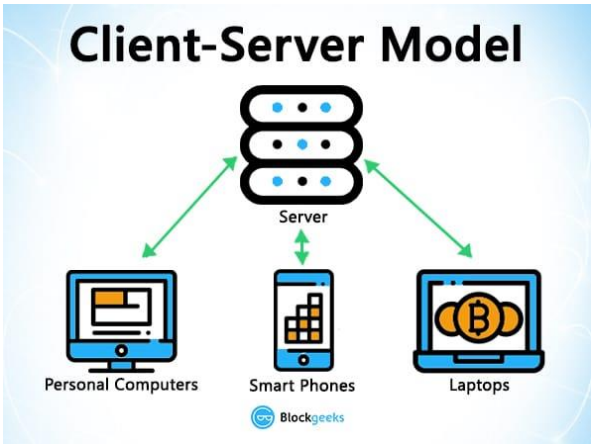


Fig.9.Client-Server Model

TRANSPERECY:

In blockchain the most important and misunderstood concept is its transparency. Most of the people think that transparency means hidden or privacy from the public or transparent…? What do you think so?

So lets understand the concept of the tranperency in the blockchain . In blockchain with the help of transperecy technology we can hide certain information from the public while doing the transaction it will not show the name of the person instead it will show the public address . foreg "Bob sent 1 BTC" instead you will see "1MF1bhsFLkBzzz9vpFYEmvwT2TbyCt7NZJ sent 1 BTC".

In blcokchain with the help of the transperecy technology people cant do fraud while doing the transaction. If we give the public address in the internet then it will show the full transaction that has been done by the party. For eg if there is a company and customers buy clothes from the compay for egflipkart if flipkart starts using this technology then the company can't do fraud in these. we can catch the company if company does fraud transaction.

This way we can maintain proper transaction records.

Fig.10.Transaction record

IMMUTABILITY:

This is the very most and valuable cocept used in the blockchain system. This technology is used in the digital transaction that are done by the 2 persons. In these the transaction that are entered once cant be changed this is the main feature of this technology . So if we start using this technology then we don't have to fiddle around with the company accounts and there will be no misuse of the transaction record details that are: deleting some of the transaction earlier people used to do it.

This technology uses a cryptographic hash function or hashing algorithm know as SHA-256.

INPUT	HASH
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome to blockgeeks. Glad to have you here.	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Fig.11.Cryptography

VII. COMPARISION OF TECHNOLOGY USED IN BLOCKCHAIN

BITCOIN:

This was the first and the earliest product of the block chain which used the system of decentralisation in the transactions that were done between 2 people. Bitcoin is a public type blockchain where anyone in invited to join. The main components that are used in the bitcoin mechanism are as follows cryptographic hash function, digital signature, private-and-public key encryption, peer-to-peer (P2P) network, and proof of work (POW) consensus algorithm.

This technology allows people to do non reversible transactions without having the use of the third party. A single transaction contains a unique transaction ID, input bitcoin address, the number of bitcoins to be transferred and the output bitcoin address of the recipient. In this technology every node has the complete information about the blockchain so this makes this decentralised one .

ETEHEREUM

Ethereum is different from bitcoin; it is built for allowing the transactions of crypto payment on a decentralized network. Ethereum was designed which has much larger aim in their mind. The developers can launch their own block chain projects which include their own cryptocurrencies the platform has been provided. The platform which is used to launch their projects commonly is called as Ethereum Virtual Machine (EVM) which has been used to launch over thousands and thousands of DApps. Using EVM many famous cryptocurrency projects which is VeChain and OmiseGo has been launched. Smart contracts like this make it possible.

These are the pieces of code, which will allow the execution of legal function such as taking control of an entity based on particular conditions, and based on fulfilling the required conditions the transferring crypto token is done.Ethereum proprietary language Solidity uses smart contracts on the Ethereum platform, which is motivated by C++ language, Java, Python and JavaScript languages. It also gives access to a way for the user to tell how much of computing power can be extended for a transaction, which uses to measure the processing power which is also called 'Gas'. The gas limit is specified by the user. The execution of a transaction is done which remains within a limit, like wise, the changes are made when it exceeds the limit. The requirement of the gas is less when it is simple payment transaction, if it is more complex operations for ex: deployment of smart contracts requires more gas.

RIPPLE PROTOCOL

It uses most of the features of Bitcoin/Ethereum which is decentralized design and cryptographic hash functions and P2P network, and private public key encryption. The Ripple Protocol was specifically designed to facilitate rapidly and less of global transfer of money, which gives so many unique features in each one.

RPCA happens in 5 rounds and they are:

- At first each server takes all valid and also unapplied transactions and makes a list, public in the form of a candidate set.
- Each and every server has one unique node list (UNL), where the other entire server queried by this server is listed.
- Each and every server takes all candidate sets of entire servers in its unique node list and together makes a mixed list, before voting on the unique node list.
- Transactions thathave been received larger than the threshold of 'yes' votes then it is taken to next round, and the others votes are discarded/moved to the candidate list for next round.
- The final round always requires an average of 80% of the servers on a server's unique node list to be considered on the transaction and before being applied to the ledger.

  After applying to the ledger all the accepted transactions in the ledger, the ledger is will be closed, and it is named as new last closed ledger.

VIII. CONCLUSION

Hence we conclude that it is very useful to understand the concept of the blockchain in these days. Earlier people used to think that all blockchain mechanisms uses the bitcoin technology but it is not true. These days many new technology came which uses the system of Blockchain like pow, longest chain rule,etc. bitcoins were the first to maintain decentralised, public ledger with no formal control or government. These blockchain system will now solve the problem of pen paper ledgers which were earlier used. This technology also has lots of pros and cons.

IX. REFERENCES

[1]. Introduction-https://www.google.com/amp/s/www.geeksforgeeks.org/blockchain-technology-introduction/amp/
[2]. definition of block chain:https://en.m.wikipedia.org/wiki/Blockchain
[3]. major application of block and its use:https://www.blockchaintechnologies.com/applications/
[4]. blockchain algorithms: https://blog.goodaudience.com/a-simple-introduction-to-blockchain-algorithms-ca05b9bcc32f
[5]. what all technologies used in the blockchain:https://blockgeeks.com/guides/what-is-blockchain-technology/
[6]. comparision of technologies used in blockchain:https://medium.com/edchain/a-comparison-between-5-major-blockchain-protocolsb8a6a46f8b1f

Cite this article as :

V. Prushotam, Vibha. B. G, Dr. Kavitha, "Case Study on Block Chain for Current Era", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 55-61, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194710

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Comparative Study on Natural Language Processing

Lakshya Muralidhara, Ashwini Patil, Greeshma Murthy, Dr. S. Kavitha
Dayananda Sagar College of Art Science and Commerce, Bangalore, Karnataka, India

ABSTRACT

Natural language processing (NLP) is a branch of that helps computers understand, interpret and manipulate human language. NLP draws from many disciplines, including computer science and computational linguistics, in its quest to fill the gap between human communication and computer understanding. Many organizations use NLP techniques to optimize customer support, improves the efficiency of text analytics by easily finding the information they need, and enhance social media monitoring. For example, banks might implement NLP algorithms to optimize customer support; a large consumer products brand might combine natural language processing and semantic analysis to improve their knowledge management strategies and social media monitoring.

Keywords : Artificial Intelligence, Machine Learning, Linguistic, Ambiguous, Semantics

I. INTRODUCTION

Natural language processing (NLP) is the capability of a computer program to understand human language as it is spoken. NLP is a component of artificial intelligence (AI). The history of NLP generally started in the 1950's, although works can be found from the earlier periods. In 1950 Alan Turing published an article titled "COMPUTING MACH IN ERY A N D IN TE LL IGEN CE" , which is at present called the "TURING TEST" as a criterion of intelligence. . Starting in the late 1980s, however, there was a revolution in natural language processing with the introduction of machine learning algorithms for language processing Some of the earliest-used machine learning algorithms, such as decision trees, produced systems of hard if-then rules similar to existing hand-written rules. However, part-of-speech tagging introduced the use of hidden Markov models to natural language processing, and increasingly, research has focused on statistical models, which make soft, probabilistic decisions based on attaching real- valued weights to the features making up the input data. Some of the recent algorithms for Natural Language Processing Some of the recent algorithms for Natural Language Processing are (WOS) WORD SENSE DISAMBIGUATION TECHNIQUE, MACHINE TRANSLATION, SPEECH TAGGING AND RECOGNITION, and GENERATION OF NATURAL LANGUAGE.

Natural Language Processing is the driving force behind the following common applications: Google Translate, Word Processors such as Microsoft Word and Grammarly (to check grammatical accuracy), Interactive Voice Response (IVR) , Personal assistant applications such as OK Google, Siri, Cortana, and Alexa.

Here are some tools available for NLP: CoreNLP, NLTK, TextBlob, Gensim, spaCy.

There are three different levels of linguistic analysis done before performing NLP:

- ✓ Syntax – What part of given text is grammatically true.
- ✓ Semantics – What is the meaning of given text?
- ✓ Pragmatics – What is the purpose of the text?

NLP deal with different aspects of language such as: Phonology, Morphology.

Approaches of NLP for understanding semantic analysis:

- ✓ Distributional – It employs large-scale statistical tactics of Machine Learning and Deep Learning.
- ✓ Frame – Based – The sentences which are syntactically different but semantically same are represented inside data structure (frame) for the stereotyped situation.
- ✓ Theoretical – This approach is based on the idea
- ✓ that sentences refer to the real word (the sky is blue) and parts of the sentence can be combined to represent whole meaning.
- ✓ Interactive Learning – It involves pragmatic approach and user is responsible for teaching the computer to learn the language step by step in an interactive learning environment. The true success of NLP lies in the fact that humans deceive into believing that they are talking to humans instead of computers.

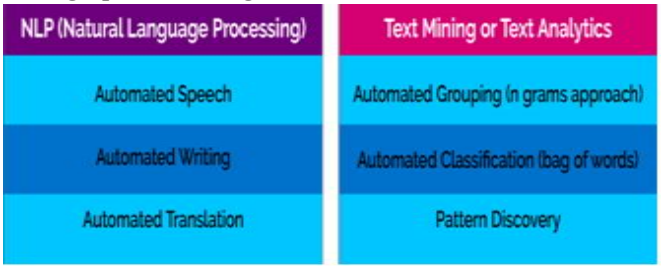
STEPS FOR NATURAL LANGUAGE PROCESSING

The user needs to import a file containing text written and then perform the following steps for natural language processing.

- ✓ Sentence segmentation – It identifies the start and end points of a given sentence. Usually start of a sentence uses capital letters or bullets or numbering whereas end of a sentence contains punctuation marks like '.' or '?'
- ✓ Tokenization – It recognizes words, numbers, and other punctuation marks and symbols.
- ✓ Stemming – It casts off the ending of the words.
- ✓ For example 'drinking' or 'drunk' is reduced to 'drink'.
- ✓ Part of speech (POS) tagging – It designates each sentence its part of speech tag such as assigning given word as adjective or verb or pronoun etc.
- ✓ Parsing – It is used to divide a given text into different categories. For example the first category can be to answer the part of a sentence and second category to modify another part of the sentence.
- ✓ Named Entity Recognition – It recognizes the entities or units such as people, place and time within the given document.
- ✓ Co-Reference resolution – It describes the relationship between the given word in a sentence with the preceding and the succeeding sentences with reference to the given word.

DIFFERENCE BETWEEN NLP AND TEXT MINING OR TEXT ANALYTICS

Natural language processing is responsible for understanding meaning and structure of given text. Text Mining or Text Analytics is a process of extracting hidden information inside text data through pattern recognition



SOME KEY APPLICATION AREAS OF NLP

NLP has many other applications besides Big Data, Log Mining, Deep learning and Log Analysis. Despite of the fact that the term 'NLP' is not as popular as 'big data' 'machine learning' or 'artificial intelligence,' it's used very commonly on a day to day basis. Some of the other applications of NLP are:-

Automatic summarizer – When an input text is given, this gives us the summary by removing irrelevant points

Sentimental analysis – When an input is given, it analyses the given text to predict the tone of the text For example - whether the text conveys judgment, opinion, order, review or question.

Text classification – It is implemented to classify different journals, news stories according to their element. Multi-document classification is also possible. A popular example of text classification is spam detection in emails. This property can be used to detect the name of the author of the given journal based on the writing style.

Information Extraction – The process to extract specific information. One of the most common examples is when email extracts only from your messages and automatically adds the events to the calendar.

STUDY OF SOME OF THE RECENT NATURAL LANGUAGE PROCESSING ALGORITHMS

Machinery Translation Technique

Machine translation is the process of converting one natural language into another by preserving the meaning and producing a meaningful and fluent output. Machine Transition Techniques are based on different models:

1. Bilingual machine translation: A bilingual machine translation system is translates just a pair of languages and cannot be adapted to other languages.
2. Transfer-based machine translation: This translation model is based on three modules: Analysis module, Transfer module, Generation module.
3. Interlingual-based machine translation: This translation model is based on two main modules: Analysis module, Generation module
4. Memory-based machine translation: This translation model is based on the "translation memory." It is a corpus-based approach. The system just re-uses translations previously stored by the professional translator without really analyzing the source text and a dictionary (terminology support) is used to help the expert to translate the parts of texts that haven't been previously translated. This "new" translation concept frees the professional translator to attend to the finer points of translation that require the judgment of an expert by offering a computer-assisted translation that automates repetitive tasks.
5. Statistical-based machine translation: This translation is a corpus-based approach. Statistical concepts are among the first techniques for machine translation. A few examples of Machine Translation techniques are

1. Word Alignment: - Word alignment is a primary crisis in statistical machine translation. The core of the task is to identify relations between words or phrase of two sentences articulated in different languages.
2. Data Matching: - Data matching, or in other words record linking, is the process of finding the matching pieces of information in large sets of data. The purpose can be to find entries that are related to the same subject or to detect duplicates in the database.

The main issues of Machine Translation are disambiguation, non-standard speech and named entities

II. MORPHOLOGICAL SPLITTING TECHNIQUE

Split Morphology is a hypothesis which requires definite information on the Derivation and Inflection that has separate components of grammar. Whereas Derivations are mostly handled by lexical rules and Inflections are handled by syntactic rules.

WORD SENSE DISAMBIGUATION

Word sense disambiguation is a concept where a word used any times in a particular context is given an appropriate or "sense" (meaning) to the corresponding sentence which is largely unaware in people. The feature of this context provides the evidences for classification. The research on this point has always been consistent on giving exact or precise results without any doubt. They researched a variety of techniques by using dictionary based methods and also the knowledge which was encoded in lexical recourses

to supervise machine learning methods providing a collection of manually sense – annotated examples. The research of unsupervised methods has also provided cluster of repeated words including word sense. But among all these learning approaches, supervised learning approach has been considered successful algorithm.

Applications are: WSD applications of language are used in technology, information retrieval,

lexicography, knowledge mining/acquisition and semantic interpretation, bioinformatics and the Semantic Web.

III. TAGGING AND RECOGNITION

POS tagging is the process of marking up a word in a body to a corresponding part of a speech tag, based on its context and definition. Part of Speech (hereby referred to as POS) Tags are useful for building parse trees, which are used in building NER's. POS Tagging is also essential for building lemmatizers which are used to reduce a word to its root form. Different types of POS Taggings are:

1. Lexical Based Method
2. Rule-BasedMethods
3. Probabilistic Methods
4. Deep Learning Methods

Speech recognition is the ability to recognize the spoken words by a electonic device. A microphone records a person's voice and the hardware converts the signal from analog sound waves to digital audio.The audio data is then processed by software, which interprets the sound as individual words.

GENERATION OF NATURAL LANGUAGE

Generative Adversarial Networks (GANs) have gathered a lot of attention from the computer vision community, yielding impressive results for image generation. Advances in the adversarial generation of natural language from noise however are not in proportion with the progress made in generating images, and still lag far behind likelihood based methods. In this paper, we take a step towards generating natural language with a GAN objective alone. We present quantitative results on generating sentences from context-free and probabilistic context-free grammars, and qualitative language modeling results.

Benefits of NLP

NLP hosts benefits such as:

- ✓ Enhanced accuracy and efficiency of documentation.
- ✓ Automatic summarizer
- ✓ Useful for personal assistants such as Alexa.
- ✓ Allows an organization to use chatbots for customer support.
- ✓ Permits sentimental analysis.

Challenges associated with NLP

NLP has not yet been wholly perfected. For example, semantic analysis can still be a challenge for NLP. Other difficulties include the fact that abstract use of language is typically tricky for programs to understand. For instance, NLP does not pick up sarcasm easily. These topics usually require the understanding of the words being used and the context in which the way they are being used. As another example, a sentence can change meaning depending on which word the speaker puts stress on. NLP is also challenged by the fact that language, and the way people use it, is continually changing.

IV. CONCLUSION

NLP provides a wide set of techniques and tools which can be applied in all the areas of life, by learning and

using the same in our everyday interactions, our life quality would highly improve. NLP techniques help us improving our communications, our goal reaching and the outcomes we receive from every interaction. They also allow us to overcome personal obstacles and psychological problems. NLP helps us by utilizing the tools and techniques we already have with us without being aware of it. NLP supposedly makes the job easier but still demands a human interference. People and the industry fear NLP would start a trend of job snatching which is true to a certain sense but it certainly cannot function the way it does without human inputs. The will to work

V. REFERENCES

[1]. https://searchbusinessanalytics-techtarget-com.cdn.ampproject.org/v/s/searchbusinessanalytics.techtarget.com/definition/natural-language-processing-NLP?amp_js_v=a2&amp_gsa=1&amp=1&usqp=mq331AQEKAFwAQ%3D%3D#aoh=15685236195886&referrer=https%3A%2F%2Fwww.google.com&amp_tf=From%20%251%24s&ampshare=https%3A%2F%2Fsearchbusinessanalytics.techtar get.com%2Fdefinition%2Fnatural-language-processing-NLP

[2]. https://ieeexplore.ieee.org/document/1587718/keywords

[3]. https://machinelearningmastery.com/natural-language-processing/

[4]. https://www.upwork.com/hiring/for-clients/artificial-intelligence-and-natural-language-processing-in-big-data/

[5]. https://www.researchgate.net/publication/243962849_Overview_of_machine_translation_techniques

[6]. https://en.m.wikipedia.org/wiki/Machine_translation

[7]. https://towardsdatascience.com/5-heroic- tools-for-natural-language-processing-7f3c1f8fc9f0

Cite this article as :

Lakshya Muralidhara, Ashwini Patil, Greeshma Murthy, Dr. S. Kavitha, "Comparative Study on Natural Language Processing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 62-66, September-October 2019.

Journal URL : http://ijsrcseit.com/CSEIT194711

National Conference on Communication Technology & Network Security In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Movement Simulation and Analysis

Dr. Manjula Prasad[1], Mrs. Sushmitha R[2], Ms. Niveditha P[3], Mr. Nandeesh P B[4]

[1]HOD Department of Computer Science, Sri Krishna Degree College, BSK III Stage, Bangalore, Karnataka, India

[2]Professor, Department of Computer Science, Sri Krishna Degree College, BSK III Stage, Bangalore, Karnataka, India

[3,4]Assistant Professor, Department of Computer Science, Sri Krishna Degree College, BSK III Stage, Bangalore, Karnataka, India

ABSTRACT

Local mining phase finds movement patterns based on the local trajectories. This is derived on the movement patterns and moving object with similar single object or group of object. To address the energy conservation issue in resource-constrained from transmits local grouping results. Mining group movement patterns for tracking moving object efficiently is the tracking with similar movement patterns as found using a single object or group of object. And the mining results to track moving the object efficiently, at the same time data mining algorithm achieves to reduce the energy consumption by reducing the amount of data to be transmitted from one local to another local group mining. The proposed algorithm comprises a local mining phase and a cluster ensemble phase. In the local mining phase, the algorithm finds movement patterns based on local trajectories. Then, based on the derived patterns, we propose a new similarity measure to compute the similarity of moving objects and identify the local group relationships. To address the energy conservation issue in resource-constrained environments, the algorithm only transmits the local grouping results to the sink node for further assembling. In the cluster ensemble phase, our algorithm combines the local grouping results to derive the group relationships from a global view. We further leverage the mining results to track moving objects efficiently. The results of experiments show that the proposed mining algorithm achieves good grouping quality, and the mining technique helps reduce the energy consumption by reducing the amount of data to be transmitted.

I. INTRODUCTION

Data mining is a behavior process to extract useful and interesting knowledge from huge amount of data. The knowledge modes data mining exposed have a variety of different types. The general patterns are: association mode, classification model, class model, sequence pattern and so on. Mining association rubrics is one of the most important aspects in data mining. Association rules are dependency rules which foretell occurrence of an item based on occurrences of other items. It is simple but effective and can help the commercial conclusion making like the storage layout, appending sale and etc. We generally use distributed system as a solution to mining association rules when mass data is being composed and warehoused. With the development of web and distributed techniques, we begin to accumulate databases in distributed systems. Thus studies on the algorithm of mining association rules in distributed system are becoming more

important and have a broad application foreground. Distributed algorithm has behaviors of high adaptability, high flexibility, low wearing performance and tranquil to be connected etc. This algorithm is engineered to improve the existing IT infrastructure and also help to bring into line business objectives with IT strategies.

II. EXISTING SYSTEM

- These applications generate large amounts of location data, and many approaches focus on compiling the collected data to identify the repeating movement patterns of objects of interest.
- We find that discovering their movement patterns of a group of objects is more difficult than finding the patterns of a single object because we need to identify a group of object before or after discovering their movement patterns.
- The object next location we can be predicated based on its preceding locations.
- But now we used to conditional probability distribution, so we get over all of the object location in sequence dataset.
- A smaller group of relationship data's we control the movement of the range.
- A group of objects by using linear distance between the starting points to furthest point to reached.

Drawbacks

- On the other hand, previous works, such as measure, the similarity among these entire trajectory sequences to group moving objects.
- Since objects may be close together in some types of terrain, such as gorges, and widely distributed in less rugged areas, their group relationships are distinct in some areas and vague in others.
- Thus, approaches that perform clustering among entire trajectories may not be able to identify the local group relationships.
- In addition, most of the above works are centralized algorithms which need to collect all data to a server before processing it causes, unnecessary and redundant data may be delivered, leading to much more power consumption because data transmission needs more power than data processing in Wireless Sensor Networks (WSNs).

PROPOSED MODEL

- A distributed mining algorithm identifies a group of objects with similar movements patterns.
- It's used comprises a local mining phase and cluster assembling phase
- Data collect from locally and generates the group of information with GMPMine algorithm.
- CE algorithm comprised of three steps., first collect the similarly coefficient pair of objects. That means presently moving object is present in partial clusters and absent from others.
- Second the coefficient object are same group or different group, is that simple match that coefficient underestimates the object's correlations
- Final step find the normalized mutual information to select the assembling result from the group of objects.
- In network data aggregation in improves the scalability and reduces the long-distance of communication demands and thus saves energy. Therefore, energy conservation is top among all the design issues in WSNs. One important characteristic of WSNs is that sensors are organized close together to ensure complete analysis of the monitored area.

PROBLEM DEFINITION

We find that discovering the movement patterns of a group of objects is more difficult than finding the patterns of a single object because we need to identify a group of entities before or later discovering their movement patterns.

To address these difficulties, we first recommend a mining structure that can classify a group of moving objects and discover their group movement patterns in a distributed manner.

The discovered data is then used in the design of a competent tracking network.

We show that learning and manipulating the movement patterns of a group of objects can further reduce the transmission costs and thereby conserve energy.

In our system we combine local grouping results from sensor clusters with heterogeneous tracking configurations, such as different monitoring intervals, or different network structures of sensor clusters, which can reduce the tracking costs.

For example, as a replacement for of waking up all sensors at the same frequency, a shorter tracking interval is specified for some types of terrain, such as gorges, in the migration season to reduce energy consumption.

Rather than deploying the sensors in the same density, they are only highly concentrated in areas of interest in order to reduce deployment costs.

SYSTEM IMPLEMNTATION

Implementation is the maximum critical stage in achieving a successful system and giving the user's self-confidence that the innovative system is feasible and effective. Implementation of a reformed application to change an existing one. This type of conversation is comparatively easy to handle, provide there are no main changes in the system.

Recent advances in location-acquisition technologies, such as global positioning systems (GPSs) and wireless sensor networks (WSNs), have fostered many novel applications like object tracking, environmental monitoring, and location-dependent service. These applications produce large volumes of location data, and many methods focus on gathering the collected data to identify the repeating movement patterns of objects of interest. In object tracking applications, many regular phenomena display that moving objects often exhibit some degree of regularity in their movements. For example, the prominent annual wildebeest migration demonstrates that the movement of creatures is temporally and spatially correlated. These features indicate that the trajectory data of multiple objects may be correlated.

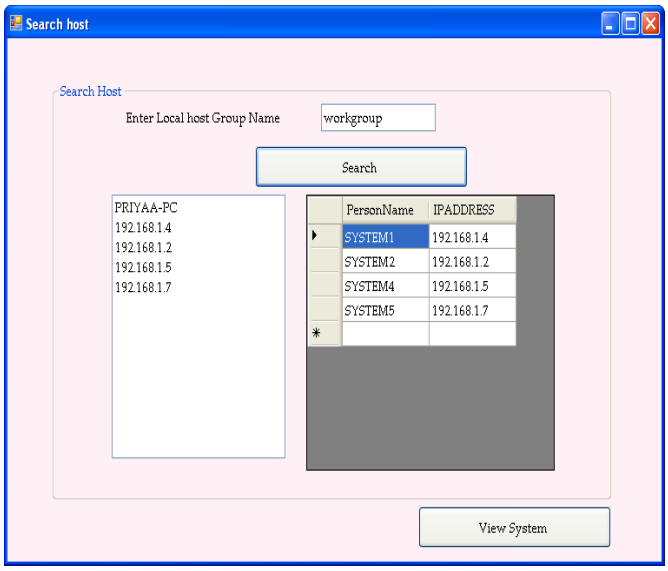
Furthermore, some research areas, such as the study of animals' social behavior and wildlife migration, are more concerned with a group of animals' movement patterns than each entity's. This raises a new task of finding moving animals belonging to the same group and recognizing their aggregated movement patterns. Additional motivation for discovering the group relationships and movement patterns behind the trajectories of moving objects, like monkeys or elephants, is to lessen tracking costs, especially in resource-constrained environments like WSNs. In a WSN, a large number of miniature sensor nodes with sensing, computing, and wireless communication capabilities are organized in isolated areas for various applications, such as environmental monitoring or wildlife tracking. As the sensors are generally battery powered, recharging a large number of them is problematic;

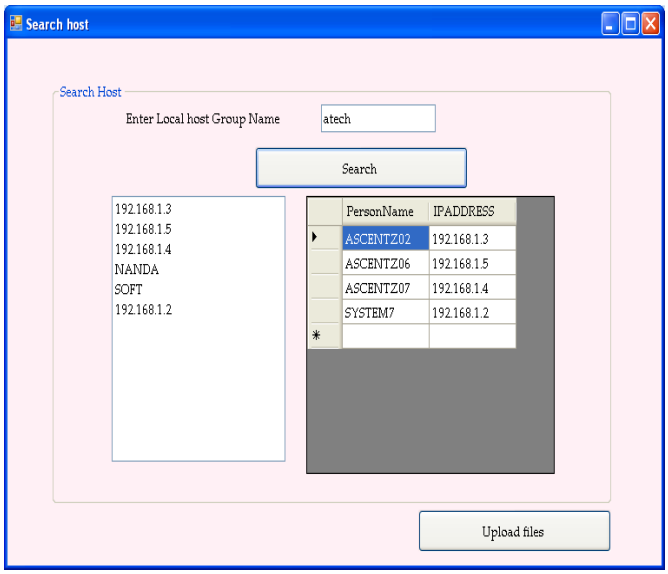
Each program is tried individually at the time of development by means of the data and has verified that this program connected together in the way identified in the programs specification, the computer system and its environment is tested to the fulfillment of the user. The system that has been developed is accepted and proved to be satisfactory for the user. And so the system is going to be implemented very soon. A simple operating procedure is involved so that the user can know the different functions visibly and quickly.

OBJECT MOVING PATTERNS

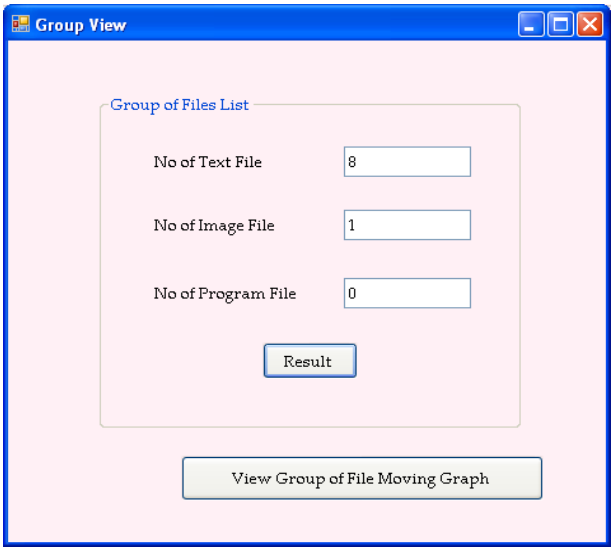
This module analysis the objects where moving from one system to another system. We find the file from group movement mining algorithm. In this algorithm we use to find file, from two types. That is a local mining phase and a cluster phase. In the local mining phase, the algorithm finds movement files based on local path. And cluster finds movement files based on the network systems. A new pair-wise measure based on similarity file to compute the similarity of moving files.

SEARCH HOST





OBJECT TRACKING



This module provides the implementation previous module. That is analysis the moving files on two segment. In this module get the regular sequential files and group of relationship in a distributed way on the detection. The network partitions the trajectories of file searching and moving are “identify the files” from our algorithm. And lastly we discovered the track of moving files efficiently.

GROUPVIEW

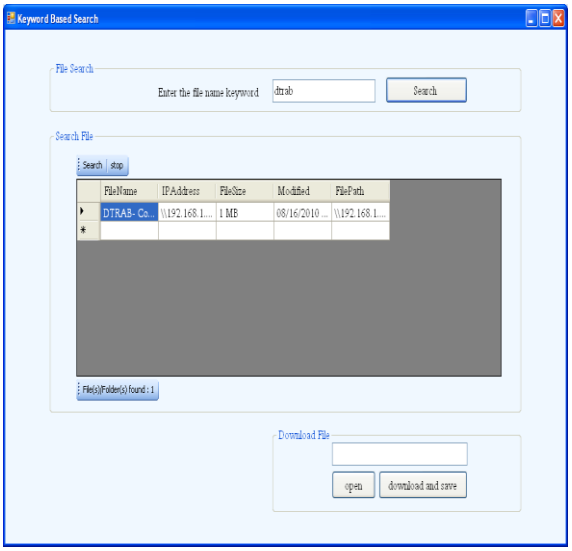
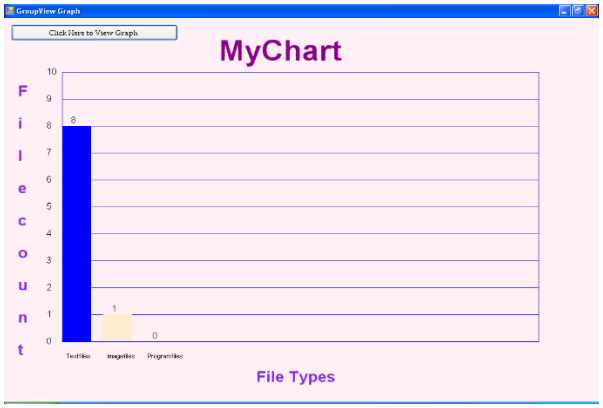
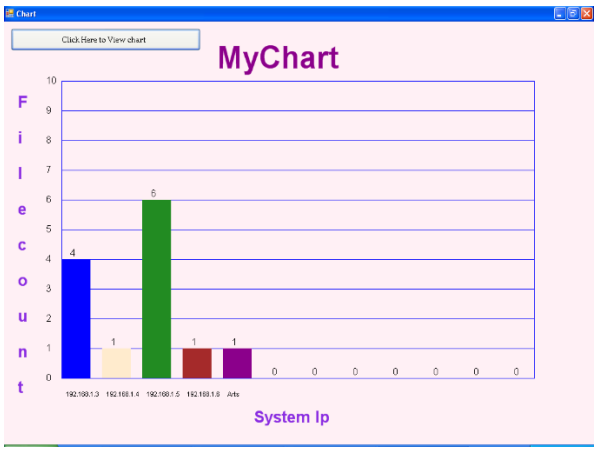


CHART VIEW





III. CONCLUSION

In this work, we exploit the characteristics of group movements to discover the information about groups of moving objects in an OTSN. In contrast to the centralized mining technique, we mine the group information in a distributed manner.

We propose a novel mining algorithm, which consists of a local GMP Mine algorithm and a CE algorithm, to discover group information. Our algorithm mines object movement patterns as well as group information and the estimated group dispersion radius. Other than clustering trajectories, we can apply the distributed clustering approach to heterogeneous and distributed sequential data sets, such as web logs or gene sequence. Using the mined object movement patterns and the group information, we design an energy-efficient OTSN. The contribution of our approach is threefold: 1) it reduces energy consumption by allowing CHs to avoid sending the prediction-hit locations, because the locations can be recovered by the sink via the same prediction model; 2) it leverages group information in data aggregation to eliminate redundant update traffic; and 3) it sets the size of an SG adaptively to limit the amount of flooding traffic.

Our experimental consequences show that the proposed mining technique achieves good grouping quality. Furthermore, the proposed OTSN with PST prediction, group data aggregation, and in-network data aggregation significantly reduces energy consumption in terms of the transmission cost, especially in the case where moving objects have distinct group relationships

IV. FUTURE ENHANCEMENT

These applications produce huge amounts of location data, and numerous approaches focus on compiling the collected data to identify the recapping movement patterns of objects of concentration. The objective is to ease the study of past movements and evaluation future movements, as well as support approximate queries on the original data.

Our experimental outcomes show that the proposed mining technique achieves good grouping quality. Furthermore, the proposed OTSN with PST prediction, group data aggregation, and in-network data aggregation significantly reduces energy consumption in terms of the transmission Cost, exclusively in the case where moving objects have distinct group relationships.

V. REFERENCES

[1]. Bill Hamilton, “Programming SQL Server”, O'Reilly Media Publisher, 2006.

[2]. Elias M.Award,”System Analysis and Design”, Galgotia Publications, Second Edition.

[3]. Daniel Solis, “Illustrated C# 2008”, Apress Publisher, 2008.

[4]. David B. Makofske, Michael J. Donahoo, Kenneth L. Calvert, “TCP/IP Sockets in C#”, Academic Press Publishers, 2004.
[5]. Richard Blum, “C# Network Programming”, John Wiley & Sons Publishers, 2006.
[6]. Robin Dewson, “Pro SQL Server ”, Apress Publisher.
[7]. Roger S. Pressman, ”Software Engineering”, Fourth Edition, 2005.
[8]. R. Agrawal and R. Srikant, “Mining Sequential Patterns” ,Proc.11th Int’l Conf. Data Eng., pp. 3-14, 1995.
[9]. www.dotnetspider.com
[10]. www.programersheaven.com
[11]. www.sql-server-performance.com
[12]. www.developerfusion.com
[13]. www.winsocketdotnetworkprogramming.com

Cite this article as :

Dr. Manjula Prasad, Mrs. Sushmitha R, Ms. Niveditha P, Mr. Nandeesh P B, "Movement Simulation and Analysis", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 67-72, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194712

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

A Self-regulatory Personal Assistant for a Smart Home

Neelima Sahu
Assistant Professor Brindavan College, Dwarkanagar, Bagalur main Road Yelhanka, Bangalore, Karnataka, India

ABSTRACT

In this smart age a speech-triggered interface to manage all electronic house- hold devices for a faraway home owner is a necessity. In a smart home an owner can convey an input in natural language form to a gadget to control one or more electronic home equipment's. The user gadget can transmit the home owner speech to a server to be converted into a textual representation. The server can find one or more command interface components and appropriate commands to be performed by the one or more electronic gadgets based on the textual representation. The command interface component includes several communication ports, each communication port related with a different type of communication interface for providing communications to and from the multiple electronic gadgets. The component also includes a speech network communication port for receiving the spoken commands from the home owner and a data network communication port for transmitting monitoring and control information between the multiple electronic devices and the home owner. In operation, the command interface component is responsive to speech triggered commands received from a remote owner via an incoming telephone line. A speech recognition unit within the command interface module is utilized to translate the received speech signal into an "action/control" signal and then perform the desired activity.

Keywords : Command interface component, speech triggered command, speech recognition unit, home gadgets/appliances

I. INTRODUCTION

If we look 20 years back, we were in the early days of internet. There were no smart phones or flat screen TVs, watching a movie at home means loading a heavy cassette into a VCR. So, what will our world really be like in 20 years in future, the technology we use and the homes we live in will probably be much like it is today, but smarter and more automatic. Today we have come to one more step of evolution. Today all our gadgets at home are intelligent and automatic .So the need of the hour is to control all our electronics gadgets at home with the help of app in our smartphone, So that it will be a great help to us when are away from home.

An app in the smart phone can serve as server, which can be used to open doors for this type of remote communication. The server in app may receive a remote command from the home owner via a computer network or Internet. The server at home may have a display unit which is connected to the status and control of the various electronic gadgets, allowing the home owner to access the status of the home devices.

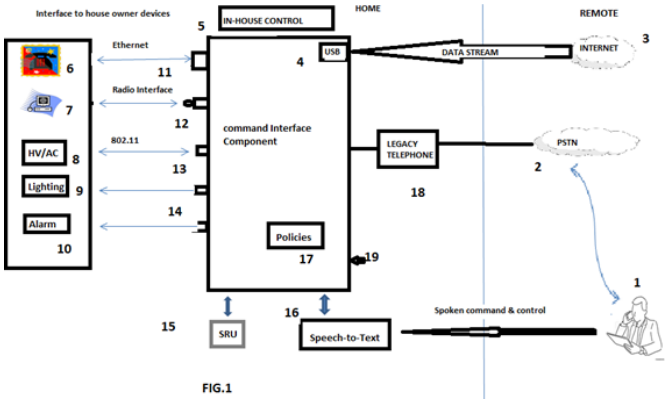


FIG.1

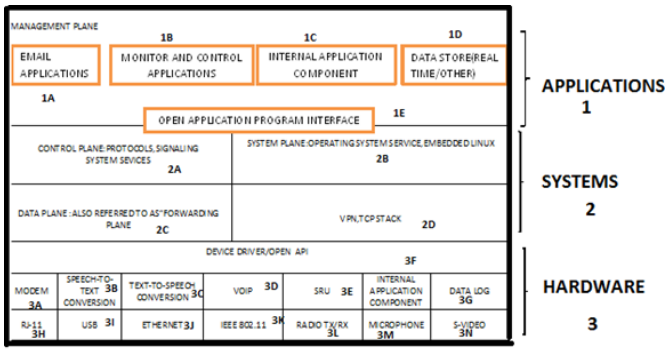


FIG.2

II. SUMMARY OF THE INVENTION

The necessity existing in the previous work can be stated by present invention which describes a system for allowing remote user to keep in touch with various gadgets in his home, more particularly, to the utilization of a single command interface component within the home to provide a communication link between a remote user, his home and other individuals. In the current invention, the command interface component is designed to communicate with several home appliances/gadgets. The command interface component acknowledges the speech commands received from a remote user via an incoming telephone line (either message or speech). A Speech accepting unit within the command interface component is applied to translate the received Voice signal into an action- control signal and then achieving the desired activity.

In addition command interface component also regulates the status like turn certain appliances/gadgets “off” or “on”, adjust settings on gadgets, provide dial tone to remote home owner, etc. A list of customized “user policies', which includes supervision of the devices, are stored in a policy data base within the command interface component. A history log database of past actions may also be stored within the command interface component.

It is a contribution of the current invention that the command interface component functions as an interface between the voice and data communication networks. Suppose, a remote home owner may give a call to home, and demand the command interface component to send an email to an particular person. The command interface component will recognize the command (“email'), the “determined party’ ‘and the Successive (spoken) message. The command interface component would then engage the home owner's computer to create the email message and transmit the message over the Internet.

In addition the current command interface component can supervise the status of several home gadgets /appliances like alarm/security, HV/AC systems etc. and send "commands' to modify one or more of these appliances, as needed. Taking into account that, the various gadget/appliances can be supervised by the voice commands of home owner (through a telephone connection) when interface is stationed between the appliance and the command interface component, even if he is at a remote location. The potentiality of the current invention can be illustrated with help of following figures. FIG. 1 is a block diagram which depicts the utilization of a command interface component in correspondence with the current invention.

FIG. 2 depicts a classic diagram of the several communication levels within a command interface component formed in correspondence with the current invention.

III. DETAILED DESCRIPTION

FIG. 1 depicts, in simplified block diagram form, a unique home arrangement utilizing a command interface component [19] constituted in correspondence with the current invention. A command interface component includes numerous different internal communication ports, an independent port for interacting with one or more home gadgets/appliances, for which monitoring and control is desired. The different communication ports which the current invention includes are Ethernet port [11], a radio communication port [12], an 802.11 port[13], and an alarm port[14] . A pair of external communication ports (USB connection [4]) and (RJ-11 connection) are used to communicate with the external world via a data network [3] and PSTN [2], respectively.

The home appliances/gadgets in connection with command interface component may include a lighting system [9], a home alarm system [10], a telephone [6], a computer [7], HV/AC system control [8], etc. Several different types of

connections may be used to provide the communication link between the communication port and home device. For example, a home computer [7] can be connected to 802.11[13] in a wireless communication environment. For an Alarm system [10] a radio port [12] may be well suited.

The idea of the current invention are not in consideration of individual connections between the several home devices and command interface component, but for as much as the communication link is capable of supporting two-way communication with the facilities of gathering “status' information/operational data from home devices and issuing "commands' to home devices. Certainly it is a symbolic aspect of the current invention that commands interface component is able to communicate utilizing several communication standards with a wide variety of different devices. This ability allows for a home owner with relatively weak computer/technology skills to access and use the control/monitoring system of the current invention. In operation, a home owner is capable of monitoring and controlling several home devices .while being remotely located with respect to the home by virtue of using voice commands to access command interface component.

In FIG.1 remote home owner[1], and uses a communication device (such as a wireless telephone) to call into his home through PSTN[2] and legacy phone device[18], where legacy phone device[18] is connected through RJ-11 connection to command interface component.

Assume the home owner gives command to his computer at home through circuit switched network like PSTN[2] to send an email to a particular person. The call home may include a first command that allows the home owner to gain access to command interface component[19] (for example, the utterance “access may be recognized by a Speech Recognition Unit (SRU)[15] in command interface component to activate the two-way interaction between the home owner[1] and command interface component[19] .

Once component has been accessed, the home owner can then send the vocal command “send email to a recipient name', where this vocal command is recognized by SRU[15] and used to activate personal computer[7] and find recipient email address. Then the content of the mail can be given as spoken message by the home owner. In this situation Speech-to-text conversion unit[16] within command interface component[19] is used to convert the speech input into text suitable for transmission as email. The message is then transmitted, and (perhaps) component transmits a reply “email sent to the remotely-located home owner as confirmation.

In another situation a home owner may again “access' command interface component [19], and request the status of any controlled device within the home. For example, a home owner makes a call to command interface component [19] and pronounce a vocal command to “switch on the lights '. In this case, the command interface component will diagnose the switch on lights on command using SRU

[15] and activate the all the light bulbs controlled through a microprocessor-based in-house control unit within component. Similarly the remotely-located home owner can supervise the state of the alarm system [10] if there sudden situation arises, which triggers an actual 'alarm condition, interface control component may be configured, using a set of user policies stored within interface control component, to immediately call the home owner's cell number—such as the number of device — (in addition to calling the proper emergency personnel). In a larger sense, the customized user policies may encompass a database of various conditions that are typically programmed by the home owner to control various devices. The policies [17] may exercise time-sensitive information like time-of- day, day-of-week, etc., to turn up/down thermostat settings, turn on/off sprinkler systems, lights, etc., while allowing real- time vocal commands from a remote homeowner to reverse the pre-established policies when necessary.

FIG. 2 depicts an ideal diagram of a multi layered software framework related with the implementation of the command interface component of the current invention. The Software framework is divided into three layers: “applications” [1], “system” [2], and “hardware” [3] displaying the locations of the several framework planes within these three layers. As indicated, with “applications' set as a first layer , a management plane is indicated and consists of a collection of the several Subsystems and components that are required to carry out the several “remote control’ commands that may be submitted by a home owner.

In the ideal organization as shown in FIG. 2, management plane is demonstrated as constituting an email applications component [1A], an internal applications component [1B], a monitor/control application component [1C] and a data storage component [1D]. A control plane and a system plane are demonstrated a system/middle layer. An open Application Program Interface (API) [1E]. Component

is employed to ensure communication between management plane and control and system planes. Control plane is established as the assembly of subsystems engaged in signalling and routing of data within command interface component.
System plane [2B] in principle is a collection of the several customary services necessary to function in the background to carry out the functionality of command interface component, such as an operating system, file system, etc. A suitable communication method, Such VPN or a TCP stack [2D] may be incorporated in the system plane. Beside this, the details of system plane are not considered as being pertinent to the subject matter of the current invention.

The system/middle layer [2] also includes a data plane [2C] which is in charge of all communication data path processing within component. Precisely, the data communications consists of the physical interface processing for all external interfaces, logical interface processing for all data protocol layers, status and statistics handling, end-point (Service Access Point) support, cross-connect handling for all connection-oriented end-points, forwarding/routing handling for all connectionless end-points, data access to end points (i.e., application access to “source' or "sink’ data), and Quality of Service (QoS) support.

The hardware level [3] contains several components that are required deploy communication ports, as

shown in FIG.1. The hardware level is depicted as including an RJ-11 component [3H], a USB module [3I], an Ethernet component [3J], an 802.11 component [3K], a radio communication component [3L], and so on. The hardware level also includes the subsystems of command interface component such as speech- to-text conversion unit [3B], SRU [3E] and control unit. Also demonstrated in the hardware level is a "text-to-speech' conversion unit [3C] that works to convert an incoming email (for example) into a speech message that may be transmitted to a remote home owner. A voice-over-IP (VoIP) unit [3D] is included and may be accessed via a "dial tone' speech command from a remote homeowner. A data history log [3G] is included and may be used to store information related to past activities of component.

In accordance with these instructions of the current invention, therefore, it is possible to design an interface command component that can efficiently interact with the existing voice and data networks, providing a smooth connection between a remote home owner and a variety of different gadgets/appliances. For the reason of using existing technologies Such as Speech recognition in fusion with the emerging wireless home device technology, a home owner will be able to contact with home from virtually any place in the earth A technique and scheme has been bring to light for remotely controlling several home gadget/appliances via speech command with the help of a cellular telephone.

Despite of the fact that the current invention has been represented in accordance with the organization as displayed, one of standard technique in the art will immediately make out that there could be variations to the structure and those variations are considered to fall within the spirit and scope of the current invention.

Subsequently many adjustments may be made by one of standard technique in the art without departing from the spirit and scope of the reclamation as appended here to. What is claimed is:

(A) A technique to control variety of electronic gadgets placed within a home, the method involving: receiving a voice telephone call over a public-Switched telephone network at a home-based command interface unit, the Voice telephone call being made by a remotely located user; receiving, at the home-based command interface component, a spoken command from the remotely-located user during the voice telephone call to the home-based command interface unit; judging the spoken command at the home-based command interface unit to discover genuineness of the remotely-located user and to find out an action requested by the spoken command; and, if authenticated, causing the home-based command interface to interact with at least one of the several electronic devices to carry out the Spoken command from the remotely- located homeowner

(B) The method of claim A, wherein the method additionally consists of a confirmation message from the home- based command interface component to the remotely-located homeowner during the telephone call upon completion of requested actions.

(C) The method of claim A also includes, getting a spoken command, obtaining a set of user policies stored within the home-based command interface component.

(D) The method of claim

(E), wherein the set of user policies comprises a database of working conditions for the several electronic devices.

(F) The method of claim A, again comprising storing the spoken command in a history log within the home-based command interface unit.

(G) An equipment for remotely controlling a variety electronic devices located within a home, the system comprising: a processor; and storage storing programming that when executed causes the processor to perform operations, the operations com prising: receiving a voice telephone call over a public-

Switched telephone network at a home- based command interface unit, the voice telephone call including a spoken command; evaluating the spoken command at the home-based command interface unit to ascertain authenticity of a remotely-located user and deciding an operation requested by the spoken command; and interface for interacting the home-based command interface unit with one of the many of electronic devices to carry out the spoken command from the remotely-located homeowner.

(H). The appliance of claim

(I) wherein the actions further comprise transmitting a confirmation message from the home-based command interface unit to the remotely-located user during the spoken telephone call upon completion of requested actions. 8. The appliance of claim (F) wherein the actions again comprise storing a history log within the home-based command interface component for finished spoken commands.

Cite this article as :

Neelima Sahu, "A Self-regulatory Personal Assistant for a Smart Home", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 73-78, September-October 2019.

Journal URL : http://ijsrcseit.com/CSEIT194713

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Cyber Encryption

A. Sruthi
The Kingdom College, Bengaluru, Karnataka, India

ABSTRACT

The paper talks about the introduction of wireless security, modes of unauthorized access and security measures. I intend to explain the generation of protocols used and their pros and cons. I also define the encryption keys that were used in each generation to manipulate security. Finally I conclude with certain protocols and their combinations that are more secured in this generation.

Keywords : Encryption, protocols and combinations.

I. INTRODUCTION

At present everyone wants to access internet; for this, people are connecting their smart phones, laptops, computers and other devices with wireless network. For example a Business man wants to transact by connecting to the wireless network or an employee of a company wants to share a document with other branch employee.

Globally for every purpose people are using Wi-Fi network so that their tasks are completed in fraction of seconds. But for any invention we do have advantages and disadvantages. While using Wi-Fi networks people have to secure their data and systems. So I am here to explain Wi-Fi security.

Wireless Security means safeguarding the devices like smart phones, computers, laptops and other devices along withthe networks they are connected to from unapproved access.

Wi-Fi is becoming very popular since last decade. We can observe Wi-Fi in airports, malls, libraries, coffee shops, hotels, and other public venues etc…

A wireless network uses radio waves to transmit data instead of wired connections.There are 4 environments built around wireless technology, they are:

1. Hardware or Software based Access Point.
2. Multiple Access Point.
3. LAN-to-LAN wireless network. 4.3G and 4G hot spot.

Modes of unauthorized Access:

Accidental association

When a user wants to connect with a wireless network, the user looks out for a nearby network which has a strong network. Later the user connects his device to that particular network. If that network is under the surveillance of the attacker, then the user data is hacked. So Accidental association is nothing but without the knowledge of the user their devices are surveillanced by hackers.

Malicious association

This happens when a wireless device wants to connect with laptops known as “soft APs”. These laptops are created when a cyber criminal runs his software that

makes the wireless network card look like a legal access point. Once the criminal gets access,

they can easily steal passwords, launch attacks or plant viruses to the network.

Ad hoc networks

Ad hoc networks are defined as peer-to-peer networks. Actually there is no internet connection, attackers setup these kind of networks and make them visible like an actual internet connection with a name Free Wi-Fi. When a user connects to the Ad hoc network they are revealing their devices to attack.

Non-traditional networks

Usually people mainly concentrate on laptops and Access points to be secured. Non-traditional networks focuses on PDA's, printers etc…, through these devices cyber criminals are injecting the threats to wireless networks.

Identity theft (MAC spoofing)

Every NIC(Network Interface Card) provides a connection to a router which contains a unique MAC (Media Access Control) address. By using this facility we have filters called MAC filtering to allow certain addresses into the network. If an attacker is listening to a network traffic and gets the MAC address of any computer,it can be very useful to an attacker. The attacker uses this MAC address and enters into the secured networks this is called

MAC spoofing(stealing and using the MAC address).
Man-in-the-middle attacks.

This attack is similar to malicious association. An attacker tempts devices to sign into a computer called "soft AP", if the user connects his devices with this computer the attacker connects to the real Access Point through some NIC.

Denial of service

This attacks usually makes the network traffic slow down or cause the network to crash. The Denial of service attacks are meant to disturb the network services. So that legal networks may be unable to connect or use the network.

Caffe Latte attack

In the past, if a hacker wants to attack a network; they had to be in the range of wireless network but by this Caffe Latte attack he could not be in the range to attack the network. This attack is to retrieve WEP encryption key.

Secured Protocols used in wireless security:
1) Wired Equivalent Privacy(WEP):
It was developed in 1999; a64 bit WEP uses 40 bit encryption key concatenated with a 24-bit initialization vector(IV) to form the Rivest Cipher 4(RC4) key and which was easily hacked by unauthorized users. To increase more security later we introduced a 104 bit(concatenated with 24 bit totally 128 bits), 128 bit (combined with 24 bit totally 152 bits), 232 bit(combined with 24 bits of system generated data i.e., totally 256 bits).Even though we could make it secure, effortlessly hackers could discover the WEP key. So that this protocol is not used at present and even the modern Wi-Fi routers don't have the option of WEP. To achieve more security WPA was introduced.

2) Wi-Fi Protected Access(WPA):
The new version of security protocol called WPA was developed in the year 2003 to solve the problems of WEP. It is far better than WEP, began implementation of IEEE 802.11i Standard, it uses a stronger encryption method called TKIP (Temporary Key Integrity Protocol). TKIP dynamically changes its keys for each data packet. When TKIP encryption used, MIC (Message Integrity Code) is included to check the data

is not hacked is known as Cyclic Redundancy Checking(CRC).

This is the major improvement in WPA compared with WEP.

3) Wi-Fi Protected Access II (WPA2):

WPA with TKIP could only be capable of encrypting "short" i.e., 128 bytes data packets. This leads TKIP to be substituted with CCMP also named as AES-CCMP (Advanced Encryption Standard- Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) encryption protocol.WPA2 was developed to provide even stronger security than WPS. Which is available from the year 2004.

The list of Wi-Fi security protocols available on the routers are:

1. WPA2+AES
2. WPA+AES
3. WPA+TKIP/AES
4. WPA+TKIP
5. WEP

6) Open Network (no security)

The order is from more security to less security and the last option is without security which means we are not setting up any key for the network so that any visitor can easily enter into that network. We can find these kind of networks in public places like Theaters, Hotels, and Resorts etc…

4) Wi-Fi Protected Access III (WPA3):

WPA3 was introduced in 2018, it adds new features to simplify Wi-Fi

Solutions:

minutes the user has to press the button on the printer to connect to the network.

2. WPS Pin number method: Like the WPS push method, the user has to enter the WPS pin number in the box and within few seconds it will connect to the printer security and enable more authentication. WPA3 upgrades to 128 bit encryption and uses SAE(Simultaneous Authentication of Equals) which is known as Dragonfly Handshake.

5) Wi-Fi Protected Setup (WPS): Designed for people who know about wirCeless networks to make it as easy as possible for devices to join a secure wireless network. In this setupwe have two methods of which either of them can be used.

1. WPS Push method:

Most routers today have physical WPS button and a lot of Wi-Fi supported printers have WPS button. If the user presses WPS button on the router, within 2

1. Change default Administrator

Username and passwords.

2. Change the default SSID(Service Set Identifier) name and hide the same.

3. Use a strong password and use good wireless encryption.

4. Turn off guest network and turn on device lists to view the devices which are connected to your Wi-Fi so that we can block the unsafe devices.

5. Enable MAC (Media Access Control) address filtering.

II. CONCLUSION

Globally people are communicating, transacting, sending and receiving messages, sharing documents and pictures by using wireless connections. So we can't come out of it. Even though security protocols and

their versions are modified to the great extent to make the network secure, hackers are finding different ways to break the code and heisting the data. If we take few precautions we may be some- what secure for a minimal time. Some precautions are:

1. Think before connecting to a free Wi-Fi network.
2. Switch off your Wi-Fi routers when not in use.

Finally I conclude that WPA+AES is the best and more secured version of wireless encryption protocol for the contemporary generation of networks.

Cite this article as :

A. Sruthi , "Cyber Encryption ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 79-82, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194714

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Review on Security Issues In Cloud And Introduction To Implementation of Devsecops To Avoid Security Issues In Cloud Computing

Chethan. C, Monisha A V, Reshma . B
Seshadripuram Academy of Business Studies Kengeri Satellite Town Bengaluru, Karnataka, India

ABSTRACT

In today's world Cloud Computing is everywhere. And it can be defined as a huge warehouse of data storage. Cloud computing enables tasks to be assigned to a combination of software and services over a internet. Cloud service vendors hosts the data of the data owners in their servers and the users can access their data through these servers through a Web consoles. Hence Cloud enables the organisation to setup a cost efficient and effective infrastructure virtually and it follows pay as you use basis. The issue here is as the data owners and the severs are two different individuals, Hence proper care to be taken that data is stored in a secured manner with proper encryption. And also the implementation of new technology called DevSecOps will avoid all most all the security issues in cloud.

I. INTRODUCTION

A BRIEF INTRODUCTION ON CLOUD COMPUTING

Cloud computing can be defined as "delivery of computing services (servers, storage, databases, networking, software, analytics, intelligence and more) over the Internet" . Here we typically pay only for cloud services we use, It helps in lowering our operating costs,and helps us to run our infrastructure more efficiently .

Types of cloud :

There are three ways to set up a cloud services :
1): public cloud, 2):private cloud 3): hybrid cloud.
Public cloud : Public clouds are owned and hosted operated by a cloud vendor, which deliver their servers and storage over the Internet.AWS, V cloud , Google cloud and Microsoft Azure is an example of a public cloud. With a public cloud, a complete infrastructure is owned and managed by the cloud provider. You access these things using a web console.

Private cloud
A private cloud refers to cloud computing resources used by a one company . A private cloud can be physically located in the company . Some companies also uses a third-party service vendor to host their cloud. A private cloud is one in which the infrastructure are maintained on a private own network.

Hybrid cloud
This is a combination of both public and private clouds. By allowing data and applications to move between private and public clouds, It gives our business greate freedom and deployment options and helps to secure our infrastructure more efficiently.

Types of cloud computing services:

There are 3 major cloud computing services and they are :

1) : Infrastructure as a service (IaaS),

2) : Platform as a service (PaaS),and 3): Software as a service (SaaS).

Knowing more about these services makes us achieve all the company requirements.

Infrastructure as a service (IaaS)

The most basic service of cloud is IaaS. On a pay as u use basis With IaaS, we can rent IT infrastructure servers and virtual machines (VMs), storage, networks, operating systems from a cloud vendor .

Platform as a service (PaaS)

Platform as a services supply an on demand environment for developing, testing, delivering and managing software applications. PaaS is designed to make it easier for developers to quickly create a app or website, without worrying about the infrastructure.

Software as a service (SaaS)

Software as a service is a method for delivering software applications over the Internet. With SaaS, cloud providers host and manage the software application and will take care of maintainance of that software like upgrades security of the software etc. Users connect to the application over the Internet using their device.

Following are the benefits of cloud computing:

1. Cost efficient to build a infrastructure
2. Dependable performance
3. Lesser Maintenance issues
4. Regular software updates
5. Improved compatibility between Operating systems
6. Backup and recovery
7. Performance and Scalability
8. Increased storage capacity

Cloud Architecture:

Cloud computing comprises of two components front end and back end. Front end consist client part of cloud computing system. It comprise of interfaces and applications that are required to access the cloud platform.

While back end refers to the cloud itself, it comprises of the resources that are required for cloud computing services. It consists of VMs, servers,storage, security units etc. It is under the control of cloud provider.

Cloud computing distributes the file system that spreads over multiple hard disks and machines. Data is never stored in one place only and in case one unit fails the other will take over automatically. The user disk space is allocated on the distributed file system.

Security problems in Cloud Computing

The major issue that arises in the users mind is about its security.One concern is that cloud vendors themselves may have access to the company's unencrypted data whether it's on disk, in memory or the data that travel over the network.

To provide security for systems, networks and data, cloud computing service providers have joined hands with TCG (Trusted Computing Group) which is non-profit organization which regularly releases a set of guidelines to secure hardware, create self-encrypting drives and improve security. It protects the data from unauthorised access and make sure that data is safe.

As computing involves with different devices like hard disk drives and mobile phones, TCG has extended the security measures to include these devices to make sure that users are safe.

Privacy in Cloud

Privacy present a strong barrier for users to adapt into Cloud Computing systems

There are certain measures which can improve privacy in cloud computing.

1. The administrative staff of the cloud computing service could theoretically monitor the data moving in

memory before it is stored in disk .To keep the confidentiality of a data, administrative and legal controls should prevent this from happening.

2. Here to make sure the data is confidential , cryptographic algorithms and strong authentication process should be used . And encryption of the data is must , here encryption means storing a data in the cloud in such a way that only authorised user can understand and access that particular data. Proper encryption is so powerful that even the cloud service provider will be unable to read the data.

Various security issues in cloud

Security issues while transferring of data to CLOUD

It is the process of transferring data over a medium to one or more computing network. In Cloud environment most of the data is not encrypted in the processing time. To process data for any application that data must be unencrypted. The data theft when the attackers place themselves in the communications path between the users. Here there is the possibility that they can interrupt and change communications to their desired locations.

Security issues in VM's

Virtual Machine (VM) means sharing the resources of single physical computer into various computers. VM's provide agility, flexibility and scalability to the cloud resources by allowing the cloud service providers to copy, move and manipulate their VM's. Keeping this in mind, malicious hackers are finding ways to get their hands on data by breaching the security layers of cloud environments. The cloud computing scenario is not as transparent as it claims to be. The service user has no idea about how the data is processed and stored.And dosent have direct control over the flow of data.

Security issues in Application Programming Interfaces (API)

Customers handle and interact with cloud services through API's. Cloud service Providers must ensure that security is integrated into their service models, while users must be aware of security risks.

DevSecOps Approach to Cloud Security Majority leading firms are striving to deliver high and highly-scalable performance with 24/7 digital services that are built on customized modern architectures. Successful models of modern architectures are being developed on the stack of advanced tiers, technologies and microservices, backed by the market's leading cloud platforms such as AWS, GCP, and Azure.

Above all these advanced services, security continues to be a key concerning factor for the majority of them. Applying DevSecOps for Cloud Security definitely solves the issue. As the surveys show, the majority of firms developing apps on the cloud are inclined towards adopting DevSecOps security tools and processes for improved agility and high reliability.

Adopting DevSecOps principles in Cloud requires an effective strategy and planning involving cultural changes, especially in automating security and configuration of assets in the cloud.

For this, security teams will need to:

• Work in collaboration with Development teams who push code to cloud-based applications, to ensure quality aspect in the production cycle is achieved without affecting the pace of the process

• Coordinate with the Quality Analysis and Development teams in defining qualifier and parameter prerequisites needed for promoting code

Cloud-native machine data analytics platform is also an important requirement to enhance cloud security,

considering the short-term nature of modern applications and limitations associated with the traditional monitoring and security mechanisms.

Adding to the machine data analytics solutions, DevSecOps principles brings you closer to achieving software agility, high reliability and enhanced security through continuous monitoring and keen analyzation of end-to-end tools and processes across the lifecycle.

Implementation of DevSecOps
Separation of development and security are no longer two different aspects.
DevSecOps combined them into a single streamlined process by incorporating security at the level of code, thus ensuring safety of applications and processes at all levels of the process chain.

Five features speak the successful implementation of DevSecOps:

• Mandatory security at every stage
• Thorough Assessment before security
• Security-related changes right at the code level
• Automation of all possible processes
• Continuous monitoring through alerts and dashboards

II. CONCLUSION

In today's world cloud computing is an essential technology where each and every organisation are moving towards cloud but the major fear that is running in users mind is about the security of their data.
Usage of DevSecOps in organisation will reduce the security issues in cloud and also from the clients there should be a proper legal agreement to be done with the cloud provider before the setup of cloud in the organisation . And also an active and efficient team need to be working on encryption of data before storing or transferring the data to the cloud .

III. REFERENCES

[1]. V.Suresh Babu , Maddali M.V.M kumar "An efficient and secure data storage operations in cloud computing". – 2018 IJSRSET volume 4. Themed section engineering and technology
[2]. Supriya D Patil, Komal S Talekar,Reshma R Raskar,Pooja A Chavans –"Attribute based access control in personal health records using cloud computing – 2018 IRJET volume 4.
[3]. Vivek paul , Supriya Panditha – "Cloud computing review" – Mar 2018 IRJET volume 5.
[4]. A Venkatesh , Marrynal S Eastaff – "A Study of data storage issues in cloud computing" – 2018 IJSRCSEIT volume 3.
[5]. M. AlZain, E. Pardede, B. Soh, and J. Thom, "Cloud computing security: From single to multi-clouds," in System Science (HICSS), 2012 45th Hawaii International Conference on, Jan 2012, pp. 5490–5499.
[6]. E. Aguiar, Y. Zhang, and M. Blanton, "An overview of issues and recent developments in cloud computing and storage security," in High Performance Cloud Auditing and Applications. Springer, 2014
[7]. CLOUD COMPUTING: STUDY OF SECURITY ISSUES AND RESEARCH
[8]. CHALLENGES Adnaan Arbaaz Ahmed, Dr.M.I.Thariq Hussan Volume 7, Issue 4,April 2018, ISSN: 2278 – 1323

Cite this article as : Chethan. C, Monisha A V, Reshma . B , "Review on Security Issues In Cloud And Introduction To Implementation of Devsecops To Avoid Security Issues In Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 83-86, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194715

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Wireless Security

Sachin Kumar
IIFA Lancaster Degree College, Bengaluru, Karnataka, India

ABSTRACT

Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks. The most common type is Wi-Fi security, which includes Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard: the password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1997, [1] which was superseded in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP.

Keywords : Wired Equivalent Privacy, Wi-Fi Protected Access, Encryption, Hacking, WLAN, NFC, ZigBee

I. INTRODUCTION

The current standard is WPA2; some hardware cannot support WPA2 without f irmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP. Enterprises often enforce security using a certificate-based system to authenticate the connecting device, following the standard 802.1X.

Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks. [2] As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. [3] Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

The risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was f irst introduced. Hackers had not yet had time to latch on to the new technology, and wireless networks were not commonly found in the work place. However, there are many security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. [4] Hacking methods have become much more sophisticated and innovative with wireless access. Hacking has also become much easier and more accessible with easy-touse Windows- or Linux- based tools being made available on the web at no charge.

Some organizations that have no wireless access points installed do not feel that they need to address wireless security concerns. In-Stat MDR and META Group have estimated that 95% of all corporate laptop

computers that were planned to be purchased in 2005 were equipped with wireless cards. Issues can arise in a supposedly non- wireless organization when a wireless laptop is plugged into the corporate network. A hacker could sit out in the parking lot and gather information from it through laptops and/or other devices, or even break in through this wireless card–equipped laptop and gain access to the wired network.

Background

Anyone within the geographical network range of an open, unencrypted wireless network can " sniff", or capture and record, the traffic, gain unauthorized access to internal network resources as well as to the internet, and then use the information and resources to perform disruptive or illegal acts. Such security breaches have become important concerns for both enterprise and home networks.

If router security is not activated or if the owner deactivates it for convenience, it creates a free hotspot. Since most 21stcentury laptop PCs have wireless networking built in (see Intel " Centrino" technology), they don't need a third-party adapter such as a PCMCIA Card or USB dongle. Built-in wireless networking might be enabled by default, without the owner realizing it, thus broadcasting the laptop's accessibility to any computer nearby.

Modern operating systems such as macOS, or Microsoft Windows make it fairly easy to set up a PC as a wireless LAN "base station" using Internet Connection Sharing, thus allowing all the PCs in the home to access the Internet through the "base" PC.

However, lack of knowledge among users about the security issues inherent in setting up such systems often may allow others nearby access to the connection. Such "piggybacking" is usually achieved without the wireless network operator's knowledge; it may even be without the knowledge of the intruding user if their computer automatically selects a nearby unsecured wireless network to use as an access point.

The threat situation

Wireless security is just an aspect of computer security; however, organizations may be particularly vulnerable to security breaches [5] caused by Rogue access points.

If an employee (trusted entity) brings in a wireless router and plugs it into an unsecured switchport, the entire network can be exposed to anyone within range of the signals. Similarly, if an employee adds a wireless interface to a networked computer using an open USB port, they may create a breach in network security that would allow access to confidential materials. However, there are effective countermeasures (like disabling open switchports during switch configuration and VLAN configuration to limit network access) that are available to protect both the network and the information it contains, but such countermeasures must be applied uniformly to all network devices.

Threats and Vulnerabilities in an industrial (M2M) context.

Due to its availability and low cost, the use of wireless communication technologies increases in domains beyond the originally intended usage areas, e.g. M2M communication in industrial applications. Such industrial applications often have specific security requirements. Hence, it is important to understand the characteristics of such applications and evaluate the vulnerabilities bearing the highest risk in this context. Evaluation of these vulnerabilities and the resulting vulnerability catalogs in an industrial context when considering WLAN, NFC and ZigBee are available.

The mobility advantage

Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards preinstalled. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired network resource. As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

The air interface and link corruption risk

There were relatively few dangers when wireless technology was first introduced, as the effort to maintain the communication was high and the effort to intrude is always higher. The variety of risks to users of wireless technology have increased as the service has become more popular and the technology more commonly available. Today there are a great number of security risks associated with the current wireless protocols and encryption methods, as carelessness and ignorance exists at the user and corporate IT level. [4] Hacking methods have become much more sophisticated and innovative with wireless.

Modes of unauthorized access

The modes of unauthorised access to links, to functions and to data is as variable as the respective

entities make use of program code. There does not exist a full scope model of such threat. To some extent the prevention relies on known modes and methods of attack and relevant methods for suppression of the applied methods. However, each new mode of operation will create new options of threatening. Hence prevention requires a steady drive for improvement. The described modes of attack are just a snapshot of typical methods and scenarios where to apply.

Accidental association

Violation of the security perimeter of a corporate network can come from a number of different methods and intents. One of these methods is referred to as “accidental association”. When a user turns on a computer and it latches on to a wireless access point from a neighboring company's overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network.

Accidental association is a case of wireless vulnerability called as "misassociation". [8] Mis-association can be accidental, deliberate (for example, done to bypass corporate firewall) or it can result from deliberate attempts on wireless clients to lure them into connecting to attacker's APs.

Malicious Association

“Malicious associations” are when wireless devices can be actively made by attackers to connect to a company network through their laptop instead of a company access point (AP). These types of laptops are known as “soft APs” and are created when a cyber criminal runs some software that makes his/her wireless network card look like a legitimate access point. Once the thief has gained access, he/she can steal passwords, launch attacks on the wired network, or plant trojans. Since wireless networks operate at the Layer 2 level, Layer 3

protections such as network authentication and virtual private networks (VPNs) offer no barrier.

Wireless 802.1X authentications do help with some protection but are still vulnerable to hacking. The idea behind this type of attack may not be to break into a VPN or other security measures. Most likely the criminal is just trying to take over the client at the Layer 2 level.

Ad hoc networks

Ad hoc networks can pose a security threat. Ad hoc networks are defined as [peer to peer] networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.

The security hole provided by Ad hoc networking is not the Ad hoc network itself but the bridge it provides into other networks, usually in the corporate environment, and the unfortunate default settings in most versions of Microsoft Windows to have this feature turned on unless explicitly disabled. Thus the user may not even know they have an unsecured Ad hoc network in operation on their computer. If they are also using a wired or wireless

infrastructure network at the same time, they are providing a bridge to the secured organizational network through the unsecured Ad hoc connection. Bridging is in two forms. A direct bridge, which requires the user actually configure a bridge between the two connections and is thus unlikely to be initiated unless explicitly desired, and an indirect bridge which is the shared resources on the user computer. The indirect bridge may expose private data that is shared from the user's computer to LAN connections, such as shared folders or private Network Attached Storage, making no distinction between authenticated or private connections and unauthenticated Ad-Hoc networks. This presents no threats not already familiar to open/public or unsecured wifi access points, but firewall rules may be circumvented in the case of poorly configured operating systems or local settings.

Non-traditional networks

Non-traditional networks such as personal network Bluetooth devices are not safe from hacking and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured. These nontraditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points.

Identity theft (MAC spoofing)

Identity theft (or MAC spoofing) occurs when a hacker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to allow only authorized computers with specific MAC IDs to gain access and utilize the network. However, programs exist that have network " sniffing" capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the hacker desires, [11] and the hacker can easily get around that hurdle.

MAC filtering is effective only for small residential (SOHO) networks, since it provides protection only when the wireless device is "off the air". Any 802.11 device "on the air" freely transmits its unencrypted MAC address in its 802.11 headers, and it requires no special equipment or software to detect it.

Anyone with an 802.11 receiver (laptop and wireless adapter) and a freeware wireless packet analyzer can obtain the MAC address of any transmitting 802.11 within range. In an organizational environment, where most wireless devices are "on the air"

throughout the active working shift, MAC filtering provides only a false sense of security since it prevents only "casual" or unintended connections to the organizational infrastructure and does nothing to prevent a directed attack.

Man-in-the-middle attacks

A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. One type of man-in-themiddle attack relies on security faults in challenge and handshake protocols to execute a “de-authentication attack”. This attack forces AP-connected computers to drop their connections and reconnect with the hacker's soft AP (disconnects the user from the modem so they have to connect again using their password which one can extract from the recording of the event). Man-in- the-middle attacks are enhanced by software such as LANjack and AirJack which automate multiple steps of the process, meaning what once required some skill can now be done by script kiddies.

Hotspots are particularly vulnerable to any attack since there is little to no security on these networks.
Denial of service

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

The DoS attack in itself does little to expose organizational data to a malicious attacker, since the interruption of the network prevents the flow of data and actually indirectly protects data by preventing it from being transmitted. The usual reason for performing a DoS attack is to observe the recovery of the wireless network, during which all of the initial handshake codes are re-transmitted by all devices, providing an opportunity for the malicious attacker to record these codes and use various cracking tools to analyze security weaknesses and exploit them to gain unauthorized access to the system.

This works best on weakly encrypted systems such as WEP, where there are a number of tools available

which can launch a dictionary style attack of "possibly accepted" security keys based on the "model" security key captured during the network recovery.

Network Injection

In a network injection attack, a hacker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as “ Spanning Tree” (802.1D), RIP, and OSPF, HSRP. The hacker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.
Caffe Latte attack.

The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. [12] By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in

802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.

Wireless intrusion prevention concepts. There are three principal ways to secure a wireless network.

- ✓ For closed networks (like home users and organizations) the most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address. Wireless Intrusion Prevention Systems can be used to provide wireless LAN security in this network model.
- ✓ For commercial providers, hotspots, and large organizations, the preferred solution is often to have an open and unencrypted, but completely isolated wireless network. The users will at first have no access to the Internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to require the users to connect securely to a privileged network using VPN.
- ✓ Wireless networks are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it is also often possible for remote intruders to gain access to the network through backdoors like Back Orifice. One general solution may be end-to-end encryption, with independent authentication on all resources that shouldn't be available to the public.

There is no ready designed system to prevent from fraudulent usage of wireless communication or to protect data and functions with wirelessly communicating computers and other entities. However, there is a system of qualifying the taken measures as a whole according to a common understanding what shall be seen as state of the art.

The system of qualifying is an international consensus as specified in ISO/IEC 15408.

A wireless intrusion prevention system

A Wireless Intrusion Prevention System (WIPS) is a concept for the most robust way to counteract wireless security risks. [14] However such WIPS does not exist as a ready designed solution to implement as a software package. A WIPS is typically implemented as an overlay to an existing Wireless LAN infrastructure, although it may be deployed standalone to enforce no-wireless policies within an organization. WIPS is considered so important to wireless security that in July 2009, the Payment Card Industry Security Standards Council published wireless guidelines [15] for PCI DSS recommending the use of WIPS to automate wireless scanning and protection for large organizations.

Security measures

There are a range of wireless security measures, of varying effectiveness and practicality.

SSID hiding

A simple but ineffective method to attempt to secure a wireless network is to hide the SSID (Service Set Identifier). [16] This provides very little protection against anything but the most casual intrusion efforts.

MAC ID filtering

One of the simplest techniques is to only allow access from known, pre-approved MAC addresses. Most wireless access points contain some type of MAC ID filtering. However, an attacker can simply sniff the MAC address of an authorized client and spoof this address.

Static IP addressing

Typical wireless access points provide addresses to clients via IP DHCP. Requiring clients to set their own addresses makes it more difficult for a casual or

unsophisticated intruder to log onto the network, but provides little protection against a sophisticated attacker.

Regular WEP

The Wired Equivalent Privacy (WEP) encryption standard was the original encryption standard for wireless, but since 2004 with the ratification WPA2 the IEEE has declared it "deprecated", [17] and while often supported, it is seldom or never the default on modern equipment.

Concerns were raised about its security as early as 2001, [18] dramatically demonstrated in 2005 by the FBI, 2007 [19] yet in T.J. Maxx admitted a massive security breach due in part to a reliance on WEP [20] and the Payment Card Industry took until 2008 to prohibit its use - and even then allowed existing use to continue until June 2010.

WPAv1

The Wi-Fi Protected Access (WPA and WPA2) security protocols were later created to address the problems with WEP. If a weak password, such as a dictionary word or short character string is used, WPA and WPA2 can be cracked. Using a long enough random password (e.g. 14 random letters) or passphrase (e.g. 5 randomly chosen words) makes preshared key WPA virtually uncrackable.

The second generation of the WPA security protocol (WPA2) is based on the final 802.11i amendment to the standard and is eligible for 802.11 IEEE FIPS 140 -2 compliance. With all those encryption schemes, any client in the network that knows the keys can read all the traffic.

Wi-Fi Protected Access (WPA) is a software/firmware improvement over WEP. All regular WLAN-equipment that worked with WEP are able to be simply upgraded and no new equipment needs to be bought. WPA is a trimmed-down version of the 802.11i security standard that was developed by the IEEE 802.11 to replace WEP. The TKIP encryption algorithm was developed for WPA to provide improvements to WEP that could be f ielded as f irmware upgrades to existing 802.11 devices.

The WPA profile also provides optional support for the AESCCMP algorithm that is the preferred algorithm in 802.11i and WPA2.

WPA Enterprise provides RADIUS based authentication using 802.1X. WPA Personal uses a pre-shared Shared Key (PSK) to establish the security using an 8 to 63 character passphrase. The PSK may also be entered as a 64 character hexadecimal string. Weak PSK passphrases can be broken using off-line dictionary attacks by capturing the messages in the four-way exchange when the client reconnects after being reauthenticated.

Wireless suites such as aircrack-ng can crack a weak passphrase in less than a minute. Other WEP/WPA crackers are AirSnort and Collection. Auditor Security [22] Still, WPA Personal is secure when used with ‘good’ passphrases or a full 64- character hexadecimal key.

There was information, however, that Erik Tews (the man who created the fragmentation attack against WEP) was going to reveal a way of breaking the WPA TKIP implementation at Tokyo's PacSec security conference in November 2008, cracking the encryption on a packet in between 12–15 minutes. [23] Still, the announcement of this 'crack' was somewhat overblown by the media, because as of August, 2009, the best attack on WPA (the Beck- Tews attack) is only partially successful in that it only works on short data packets, it cannot decipher the WPA key, and it requires very specific WPA implementations in order to work.

Additions to WPAv1

In addition to WPAv1, TKIP, WIDS and may be added alongside. Also, EAP VPNnetworks (non-continuous secure network connections) may be set up under the 802.11-standard. VPN implementations include PPTP, L2TP, IPsec and SSH. However, this extra layer of security may also be cracked with tools such as Anger, Deceit and Ettercap for PPTP; [25] and ikescan, IKEProbe for IPsec-connections.

TKIP

This stands for Temporal Key Integrity Protocol and the acronym is pronounced as tee-kip. This is part of the IEEE 802.11i standard. TKIP implements per-packet key mixing with a re-keying system and also provides a message integrity check. These avoid the problems of WEP.

EAP

The WPA-improvement over the IEEE 802.1X standard already improved the authentication and authorization for access of wireless and wired LANs.

In addition to this, extra measures such as the Extensible Authentication Protocol (EAP) have initiated an even greater amount of security. This, as EAP uses a central authentication server.

Unfortunately, during 2002 a Maryland professor discovered some shortcomings. Over the next few years these shortcomings were addressed with the use of TLS and other enhancements. [26] This new version of EAP is now called Extended EAP and is available in several versions; these include: EAP- MD5, PEAPv0, PEAPv1, EAP-MSCHAPv2, LEAP, EAP- FAST, EAP-TLS, EAP-TTLS, MSCHAPv2, and EAP- SIM.

EAP-versions

EAP-versions include LEAP, PEAP and other EAP's.

LEAP

This stands for the Lightweight Extensible Authentication Protocol. This protocol is based on

802.1X and helps minimize the original security flaws by using WEP and a sophisticated key management system. This EAP-version is safer than EAP-MD5. This also uses MAC address authentication. LEAP is not secure; LeapCracker can be used to break Cisco's version of LEAP and be used against computers connected to an access point in the form of a dictionary attack. and Anwrap asleap finally are other crackers capable of breaking LEAP.

PEAP

This stands for Protected Extensible Authentication Protocol. This protocol allows for a secure transport of data, passwords, and encryption keys without the need of a certificate server. This was developed by Cisco, Microsoft, and RSA Security.

Other EAPs There are other types of Extensible Authentication Protocol implementations that are based on the EAP framework. The framework that was established supports existing EAP types as well as future authentication methods. [27] EAP-TLS offers very good protection because of its mutual authentication. Both the client and the network are authenticated using certificates and per-session WEP keys. [28] EAP-FAST also offers good protection. EAP-TTLS is another alternative made by Certicom and Funk Software. It is more convenient as one does not need to distribute certificates to users, yet offers slightly less protection than EAP- TLS.

Restricted access networks

Solutions include a newer system for authentication, IEEE 802.1X, that promises to enhance security on both wired and wireless networks. Wireless access points that incorporate technologies like these often also have routers built in, thus becoming wireless gateways.

End-to-end encryption

One can argue that both layer 2 and layer 3 encryption methods are not good enough for protecting valuable data like passwords and personal emails. Those technologies add encryption only to parts of the communication path, still allowing people to spy on the traffic if they have gained access to the wired network somehow. The solution may be encryption and authorization in the

application layer, using technologies like PGP and similar. SSL, SSH, GnuPG, PGP and similar.

The disadvantage with the end-to-end method is, it may fail to cover all traffic. With encryption on the router level or VPN, a single switch encrypts all traffic, even UDP and DNS lookups. With end-to-end encryption on the other hand, each service to be secured must have its encryption "turned on", and often every connection must also be "turned on" separately. For sending emails, every recipient must support the encryption method, and must exchange keys correctly. For Web, not all web sites offer https, and even if they do, the browser sends out IP addresses in clear text.

The most prized resource is often access to the Internet. An office LAN owner seeking to restrict such access will face the nontrivial enforcement task of having each user authenticate themselves for the router. 802.11 i security The newest and most rigorous security to implement into WLAN's today is the 802.11i RSN- standard. This full-fledged 802.11i standard (which uses WPAv2) however does require the newest hardware (unlike WPAv1), thus potentially requiring the purchase of new equipment. This new hardware required may be either AES-WRAP (an early version of 802.11i) or the newer and better AES-CCMP equipment. One should make sure one needs WRAP or CCMP-equipment, as the 2 hardware standards are not compatible.

WPAv2

WPA2 is a WiFi Alliance branded version of the final 802.11i standard. [30] The primary enhancement over WPA is the inclusion of the AES-CCMP algorithm as a mandatory feature. Both WPA and WPA2 support EAP authentication methods using RADIUS servers and preshared key (PSK).

The number of WPA and WPA2 networks are increasing, while the number of WEP networks are decreasing, [31] because of the security vulnerabilities in WEP.

WPA2 has been found to have at least one security vulnerability, nicknamed Hole196. The vulnerability uses the WPA2 Group Temporal Key (GTK), which is a shared key among all users of the same BSSID, to launch attacks on other users of the same BSSID. It is named after page 196 of the IEEE 802.11i specification, where the vulnerability is discussed. In order for this exploit to be performed, the GTK must be known by the attacker.

Additions to WPAv2

Unlike 802.1X, 802.11i already has most other additional security-services such as TKIP. Just as with WPAv1, WPAv2 may work in cooperation with EAP and a WIDS.

WAPI

This stands for WLAN Authentication and Privacy Infrastructure. This is a wireless security standard defined by the Chinese government.

Smart cards, USB tokens, and software tokens

This is a very strong form of security. When combined with some server software, the hardware or software card or token will use its internal identity code combined with a user entered PIN to create a powerful algorithm that will very frequently generate a new encryption code. The server will be time synced to the card or token. This is a very secure way to conduct wireless transmissions. Companies in this area make USB tokens, software tokens, and smart cards. They even make hardware versions that double as an employee picture badge. Currently the safest security measures are the smart cards / USB tokens. However, these are expensive. The next safest methods are WPA2 or WPA with a RADIUS server. Any one of the three will provide a good base foundation for security. The third item on the list is to educate both employees and contractors on security risks and personal preventive measures. It is also IT's task to keep the company workers' knowledge base up-to-date on any new dangers that they should be cautious about. If the employees are educated, there will be a much lower chance that anyone will accidentally cause a breach in security by not locking down their laptop or bring in a wide open home access point to extend their mobile range.

Employees need to be made aware that company laptop security extends to outside of their site walls as well. This includes places such as coffee houses where workers can be at their most vulnerable. The last item on the list deals with 24/7 active defense measures to ensure that the company network is secure and compliant. This can take the form of regularly looking at access point, server, and firewall logs to try to detect any unusual activity. For instance, if any large f iles went through an access point in the early hours of the morning, a serious investigation into the incident would be called for.

There are a number of software and hardware devices that can be used to supplement the usual logs and usual other safety measures.

RF shielding

It's practical in some cases to apply specialized wall paint and window film to a room or building to significantly attenuate wireless signals, which keeps the signals from propagating outside a facility. This can significantly improve wireless security because it's difficult for hackers to receive the signals beyond the controlled area of an enterprise, such as within parking lots.

Denial of service defense

Most DoS attacks are easy to detect. However, a lot of them are difficult to stop even after detection.

Here are three of the most common ways to stop a DoS attack.

Black holing

Black holing is one possible way of stopping a DoS attack. This is a situation where we drop all IP packets from an attacker. This is not a very good long-term strategy because attackers can change their source address very quickly.

This may have negative effects if done automatically. An attacker could knowingly spoof attack packets with the IP address of a corporate partner.
Automated defenses could block legitimate traffic from that partner and cause additional problems.

Validating the handshake

Validating the handshake involves creating false opens, and not setting aside resources until the sender acknowledges. Some firewalls address SYN floods by prevalidating the TCP handshake. This is done by creating false opens. Whenever a SYN segment arrives, the firewall sends back a SYN/ACK segment, without passing the SYN segment on to the target server.
Only when the firewall gets back an ACK, which would happen only in a legitimate connection, would the firewall send the original SYN segment on to the server for which it was originally intended. The f irewall doesn't set aside resources for a connection when a SYN segment arrives, so handling a large number of false SYN segments is only a small burden.

Rate limiting

Rate limiting can be used to reduce a certain type of traffic down to an amount the can be reasonably dealt with. Broadcasting to the internal network could still be used, but only at a limited rate for example. This is for more subtle DoS attacks. This is good if an attack is aimed at a single server because it keeps transmission lines at least partially open for other communication.
Rate limiting frustrates both the attacker, and the legitimate users. This helps but does not fully solve the problem. Once DoS traffic clogs the access line going to the internet, there is nothing a border f irewall can do to help the situation. Most DoS attacks are problems of the community which can only be stopped with the help of ISP's and organizations whose computers are taken over as bots and used to attack other firms.

Mobile devices

With increasing number of mobile devices with 802.1X interfaces, security of such mobile devices becomes a concern. While open standards such as Kismet are targeted towards securing laptops, [34] access points solutions should extend towards covering mobile devices also.

Host based solutions for mobile handsets and PDA's with 802.1X interface.

Security within mobile devices fall under three categories:
1. Protecting against ad hoc networks
2. Connecting to rogue access points
3. Mutual authentication schemes such as WPA2 as described above Wireless IPS solutions now offer wireless security for mobile devices. Mobile patient monitoring devices are becoming an integral part of healthcare industry and these devices will eventually become the method of choice for accessing and implementing health checks for patients located in remote areas. For these types of patient monitoring systems, security and reliability are critical, because they can influence the condition of patients, and could leave medical professionals in the dark about the condition of the patient if compromised. Implementing network encryption In order to implement 802.11i, one must f irst make sure both that the router/access point(s), as well as all client devices are indeed equipped to support the network encryption. If this is done, a server such as RADIUS, ADS, NDS, or LDAP needs to be integrated. This server can be a computer on the local network, an access point / router with integrated authentication server, or a remote server.

AP's/routers with integrated authentication servers are often very expensive and specifically an option for commercial usage like hot spots. Hosted 802.1X servers via the Internet require a monthly fee; running a private server is free yet has the disadvantage that one must set it up and that the server needs to be on continuously.

To set up a server, server and client software must be installed. Server software required is an enterprise authentication server such as RADIUS, ADS, NDS, or LDAP. The required software can be picked from

various suppliers as Microsoft, Cisco, Funk Software, Meetinghouse Data, and from some opensource projects. Software includes:

• Aradial RADIUS Server
• Cisco RADIUS Server Secure Access Control

Software

- freeRADIUS (open-source)
- Funk Software steel belted Radius (Odyssey)
- Microsoft Internet Authentication Service
- Meetinghouse Data EAGIS
- SkyFriendz (free cloud solution based on free RADIUS)

Client software comes built-in with Windows XP and may be integrated into other OS's using any of following software:

• AEGIS-client
• Cisco ACU-client
• Intel PROSet/Wireless Software
• Odyssey client RADIUS

Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization and accounting) protocol used for remote network access. RADIUS was originally proprietary but was later published under ISOC documents 2138 and RFC RFC 2139 . The idea is to have an inside server act as a gatekeeper by verifying identities through a username and password that is already predetermined by the user. A RADIUS server can also be configured to enforce user policies and restrictions as well as record accounting information such as connection time for purposes such as billing.

Open access points

Today, there is almost full wireless network coverage in many urban areas the infrastructure for the wireless community network (which some consider to be the future of the internet) is already in place. One could roam around and always be connected to Internet if the nodes were open to the public, but due to security concerns, most nodes are encrypted and the users don't know how to disable encryption. Many people consider it proper etiquette to leave access points open to the public, allowing free access to Internet. Others think the default encryption provides substantial protection at small inconvenience, against dangers of open access that they fear may be substantial even on a home DSL router.

The density of access points can even be a problem - there are a limited number of channels available, and they partly overlap. Each channel can handle multiple networks, but places with many private wireless networks (for example, apartment complexes), the limited number of Wi-Fi radio channels might cause slowness and other problems.

According to the advocates of Open Access Points, it shouldn't involve any significant risks to open up wireless networks for the public:

- ✓ The wireless network is after all confined to a small geographical area. A computer connected to the Internet and having improper configurations or other security problems can be exploited by anyone from anywhere in the world, while only clients in a small geographical range can exploit an open wireless access point. Thus the exposure is low with an open wireless access point, and the risks with having an open wireless network are small. However, one should be aware that an open wireless router will give access to the local network, often including access to file shares and printers.
- ✓ The only way to keep communication truly secure is to use end-to-end encryption. For example, when accessing an internet bank, one would almost always use strong encryption from the web

browser and all the way to the bank - thus it shouldn't be risky to do banking over an unencrypted wireless network. The argument is that anyone can sniff the traffic applies to wired networks too, where system administrators and possible hackers have access to the links and can read the traffic. Also, anyone knowing the keys for an encrypted wireless network can gain access to the data being transferred over the network.

- ✓ If services like file shares, access to printers etc. are available on the local net, it is advisable to have authentication (i.e. by password) for accessing it (one should never assume that the private network is not accessible from the outside). Correctly set up, it should be safe to allow access to the local network to outsiders.
- ✓ With the most popular encryption algorithms today, a sniffer will usually be able to compute the network key in a few minutes.
- ✓ It is very common to pay a fixed monthly fee for the Internet connection, and not for the traffic - thus extra traffic will not be detrimental.
- ✓ Where Internet connections are plentiful and cheap, freeloaders will seldom be a prominent nuisance.
- ✓ On the other hand, in some countries including Germany, [38] persons providing an open access point may be made (partially) liable for any illegal activity conducted via this access point. Also, many contracts with ISPs specify that the connection may not be shared with other persons.

Cite this article as :

Sachin Kumar, "Wireless Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 87-99, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194716

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Cloud Security Mechanism : Prevent Access with Location

Prof. Prashant D. Londhe
Department of Computer Science, Gogate-Jogalekar College, Ratnagiri, Maharashtra, India

ABSTRACT

Cloud Services are efficiently used in large organizations and educational sector. Security is major concern whenever anyone is using cloud services and operating system. Cloud Security is highly vulnerable to threats, which results in Data loss. The purpose of this research is to develop Cloud security model. In this paper, we have developed cloud security mechanism with location tracing. We have also analyzed various security mechanisms available and trying to develop a model, which will be least costly and affordable to small organization.
Keywords : Cloud Security, Honeypot, Tonido, Security, Location Tracing.

I. INTRODUCTION

Many Industries, organizations and Individual person uses Cloud as Data storage mechanism in increasing way. High scale Company also do not store the data on own servers, they choose cloud Storage considering reliability. Due to this Cloud security becomes important security aspects due to confidential information and responsive data[4]. Cloud computing is very emerging computer science mechanism which provides computing services and data storage at very effective cost. This cost is quite acceptable and affordable consider metrics provided by parent cloud organization[1]. High availability, Cost saving feature and High scalability makes cloud services more favorite to use. There are three types of Service model used in Cloud architecture[2].

1) **IaaS (Infrastructure as a Service)** : Users get resources like CPU time, Processing power, Network Bandwidth and storage. After registering service user can treat is as its own machine having desired Operating System[2].

2) **PaaS (Platform as a Service)** : Users get resources like Hardware infrastructure and Networking environment. Many Large Scale organization uses this system as base of development[6].
3) **SaaS (Software as a Service)** : Users get access to application without any restriction on operating system, Network Bandwidth and Environment[5].

Figure 1 : Cloud Architecture

Characteristics of Cloud Architecture is as below[7]:-

1) **Scalability:-** Architecture changes according to demand of the application. If need is less it will take less space and high in case of higher with a single click.
2) **Cost-effectiveness:-** Cloud computing reduces hardware expenses, as hardware is provided by a vendor without any need of buying ,installing, configuring and maintaining server.
3) **Immediate availability:-** This applications are immediately available.
4) **Performance:-** Application are of high caliber providing proper output.
5) **Security:-** Cloud infrastructure is kept in safe data centers to ensure security with data back-up and recovery.

II. INTRUSION DETECTION SYSTEM

An Intrusion detection system (IDS) monitors cloud network traffic for abnormal, suspicious transaction, activities and provides alert messages if discovered. This prevents system form malicious activity or traffic which can be dangerous to server. It eventually blocks the activity in seek of security[6].

IDS are mainly developed to block intrusion detection but they are highly prone to false alarms. Therefore developer needs to set and configure IDS properly[14,18].

Different types of intrusion detection systems:-

A **Network intrusion detection system (NIDS)** is developed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network[18].

Host intrusion detection systems (HIDS) run on all computers or devices in the network with direct access to both the internet and the enterprise internal network. HIDS have an advantage over NIDS in that they may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to detect. HIDS may also be able to identify malicious traffic that originates from the host itself, as when the host has been infected with malware and is attempting to spread to other systems[18].

Signature-based intrusion detection systems monitor all the packets traversing the network and compares them against a database of signatures or attributes of known malicious threats, much like antivirus software[20,21]

Anomaly-based intrusion detection systems monitor network traffic and compare it against an established baseline, to determine what is considered normal for the network with respect to bandwidth, protocols, ports and other devices. This type of IDS alerts administrators to potentially malicious activity[12].

Historically, intrusion detection systems were categorized as passive or active; a passive IDS that detected malicious activity would generate alert or log entries, but would take no actions. An active IDS, sometimes called an intrusion detection and prevention system, would generate alerts and log entries, but could also be configured to take actions, like blocking IP addresses or shutting down access to restricted resources[13].

Snort, one of the most widely used intrusion detection systems is an open source, freely available and lightweight NIDS that is used to detect emerging threats. Snort can be compiled on most Unix or Linux operating systems, and a version is available for Windows as well[15].

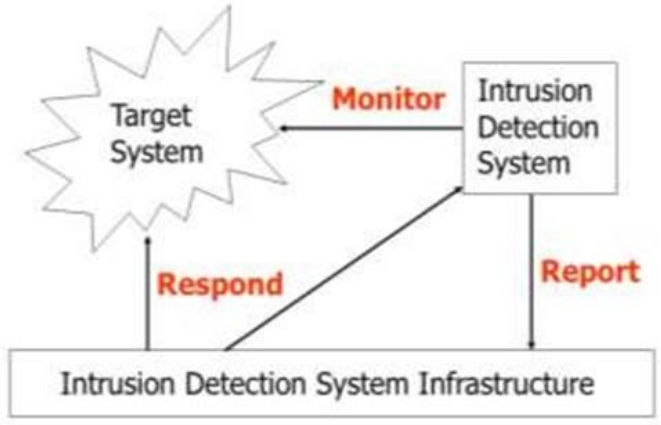


Figure 2: Intrusion Detection System Infrastructure

Capabilities of Intrusion detection systems:-

Intrusion detection systems monitor network traffic in order to detect when an intrusion is being carried out by unauthorized entities. IDSes do this by providing some or all of these functions to security professionals[15]. monitoring the operation of routers, firewalls, key management servers and files that are needed by other security controls aimed at detecting, preventing or recovering from cyberattacks[16]. providing administrators a way to tune, organize and understand relevant operating system audit trails and other logs that are often otherwise difficult to track or parse[20]. including an extensive attack signature database against which information from the system can be matched[15].recognizing and reporting when the IDS detects that data files have been altered; generating an alarm and notifying that security has been breached; and reacting to intruders by blocking them or blocking the server[11].

An intrusion detection system may be implemented as a software application running on customer hardware, or as a network security appliance; cloud-based intrusion detection systems are also available to protect data and systems in cloud deployments[10].

Benefits of intrusion detection systems

Intrusion detection systems offer ability to identify security incidents. An IDS can be used to help analyze the quantity and types of attacks, and organizations can use this information to change their security systems or implement more effective controls. An intrusion detection system can also help companies identify bugs or problems with their network device configurations. These metrics can then be used to assess future risks[3,4].

Intrusion detection systems can also help the enterprise attain regulatory compliance. An IDS gives companies greater visibility across their networks, making it easier to meet security regulations. Additionally, businesses can use their IDS logs as part of the documentation to show they are meeting certain compliance requirements[1].

Intrusion detection systems can also improve security response. Since IDS sensors can detect network hosts and devices, they can also be used to inspect data within the network packets, as well as identify the operating systems of services being used. Using an IDS to collect this information can be much more efficient that manual censuses of connected systems[12].

III. RELATED WORK

Many research works is carried out considering Intrusion detection system. [8] represents intrusion detection based on regression models deciding the security features and load balancing monitoring techniques to maintain specific trust level. Paper [1] represents security features required to maintain trust in cloud system. A new security framework is defined based on Genetic algorithm. Author [9] states different strategically issues in cloud computing services regarding to security suggesting solutions. There are many ways to migrate cloud data securely in IaaS [2]. In [10] different Cloud Security threats are explained and discussed accordingly. Identify and Authentication management specifically focuses on secure access in cloud system with having proper

authority and privileges. The Markovian process algebra PEPA is used to evaluate the models behavior under different scenarios [5]. The multilevel classification model leads to the provision of dynamic security contract for each cloud layer that dynamically decides about security requirements for cloud consumer and provider[5,6]. In paper[10,19], risk factors and solutions regarding these technologies are reviewed then current and future trends are discussed. This paper studies the modeling and analysis methods of some key problems of data security in cloud storage, such as encryption storage, integrity verification, access control, and verification and so on[12]. The simulation carried in [13] results demonstrate that the use of Support Vector Machines (SVM) is an efficient concept for simultaneous image segmentation and data protection.

IV. METHODOLOGY

1) Intrusion detection with mobile agents:

This method mainly focuses on device to device interconnecting security. It correlate on suspicious transactions in different monitored host. These agents are autonomous, goal-driven, reactive, social , adaptive and movable. IDS –AM-CLUST is defined in Java Agent Development (Version 3.7) and JDK 7 has following network traffic process[17].

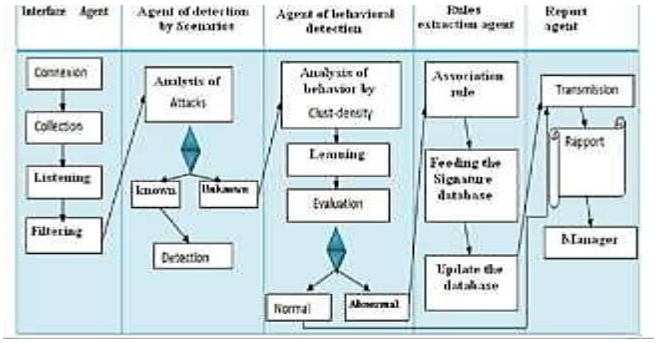


Figure 3 : IDS Architecture

2) Honeycomb :- Honeycomb is a pattern detection engine that monitors any network traffic that Honeyd receives and creates NIDS signatures for any patterns that occur regularly [5]. It is assumed that any regular traffic that Honeyd receives is malicious in nature, as honeypots in general serve no other network purpose and should not be receiving valid traffic. The advantages to use Honeycomb include reducing overhead caused by using additional programs to perform the same task and it is integrated into Honeyd hence will not have any synchronization issues. Additionally the creation of NIDS signatures could be very useful for detecting very new automated mobile malware and integrating the signatures into Network Intrusion Detection Systems on wireless networks to track the spread and effect of such malware [17].

3) Honeynet :- Honeynet is high interaction honeypot. Data capture, Data control and Data analysis are main three component of Honeynet. Data capturing is nothing but monitoring and capturing all activities regarding to cloud services. Data control checks possibility of attacker in cloud services. Data analysis is used to analysed retrieved information which will be responsible for detection of malicious attack.

V. EXPERIMENTAL SETUP & RESULT DISCUSSION

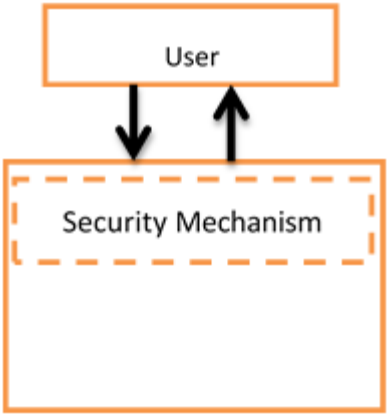


Figure 4: Proposed Model

In Figure we are proposing model for cloud security Where we are implementing security

part in cloud server itself. We are developing a private cloud server with Tonido Interface which provides free cloud architecture for Server as well as client (Computer or Mobile).

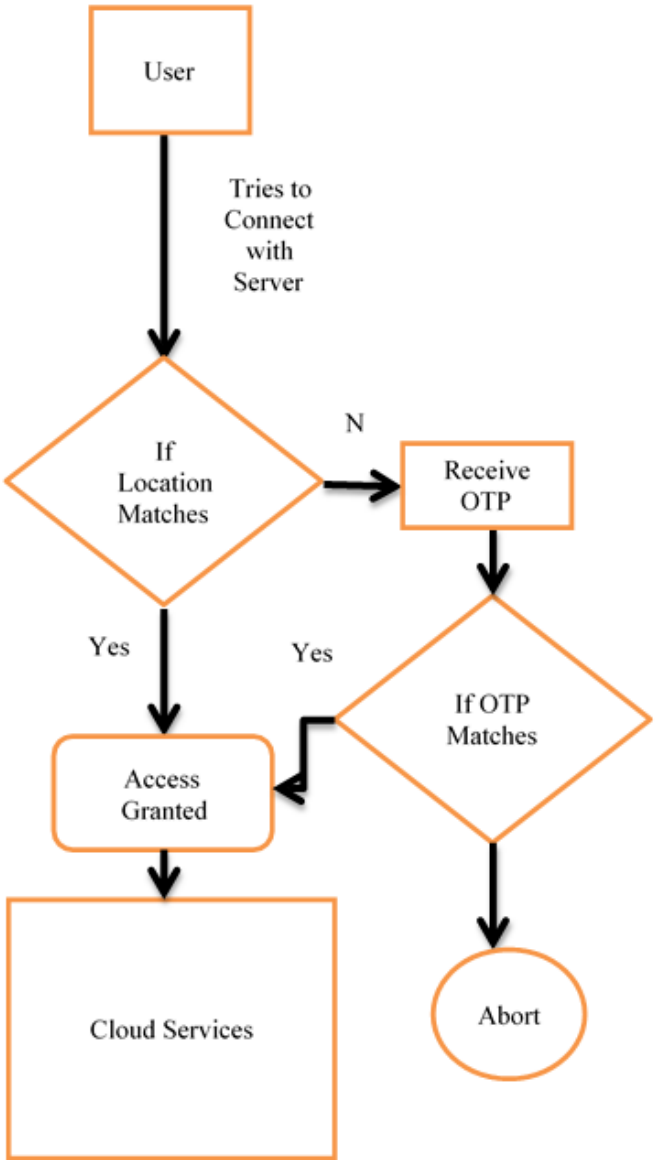


Figure 5 : System Flow of Proposed Model

The Experimental Setup is done with computer having following configuration

1) **Client Machine:-** Pentium Core2 Duo, 500 GB HDD, 4 GB RAM, Window 7 OS
2) **Server Machine:-** Pentium Core I5, 1 Tb HDD,8 GB RAM, Window 7 OS

Setup provides URL to access the server Machine. https://pdlpdlpdl.tonidoid.com is url for cloud server.

Currently we are considering location blockage to prevent unauthorized access to the application. The current location is recorded while logging from the person and if it is found different it is blocked by server otherwise allowed. False alarm is generated when authorized user tries to login from different location. In such case user will receive SMS to registered mobile and after submitting OTP user will be able to login to specified account.

VI. CONCLUSION

In this paper we are trying to avoid unauthorized access to cloud server developed based on Location tracing. We found it as one of the innovative and easiest way of implementing security mechanism. False alarm may arises when an authorized user is trying to login from the different location but it can be solved with OTP received. Still pros and cons are there like everything depends location at now case still there is chance of improvement.

VII. REFERENCES

[1]. Mall, S., & Saroj, S. K. (2018). A new security framework for cloud data. Procedia Computer Science, 143, 765–775. https: //doi.org/10.1016/j.procs.2018.10.397

[2]. Chawki, E. B., Ahmed, A., & Zakariae, T. (2018). IaaS Cloud Model Security Issues on Behalf Cloud Provider and User Security Behaviors. Procedia Computer Science, 134, 328–333. https://doi.org/10.1016/j.procs.2018.07.180

[3]. Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (2016). A Cooperative and Hybrid Network Intrusion Detection Framework in Cloud Computing Based on Snort and Optimized Back Propagation Neural Network. Procedia Computer Science, 83, 1200–1206. https://doi.org/10.1016/j.procs.2016.04.249

[4]. Ghosh, P., Saha, A., & Phadikar, S. (2016). Penalty- Reward Based Instance Selection Method in Cloud Environment Using the Concept of Nearest Neighbor. Procedia Computer Science, 89, 82–89. https://doi.org/10.1016/j.procs.2016.06.012

[5]. Hussain, S. A., Fatima, M., Saeed, A., Raza, I., & Shahzad, R. K. (2017). Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics, 13(1), 57–65. https://doi.org/10.1016/j.aci.2016.03.001

[6]. Idhammad, M., Afdel, K., & Belouch, M. (2018). Distributed intrusion detection system for cloud environments based on data mining techniques. Procedia Computer Science, 127, 35–41. https://doi.org/10.1016/j.procs.2018.01.095

[7]. Kamil, S. N. S., & Thomas, N. (2018). Investigating the Cost of Transfer Delay on the Performance of Security in Cloud Computing. Electronic Notes in Theoretical Computer Science, 337, 105–117. https://doi.org/10.1016/j.entcs.2018.03.036

[8]. Khan, N., & Al-Yasiri, A. (2016). Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework. Procedia Computer Science, 94, 485–490. https://doi.org/10.1016/j.procs.2016.08.075

[9]. Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud

[10]. Computing. Procedia Computer Science, 125(2009), 691–697. https://doi.org/10.1016/j.procs.2017.12.089

[11]. Majhi, S. K., & Dhal, S. K. (2016). Placement of Security Devices in Cloud Data Centre Network: Analysis and Implementation. Physics Procedia, 78(December 2015), 33–39. https://doi.org/10.1016/j.procs.2016.02.007

[12]. Mall, S., & Saroj, S. K. (2018). A new security framework for cloud data. Procedia Computer Science, 143, 765–775. https://doi.org/10.1016/j.procs.2018.10.397

[13]. Manogaran, G., Thota, C., & Kumar, M. V. (2016). MetaCloudDataStorage Architecture for Big Data Security in Cloud Computing. Procedia Computer Science, 87, 128–133. https://doi.org/10.1016/j.procs.2016.05.138

[14]. Marwan, M., Kartit, A., & Ouahmane, H. (2018). Security enhancement in healthcare cloud using machine learning. Procedia Computer Science, 127, 388–397. https://doi.org/10.1016/j.procs.2018.01.136

[15]. Mazini, M., Shirazi, B., & Mahdavi, I. (2018). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. Journal of King Saud University Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2018.03.011

[16]. Prasad, V. K., Shah, M., Patel, N., & Bhavsar, M. (2018). Inspection of Trust Based Cloud Using Security and Capacity Management at an IaaS Level. Procedia Computer Science, 132(Iccids), 1280–1289. https://doi.org/10.1016/j.procs.2018.05.044

[17]. Saadi, C., & Chaoui, H. (2016). Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb. Procedia Computer Science, 85(Cms), 433–442. https://doi.org/10.1016/j.procs.2016.05.189

[18]. Saadi, C., & Chaoui, H. (2016). Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb. Procedia Computer Science, 85(Cms), 433–442. https://doi.org/10.1016/j.procs.2016.05.189

[19]. Saeed, A., Ahmadinia, A., Javed, A., & Larijani, H. (2016). Random neural network based intelligent intrusion detection for wireless sensor networks. Procedia Computer Science, 80, 2372–2376. https://doi.org/10.1016/j.procs.2016.05.453

[20]. Sahmim, S., & Gharsellaoui, H. (2017). Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of

Things: A review. Procedia Computer Science, 112, 1516–1522. https://doi.org/10.1016/j.procs.2017.08.050

[21]. Sharma, D. H., Dhote, C. A., & Potey, M. M. (2016). Identity and Access Management as Security- as-a-Service from Clouds. Procedia Computer Science, 79, 170–174. https://doi.org/10.1016/j.procs.2016.03.117

[22]. Wang, R. (2017). Research on Data Security Technology Based on Cloud Storage. Procedia Engineering, 174, 1340–1355. https://doi.org/10.1016/j.proeng.2017.01.286

Cite this article as :

Sh

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Cloud Security Issues and Implications

Shruthi M G
Assistant Professor, Maharani Lakshmi Ammani College for Women, Bengaluru, Karnataka, India

ABSTRACT

In the recent days the data security is a big issue. Cloud security is one of the most prominent tasks for data security. Cloud security is mainly used for protection of data that has been stored in cloud from theft, leakage and unauthorized access. Different methods have been adopted for cloud security like tokenization, Virtual private network, Firewalls, obfuscation and avoiding public internet connections. Many threats to cloud security has been raised like account hijacking, data hijacking, service traffic hijacking, Application Programming interfaces in-security which leads to duplication of data in different fields and insecure way of data life. In Companies security of data has become a major issue where huge amount of data is stored in cloud and protection of these data is been high challenge. Many threats to cloud security has been raised like account hijacking, data hijacking, service traffic hijacking, Application Programming interfaces in-security which leads to duplication of data in different fields and insecure way of data life. In focus is mainly on Cloud security issues and the different ways of implications on these issues. An incredible increase in hacking of data leads to less productivity to application users, Companies etc. By applying different methods, the main aspect of security of data is been done. Some of the risks have been raised by "Week Cloud Security" is also discussed.

Keywords : Cloud Security, Cloud Threats, Data hijacking, intellectual property, Compliance violation.

I. INTRODUCTION

Cloud Security is the data securing from unauthorized theft, duplication and deletion. Cloud security is very essential for safe guarding data for many users and company's confidentiality. Security of data is most prominent than cloud itself, as cloud users need to protect the access to the cloud as access may be gained using other devices like mobile phones, tab etc.

Cloud security is also known as Cloud computing security as it contains a set of policies, controls, procedures and technologies which is going to protect cloud system entirely along with data and also infrastructure.

II. LITERATURE SURVEY

In recent days the survey about hijacking of data, different applications have become very crucial.
Xiaodong Lin, Xiahui Liang, Shen have proposed the new way of security model for the data forensics and also for the examining cloud computing. Mainly to provide privacy and security of huge data that has been stored in the cloud.

Amazon has provided Infrastructure Security also called as Amazon Web Services (AWS) by providing capabilities and services to increase privacy and to control network access. Wenchao has presented in his paper alternative perspective and also proposed data centric about Cloud security. They also guided security properties mainly to secure data sharing

among the applications hosted on Clouds. Also, have discussed different ways of data management issues to process the query, Forensic as well as system analysis and query correction guaranteed. The proposal of new security platform to perform Cloud computing, it was named as Declarative Secure Distributed Systems.

III. Issues and Implications

Issue 1: Loss of intellectual property Many companies increasingly store the sensitive data in the cloud. Cyber criminals gain access to this sensitive data as 21% of files are sensitive data. Absence of breach and certain services can pose a risk by claiming ownership of the data uploaded.

Issue 2: Compliance violations and regulatory actions Most companies are operating some kid of regulatory controls for their information including government and industry issues. BYOC (Bring Your Own Computer) often violates these tenets by putting the company in a state of non-compliance which leads to serious problems.

Issue 3: Loss of control over end user actions Companies using cloud services, employees working may be doing work without noticing until it's too late. For instance, a salesperson who is about to resign from the company could download a report of all customer contacts, upload the data to a personal cloud storage service, and then access that information once she is employed by a competitor.

Issue 4: Malware infections that unleash a targeted attack Cloud security services are used as a vector of data ex-filtration. Skyhigh uncovered a novel data ex-filtration when the attackers loaded sensitive data into video files and also uploaded the videos online they detected malware that ex-filtrates sensitive data using a private Twitter account 140 characters at a time cyber criminal used file sharing services to deliver the malware to targets using phishing attacks.

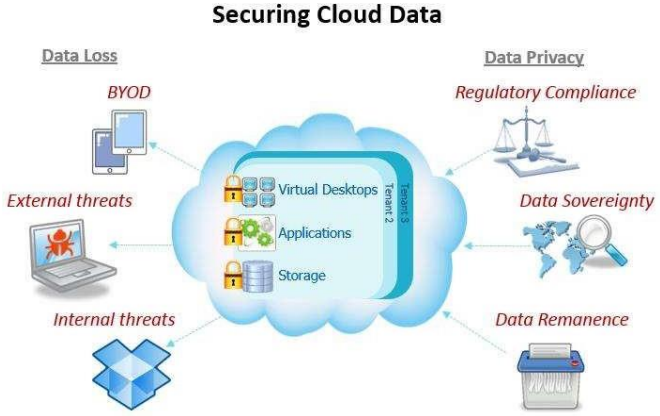
Issue 5: Contractual breaches with customers or business partners Contracts among business parties often restrict how data is used and who is authorized to access it. Consider the example of a cloud service that maintains the right to share all data uploaded to the service with third parties in its terms and conditions, thereby breaching a confidentiality agreement the company made with a business partner.

Issue 6: Diminished customer trust Data breaches inevitably result in diminished trust by customers. Cyber criminals stole over 40 million customer credit and debit card numbers from Target.

Issue 7: Data breach requiring disclosure and notification to victims The company may be required to disclose the breach and send notifications to potential victims. Certain regulations such as HIPAA and HITECH the healthcare industry and the EU Data Protection Directive require these disclosures.

Issue 8: Increased customer churn If customers even suspect that their data is not fully protected by enterprise-grade security controls, they may take their business elsewhere to a company they can trust.

Issue 9: Revenue losses News of the Target data breach made headlines and many consumers stayed away from Target stores over the busy holiday season, leading to a 46% drop in the company's quarterly profit.



IV. Measures taken for Cloud Security

To ensure you put in place proper security measures when beginning your cloud venture, here are five actions every small business owner should take.

1. Creation of unique usernames and passwords: Login credentials represent one of the cloud's main security vulnerability.
2. Usage of industry standard encryption and authentication protocols: IP sec (Internet Protocol Security) is a reliable technology choice.
3. Encryption of data before uploaded to the cloud: Once data is ready hide the data by encryption and only decrypt when reached the destination.
4. Checking IT providers what cloud security policies have been adopted: The most important security measure that can be adopted by finding a trusted IT person and also have signed cloud security policies.
5. Physical cloud server address know: Some cloud servers may be in different locations wherever they are, it's wise to make sure they're located in a safe data center area with proper security afforded to them.

V. CONCLUSION

The biggest cloud security challenge is the sharing of resources. Level of security should be given the most importance prominence.

In this paper I have highlighted the issues and implications of security when data stored in cloud. As Amazon had adopted new cloud security measures need to be developed and implemented in further days.

VI. REFERENCES

[1]. Hassan Takabi.et.al.(2010). "Security and Privacy Challenges in Cloud Computing Environments". IEEE security and privacy. w ww.computer.org/security.

[2]. Rongxing Lu. et.al (2010). "Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing". ASIACCS '10 Proceedings of the 5th ACM Symposium on Information. Computer and Communications Security. pp. 282-292.

[3]. Shuai Z; Shufen Z; Xuebin C; Xiuzhen H; (2010), "Cloud Computing Research and Development Trend", 2nd International conference on Future Networks, 2010. ICFN ' 10. pp 23, 22-24 Jan 2010.

[4]. Basit Ali; (2009), "Ufone Launches Uconnect", published in TelecomPK.Net,12 August 2009.

[5]. Xue J; Zhang J.J; (2010),"A Brief Survey on the Security Model of Cloud Computing",2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science.

Cite this article as :

Shruthi M G, "Cloud Security Issues and Implications", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 107-109, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194718

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

A Review Blockchain

Nitin S Avanthkar, J Dhanush Panalkar
IIFA Lancaster Degree College, Bangalore University, Bangalore, Karnataka, India

ABSTRACT

Begun in the beginning of January 2009, the blockchain technology got oriented in the world and created one of the historical change into what we call network and cyber security till this day. With every block being solved, the computing power to solve the next block of the chain requires exponentially higher power than the previous block.

Keywords : Blockchain, Computing Power

I. INTRODUCTION

Blockchain technology enables decentralised transactions between two people or nodes in general, wherein there is no involvement of a central authority that governs it. The reason behind it's vast success in the past decade is that when a transaction is made under blockchain technology, such as a cryptocurrency transaction, typically a Bitcoin transaction, a verification is to be made for each and every transaction and must be accepted by all clients involved in the transaction, making it secure and unhackable.

Cryptocurrency:- Ever since the rise in the prices and popularity of Bitcoin, people have always kept an eye towards it, may it be seriously or as a side look. The main concept used here is of cryptocurrencies, which is a form of digital cash or credit transactions. Since Bitcoin was the first to be developed, it is widely recognised. Today there are more than a thousand varieties of cryptocurrencies.

Encryption:- Encryption or encrypting information is known as the hiding or capsuling of information so that no one can view it without the right code or password. This helps in keeping sensitive information safe, both online and offline.

Nodes:- The blockchain today is formed by a network of various computers irrespective of their location in the world. These computers are otherwise called as nodes.

Hash:- Hashes are what give the cryptocurrencies their value. The power of mining cryptocurrencies from their block requires power and it is called hash power. Blocks are otherwise called the digital records stored in the chain of network.

In the modern fast moving world, the man requires two factors in any of the things that they look at, reliability and quality. Expense is also a factor which comes after the above mentioned ones but is eradicated due to the requirements and the credibility of people. Under such circumstances, development takes place at a faster pace than usual with no hindrances setting them back.

Blockchain is one of those technologies which is decentralised, meaning that there is no particular authority controlling it. Everybody is their own boss

until the inflow of cash does not stop. Also, the risks come at their own costs. Developing a technology also means that we must find a appropriate security to withstand the current quality.

The brainchild of blockchain is known by the pseudonym, Satoshi Nakamoto. It records everything that is of any value virtually. Also the transactions made under this do not have any hidden charges. They are visible to everybody across the world who still are defied from being able to do anything about it.

Multiple computers are used as nodes from all across the world in order to multiply the hash power acquired to improve the speed of the mining of cryptocurrencies. These currencies are later utilised to transact all across the world. Certain blockchain technologies, such as DASH (name of a cryptocurrency), are also used so that there is complete anonymity of the transaction that you make. The future of blockchain technology lies majorly into two fields:-

Banking

Modern banking technologies lack the required security such as vulnerability to password hackers, and in certain countries such as the USA, the popular AMEx cards do not have an OTP (one time password) security system. They depend upon trust and casualties are frequent, with the modern carding (cracking credit cards) technology has come up.

Ethical hacking and Social networking

With the increase in your profile to the outer world, exploitation is a common threat. A minute (incredibly small) upgrade in the hacker's network needs an exponentially higher securing systems and software development to counter in order to prevent the wrong happenings. While blockchain is mainly financial, peer-to-peer networking is very crucial in this field. The word blockchain itself is just as impossible to hack, by which it means that developing a technology to penetrate the walls of blockchain is an absolute dream as of today. They use a cryptographic fingerprint unique to each block.

While it's yet to be put into a full fledged use, considering the options for dependability on blockchain technology is higher. The ratio of risk to reward is way higher than what humans rely upon this day on antivirus softwares, automated testings and many similar defence systems. When human error comes into play or an insider manipulates information or systems in the supply chain, the blockchain could resolve issues by automatically sharing any suspicious activity down the line.

Vulnerability is often an issue in any networking sector. Blockchain fulfills the requirement by encrypting the data, where you have no particular access to any document on the network without a proper access code.

With all these factors to consider, blockchain is a promising technology for the future which is believed to achieve wonders when placed in the right hands. It lies in the future to accumulate the resources and comprehensively understand the technical and oriental usage of it.

Cite this article as :

Nitin S Avanthkar, J Dhanush Panalkar, "A Review Blockchain", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 110-111, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194719

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Li-Fi (Light-Fidelity) Technology: The Future of 5G Wireless Communication

Mr. Pramod BN
Atria Institute of Technology, Bengaluru, Karnataka, India

ABSTRACT

Light Fidelity (Li-Fi) is a technology which is used for fast data communication through fast blinking of light which can't be observer by human eye. This technology is a better substitute among all the existing wireless communication. Li-Fi is a subset of Optical Wireless Communication (OWC) and RF communication which produces the data at the rate of more than 10 MHz/Sec. Li-Fi technology is the 5th generation of wireless communication technology.

Keywords : Li-Fi, OWC, VLC

I. INTRODUCTION

Light Fidelity (Li-Fi) technology is a wireless communication system based on the use of visible light between the violet (800 THz) and red (400 THz). Unlike Wi-Fi which uses the radio part of the electromagnetic spectrum, Li-Fi uses the optical spectrum i.e. Visible light part of the electromagnetic spectrum. The principle of Li-Fi is based on sending data by amplitude modulation of the light source in a well-defined and standardized way. LEDs can be switched on and off faster than the human eyes can detect since the operating speed of LEDs is less than 1 microsecond. This invisible on-off activity enables data transmission using binary codes. If the LED is on, a digital '1' is transmitted and if the LED is off, a digital '0' is transmitted. Also these LEDs can be switched on and off very quickly which gives us a very nice opportunity for transmitting data through LED lights, because there are no interfering light frequencies like that of the radio frequencies in Wi- Fi. Li-Fi is thought to be 80% more efficient, which means it can reach speeds of up to 1Gbps and even beyond. Li-Fi differs from fiber optic because the Li- Fi protocol layers are suitable for wireless communication over short distances (up to 10 meters).

This puts Li-Fi in a unique position of extremely fast wireless communication over short distances.

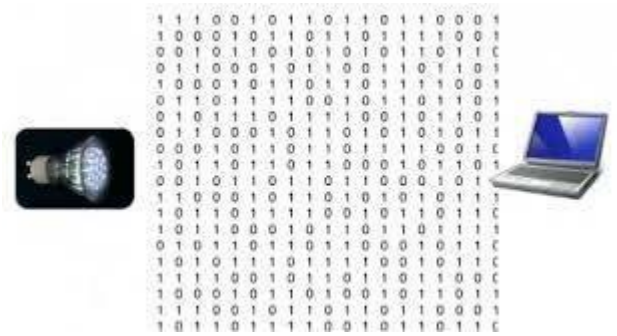


Fig 1.

II. Working of Li-Fi

The working of Li-Fi is very simple. There is a light emitter on one end i.e. an LED transmitter, and a photo detector (light sensor) on the other. The data input to the LED transmitter is encoded in to the light (technically referred to as Visible Light Communication) by varying the flickering rate at which the LEDs flicker 'on' and 'off' to generate

different strings of 1s and 0s. The on-off activity of the LED transmitter which seems to be invisible (The LED intensity is modulated so rapidly that human eye cannot notice, so the light of the LED appears constant to humans), enables data transmission in light form in accordance with the incoming binary codes: switching ON a LED is a logical '1', switching it OFF is a logical '0'. By varying the rate at which the LEDs flicker on and off, information can be encoded in the light to different combinations of 1s and 0s.

In a typical setup, the transmitter (LED) is connected to the data network (Internet through the modem) and the receiver (photo detector/light sensor) on the receiving end receives the data as light signal and decodes the information, which is then displayed on the device connected to the receiver. The receiver (photo detector) registers a binary '1' when the transmitter (LED) is ON and a binary '0' when the transmitter (LED) is OFF. Thus flashing the LED numerous times or using an array of LEDs (perhaps of a few different colors) will eventually provide data rates in the range of hundreds of Mbps. The Li-Fi working is explained in a block diagram.

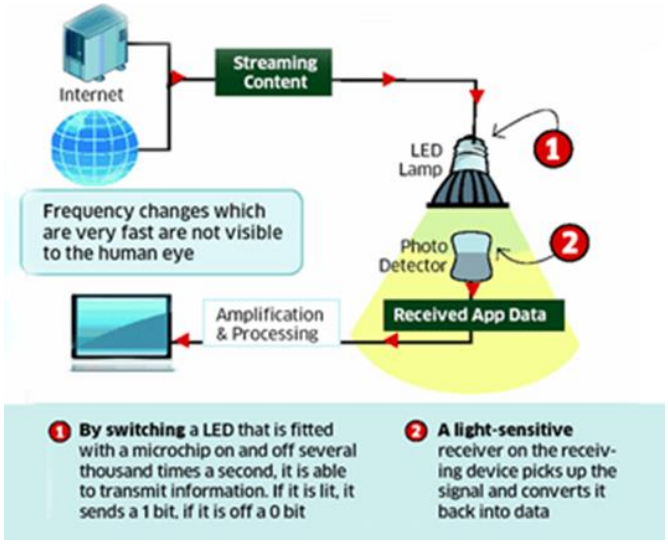


Fig.2: Block diagram of Li-Fi Sub System

Hence all that is required, is some or an array of LEDs and a controller that controls/encodes data into those LEDs. All one has to do is to vary the rate at which the LEDs flicker depending upon the data input to LEDs. Further data rate enhancements can be made in this method, by using array of the LEDs for parallel data transmission, or using mixtures of red, green and blue LEDs to alter the light's frequency, with each frequency encoding a different data channel. Figure 3 shows working/deployment of a Li- Fi system connecting the devices in a room.

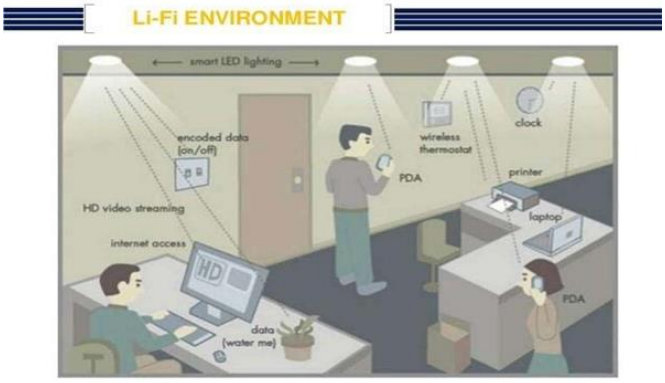


Fig 3: Li-Fi system connecting devices in a room

III. Why Visible Light Communication

The frequency spectrum that is available to us in the atmosphere consists of many wave regions like X- rays, gamma rays, u-v region, infrared region, visible light rays, radio waves, etc. Any one of the above waves can be used in the upcoming communication technologies but why the Visible Light part is chosen? The reason behind this is the easy availability and lesser harmful effects that occur due to these rays of light. VLC uses the visible light between 400 THz (780 nm) and 800 THz (375 nm) as medium which are less dangerous for high-power applications and also humans can easily perceive it and protect themselves from the harmful effects whereas the other wave regions have following disadvantages:

- ✓ Radio waves are expensive (due to spectrum charges) and less secure (due to interference and possible interception etc.).
- ✓ Gamma rays are harmful because it could be dangerous dealing with it, by the human beings

due to their proven adverse effects on human health.

- ✓ X-rays have health issues, similar to the Gamma Rays.
- ✓ Ultraviolet light can be considered for communication technology purposes at place without people, otherwise they can also be dangerous for the human body when exposed continuously.
- ✓ Infrared, due to high safety regulation, can only be used with low power.

Hence the Visible light portion (from red to blue) of the electromagnetic spectrum does not cause any harm to the people as visible rays are safe to use, provide larger bandwidth and also have a promising future in the communication field.

IV.Comparison between Li-Fi and, Wi-Fi and other Radio Communication technologies

Both Wi-Fi and Li-Fi can provide wireless Internet access to users, and both the technologies transmit data over electromagnetic spectrum. Li-Fi is a visible light communication technology useful to obtain high speed wireless communication. The difference is:

Wi-Fi technology uses radio waves for transmission, whereas Li-Fi utilizes light waves. Wi-Fi works well for general wireless coverage within building/campus/compound, and Li-Fi is ideal for high density wireless data coverage inside a confined area or room and is free from interference issues unlike the Wi-Fi. Table I shows a comparison of transfer speed of various wireless technologies. Table II shows a comparison of Li-Fi with Wi-Fi.

Table 1 : Comparison of speed of various wireless technologies

Technology	Speed
Li-Fi	~1 Gbps
Wi-Fi – IEEE 802.11n	~150 Mbps
IrDA	~4 Mbps
Bluetooth	~3 Mbps
NFC	~424 Kbps

Table 2: Comparison of Wi-Fi and Li-Fi

Parameter	Li-Fi	Wi-Fi
Spectrum Used	Visible Light	RF
Standard	IEEE 802.15.7	IEEE 802.11
Range	Based on Light Intensity (<10m)	Based on Radio propagation & interference (<300 m)
Data Transfer Rate	Very high (~1Gbps)	Low (100Mbps-1Gbps)
Power consumption	Low	High
Cost	Low	High
Bandwidth	Unlimited	Limited

V. Advantages of Li-Fi

Li-Fi, which uses visible light to transmit signals wirelessly, is an emerging technology poised to compete with Wi-Fi. Also, Li-Fi removes the limitations that have been put on the user by the Radio wave transmission such as Wi-Fi as explained above vide 4.1. Advantages of Li-Fi technology include:

i. Efficiency: Energy consumption can be minimized with the use of LED illumination which is already available in the home, offices and Mall etc. for lighting purpose. Hence the transmission of data requiring negligible additional power, which makes it very efficient in terms of costs as well as energy.
ii. High speed: Combination of low interference, high bandwidths and high- intensity output, help Li-Fi provide high data rates i.e. 1 Gbps or even beyond.
iii. Availability: Availability is not issues as light sources are present everywhere. Wherever there is a light source, there can be Internet. Light bulbs are present everywhere – in homes, offices, shops, malls

and even planes, which can be used as a medium for the data transmission.

iv. Cheaper: Li-Fi not only requires fewer components for its working, but also uses only a negligible additional power for the data transmission.

v. Security: One main advantage of Li-Fi is security. Since light cannot pass through opaque structures, Li-Fi internet is available only to the users within a confined area and cannot be intercepted and misused, outside the area under operation.

vi. Li-Fi technology has a great scope in future. The extensive growth in the use of LEDs for illumination indeed provides the opportunity to integrate the technology into a plethora of environments and applications.

VI. Limitations of Li-Fi

- ✓ Internet cannot be accessed without a light source. This could limit the locations and situations in which Li-Fi could be used.
- ✓ It requires a near or perfect line-of-sight to transmit data.
- ✓ Opaque obstacles on pathways can affect data transmission.
- ✓ Natural light, sunlight, and normal electric light can affect the data transmission speed.
- ✓ Light waves don't penetrate through walls and so Li-Fi has a much shorter range than Wi-Fi.
- ✓ High initial installation cost, if used to set up a full-fledged data network.

VII. Applications of Li-Fi

There are numerous applications of Li-Fi technology, from public Internet access through existing lighting (LED) to auto-piloted cars that communicate through their headlights (LED based). Applications of Li-Fi can extend in areas where the Wi-Fi technology lacks its presence like aircrafts and hospitals (operation theatres), power plants and various other areas, where electromagnetic (Radio) interference is of great concern for safety and security of equipments and people. Since Li-Fi uses just the light, it can be used safely in such locations or areas. In future with the Li-Fi enhancement all the street lamps can be transformed to Li-Fi connecting points to transfer data. As a result of it, it will be possible to access internet at any public place and street.

Some of the future applications of Li-Fi could be as follows:

a) Education systems: Li-Fi is the latest technology that can provide fastest speed for Internet access. So, it can augment/replace Wi-Fi at educational institutions and at companies so that the people there can make use of Li-Fi with the high speed.

b) Medical Applications: Operation theatres (OTs) do not allow Wi-Fi due to radiation concerns. Usage of Wi-Fi at hospitals interferes/blocks the signals for monitoring equipments. So, it may have hazardous effect to the patient's health, due to improper working of medical apparatus. To overcome this and to make OT tech savvy Li-Fi can be used to access internet and also to control medical equipments. This will be beneficial for conducting robotic surgeries and other automated procedures.

c) Cheaper Internet in Aircrafts: The passengers travelling in aircrafts get access to low speed Internet that too at a very high price. Also Wi-Fi is not used because it may interfere with the navigational systems of the pilots. In aircrafts Li-Fi can be used for data transmission. Li-Fi can easily provide high speed Internet via every light source such as overhead reading bulb, etc. present inside the airplane.

d) Underwater applications: Underwater ROVs (Remotely Operated Vehicles) operate from large cables that supply their power and allow them to receive signals from their pilots above. But the tether used in ROVs is not long enough to allow them to explore larger areas. If their wires were replaced with light — say from a submerged, high-powered lamp — then they would be much freer to explore. They could also use their headlamps to communicate with each other, processing data autonomously and sending their

findings periodically back to the surface. Li-Fi can even work underwater where Wi-Fi fails completely, thereby throwing open endless opportunities for military underwater operations.

e) Disaster management: Li-Fi can be used as a powerful means of communication in times of disaster such as earthquake or hurricanes. The average people may not know the protocols during such disasters. Subway stations and tunnels, common dead zones for most emergency communications, pose no obstruction for Li-Fi.

f) Applications in sensitive areas: Power plants need fast, inter-connected data systems so that demand, grid integrity and core temperature (in case of nuclear power plants) can be monitored. The Radio communication interference is considered to be bad for such sensitive areas surrounding these power plants. Li-Fi can offer safe, abundant connectivity for all areas of these sensitive locations. Also, the pressure on a power plant's own reserves (power consumption for Radio communications deployments) will be lessened.

g) Traffic management: In traffic signals Li-Fi can be used to communicate with passing vehicles (through the LED lights of the cars etc) which can help in managing the traffic in a better manner resulting into smooth flow of traffic and reduction in accident numbers. Also, LED car lights can alert drivers when other vehicles are too close.

h) Mobile Connectivity: Mobiles, laptops, tablets, and other smart phones can easily connect with each other. The short-range network of Li-Fi can yield exceptionally high data rates and higher security.

i) Replacement for other technologies: Li-Fi doesn't work using radio waves. So, it can be easily used in the places where Bluetooth, infrared, Wi-Fi, etc. are banned.

VIII. Future Scope

As light is everywhere and free to use, there is a great scope for the use and evolution of Li-Fi technology. If this technology becomes mature, each Li-Fi bulb can be used to transmit wireless data. As the Li-Fi technology becomes popular, it will lead to a cleaner, greener, safer communications and have a bright future and environment. The concept of Li-Fi is deriving many people as it is free (require no license) and faster means of data transfer. If it evolves faster, people will use this technology more and more.

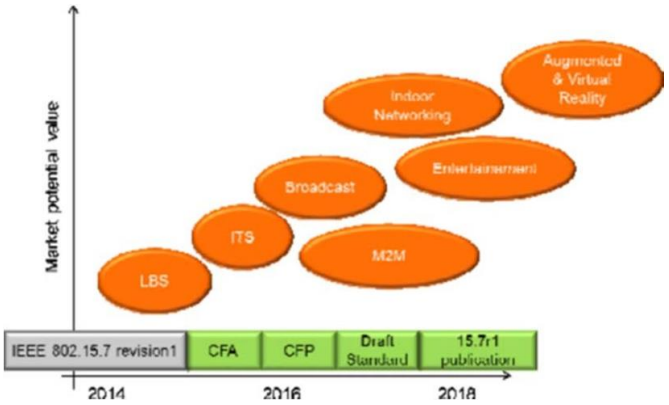


Fig 4: Li-Fi Roadmap

Currently, LBS (location Based Service) or Broadcast solution are commercially available. The next step could be a Li-Fi WLAN for B2B market with high added value on specific business cases and could grow towards mass market. In the long term, the Li-Fi could become an alternative solution to radio for wireless high data rate room connectivity and new adapted service, such as augmented or virtual reality.

IX. Conclusion

Although there's still a long way to go to make this technology a commercial success, it promises a great potential in the field of wireless internet. A significant number of researchers and companies are currently working on this concept, which promises to solve the problem of lack of radio spectrum, space and low internet connection speed. By deployment of this technology, we can migrate to greener, cleaner, safer communication networks. The very concept of Li-Fi promises to solve issues such as, shortage of radio-frequency bandwidth and eliminates the

disadvantages of Radio communication technologies. Li-Fi is the upcoming and growing technology acting as catalyst for various other developing and new inventions/technologies. Therefore, there is certainty of development of future applications of the Li-Fi which can be extended to different platforms and various walks of human life.

X. REFERENCES

[1]. http://www.warse.org/pdfs/2014/icetetssp25.pdf
[2]. http://www.onlinejournal.in/IJIRV2I6/006.pdf
[3]. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnu mb er=6685753
[4]. www.oledcomm.com
[5]. https://www.ijsr.net/archive/v5i9/26051603.pdf
[6]. https://www.ijsr.net/archive/v4i12/NOV151778 .pdf
[7]. http://www.ijsrp.org/research-paper-0416/ijsrp-p5275.pdf
[8]. http://www.ijcta.com/documents/volumes/vol5i ssu e1/ijcta201 4050121.pdf
[9]. http://www.academia.edu/6996573/CSE_Study _P aper_on_._LiFi_Technology_The_latest_techno logy_ in_wireless 13.
[10]. http://www.academia.edu/6770592/Light_Fideli t y_LI-FI_- A_Comprehensive_Study_ 15.

Cite this article as :

Mr. Pramod BN, "Li-Fi (Light-Fidelity) Technology: The Future of 5G Wireless Communication", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 112-117, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194720

National Conference on Communication Technology & Network Security In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Data Reduction Using LZW Algorithm in FOG Computing

Veena. R*, Jyothsna. R
Associate Professor, Department of Computer Science, Seshadripuram College, Bangalore, Karnataka, India

ABSTRACT

Fog Computing is related to the computational architectures located in the network edge. Fog computing is beneficial since it deals with low latency, real-time analytics, improved security and use of wireless access. There is a need to improve the fog services for faster transmission of data , thereby implementation of data reduction techniques will be beneficial for faster transmission of data. In this paper there is a depiction of data compression algorithm called Lempel- Ziv -Welch. With the incorporation of this algorithm data can be compressed and thereby sufficient data can be passed faster in the fog computing network.

Keywords : Lempel- Ziv -Welch , fog , compression , latency and transmission.

I. INTRODUCTION

Fog computing is used in the field of big data analytics and cloud computing since there is a huge demand for accessing the information from the cloud.The fog networking has a data plane and a control plane.With the help of fog computing, the computing services can obtained from the network edge.Therefore fog computing helps in latency reduction and also is useful in tackling the problems associated with bandwidth , thereby faster transmission of data can take place.In order to improve the QoS (Quality of service) a model is proposed, in which we can use the LZW (Lempel-Ziv -Welch) which is a data compression algorithm that can help in quicker transmission of data in the cloud.

II. LITERATURE SURVEY

There is a lot of research work done based on data compression in the edge computing.

Data compression means minimizing the size of huge data. Md. Rubaiyat Hasan proposed an approach by which the data size can be reduced by using the Huffman coding and LZW algorithm . Data compression techniques like lossless and lossy are also considered. Performance of LZW and Huffman algorithms are also studied. The efficiency of compression algorithms are brought about in detail.

A. Alarabeyyat, S. AlHashemi, T. Khdou, M. Hjouj Bus, S. Bani-Ahmad and R. AlHashemi have presented a paper, which describes that the digital image processing techniques requires a huge amount of storage space, thereby they proposed an approach . According to this view point they required to scale back the size of the picture without reducing the quality of the picture for this they use the LZW algorithm.

P.S Nithya Darsini and S. Renugadevi proposed a technique of incorporating the "Huffman coding" , and LZW with arithmetic coding techniques for saving

energy for wireless networks , that use sensors for saving energy.

III. LZW (LEMPEL– ZIV –WELCH)

ALGORITHM

There are two techniques for data compression i.e., lossy and lossless. Lossy compression helps to reduce the bits by removing the unnecessary information. The Lossless compression helps in eliminating the statistical redundancy by reducing the bits. The Lossless compression technique includes LZW (Lempel Ziff Welch) algorithm .

LZW compression is done by reading the sequence of symbols, then later these symbols are grouped into strings and thereafter the strings are converted into codes. This method is followed since the codes require less space than the strings and thereby these the strings are replaced.

LZW ENCODING ALGORITHM

PSEUDOCODE:

Initialize table with the help of single character strings
P1 = is the first input character
WHILE the input stream is not concluded C
1= is the next input character
IF P1 + C1 is in string table
P1 = P1 + C1
ELSE

Output code for P1
add P1 + C1 to string table
P1= C1

END WHILE
output code for P1

LZW DECOMPRESSION ALGORITHM

PSEUDOCODE:

Initialize the table with single character strings
O= first the input code
output the translation of O

WHILE not end of the input stream
N= next input code
IF N is not in string table
S = translation of O
S = S + C
ELSE

IV. PROPOSED MODEL

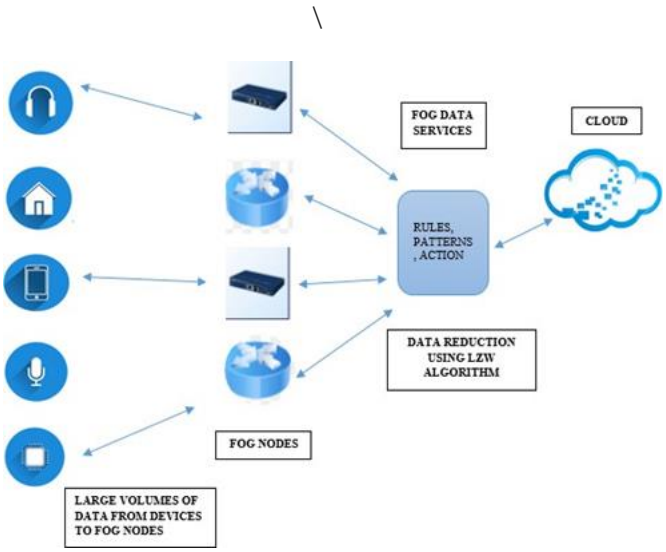


Fig 1: Data reduction using LZW Algorithm in Fog computing architecture

Fog computing was originally coined by Cisco with respect to edge computing. Compared to edge computing, the fog computing platforms are described as dense computational architectures at the edge of the network. The main characteristics of the fog platforms is that they have low latency rate and uses wireless access.

The fog computing involves many types of analytics such as transactional analytics, medium latency real-time analytics, low latency real-time analytics. According to the model, large volumes of data is

transmitted from the devices to the fog nodes. Later in the fog nodes ,there are some of the fog services, this requires large amount of data that needs to be transmitted from the fog nodes to the cloud.

In order to increase the efficiency of the fog, network data reduction must be done. Therefore this can be done that with the help of the LZW algorithm, thereafter the data is sent to the cloud. Using the LZW algorithm the encoding and the decoding of the data is done, thereby the faster analytics takes place between the fog nodes and the cloud.

V. CONCLUSION

According to the proposed model the data reduction is done when the data is transmitted between the fog nodes and the cloud, to increase the efficiency of the fog network we use the LZW algorithm since it helps in data compression by encoding the data and later decoding the data. Although the LZW algorithm is proven to be a very successful algorithm there are many other algorithms like Huffman coding, discrete cosine transform techniques that can be implemented to improve the efficiency of the model.

VI. REFERENCES

[1]. "Md. Rubaiyat Hasan", "Data Compression using Huffman based LZW Encoding Technique", IJSR, Nov 2011.

[2]. "A. Alarabeyyat, S. Al-Hashemi, T. Khdou, M. Hjouj Bus, S. Bani-Ahmad, R. Al- Hashemi", "Lossless Image Compression Technique Using Combination Methods", IJSE , Mar.2012.

[3]. "S. Renugadevi and P.S Nithya Darsini", "Huffman and Lempel-Ziv Based Data Compression Algorithm for Wireless Sensor Networks", IEEE (PRIME) February 21-22 2013.

[4]. "B. Nivedha, M. Priyadharshini, E. Thendral, T. Deenadayalan", "Lossless Image Compression in Cloud Computing"2017 International Conference on Technical Advancements in Computers and Communications.

[5]. "Weisong Shi, Fellow IEEE,Jie Cao,Student Member, IEEE, Quan Zhang Student Member, IEEE, Youhuizi Li, and Lanyu Xu "."Edge Computing: Vision and Challenges" IEEE INTERNET OF THINGS JOURNAL, VOL. 3, NO. 5, OCTOBER 2016 637.

[6]. "Hind Bangui 1,2,3,* , Said Rakrak 3 , Said Raghay 3 and Barbora Buhnova 1,2"."Moving to the Edge-Cloud-of-Things: Recent Advances and Future Research Directions" Electronics 2018, 7, 309; doi:10.3390/electronics7110309.

[7]. "Alireza Yazdanpanah and Mahmoud Reza Hashemi", "A New Compression Ratio Prediction Algorithm for Hardware Implementation of LZW Data Compression ", IEEE Computer Society 2010.

[8]. Ibrahim M. El-Hasnony , Hazem M. El Bakry and Ahmed A. Saleh,Comparative Study among Data Reduction Techniques over Classification Accuracy, International Journal of Computer Applications (0975 - 8887) Volume 122 - No.2, July 2015.

[9]. "Simrandeep kaur and V.Sulochana Verma" , Design and Implementation of LZW Data Compression Algorithm, International Journal of Information Sciences and Techniques (IJIST) .

[10]. "ADBULLAH A. , MAO ZHIGANG HUSSAIN", "Study on LZW algorithm for Embedded Instruction Memory", Proceedings of the 5th WSEAS Int. Conf. on Instrumentation, Measurement, Circuits and Systems, Hangzhou, China, April 16-18, 2006 (pp235-239).

[11]. "Shyni K, Manoj Kumar KV","Lossless LZW Data Compression Algorithm on CUDA","IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 1 (Jul. - Aug. 2013), PP 122-127."

Cite this article as :

Veena. R, Jyothsna. R, "Data Reduction Using LZW Algorithm in FOG Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 118-120, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194721

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Review on Cloud Security and Its Risk Over E-Commerce Network

Yamuna P
Assistant Professor, Department of Computer Applications Acharya Institute of Graduate Studies, Soladevanahalli, Karnataka, India

ABSTRACT

Many enterprises and businesses of all sizes take advantage of this subscription-based model in order to reduce IT costs which are often associated with traditional on premise applications. SaaS has been steadily growing over the past decade as many businesses adopt this new model of purchasing IT. The applications are remotely hosted by the service provider and can be accessed on demand by customers over the internet or private networks. This paper mainly focused on the architecture of cloud security; survey of the different security issues that has emanate due to the nature of the service delivery module of cloud system and type of attacks in cloud computing environment.

Keywords : Cloud computing, cloud security, cloud standards, cloud Risk, E-commerce Platform, software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS).

I. INTRODUCTION

Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data and infrastructure. These security measures are configured to protect data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.

The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, implementation of cloud security processes should be a joint responsibility between the business owner and solution provider.

For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.

II. CLOUD SECURITY BENEFITS

- **Centralized security**: Just as cloud computing centralizes applications and data, cloud security centralizes protection. Cloud-based business networks consist of numerous devices and endpoints. Managing these entities centrally enhances traffic analysis and filtering, streamlines

the monitoring of network events and results in fewer software and policy updates

- **Reduced costs**: One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces administrative overheads
- **Reduced Administration**: When you choose a reputable cloud services provider or cloud security platform, you can kiss goodbye to manual security configurations and almost constant security updates. These tasks can have a massive drain on resources, but when you move them to the cloud, all security administration happens in one place and is fully managed on your behalf.
- **Reliability**: Cloud computing services offer the ultimate in dependability. With the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what device they are using.

The Growth of Cloud-Based Applications

The rapid adoption of cloud computing technology in the form of rendered 'cloud services' makes it one of the hottest topics on the minds of IT and ecommerce leaders today. Cloud computing services are often referred to as a 'game-changer' amongst industry pundits, largely due to the opportunity the technology offers in organization-wide collaboration, enterprise-class scalability, and device agnostic availability while providing exceptional cost reduction advantages through optimized and efficient computing.

It is important to distinguish the three cloud computing classifications often referred to as the 'SPI model' where SPI refers to

- **Software as a Service (SaaS)**: offers users access to application software and databases.
- **Platform as a Service (PaaS)**: offers, beyond computing infrastructure, a development environment for application developers (e.g., operating systems, programming language execution environment, databases, etc.).
- **Infrastructure as a Service (IaaS)**: offers basic computing infrastructure (e.g., physical and virtual machines, location, network, backup, etc.).

All of the above SPI cloud service models can be deployed on one of the following four infrastructure deployment models

- Public cloud: the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- Private cloud: the cloud infrastructure is operated solely for a single organization. It may be managed by the organization itself or by a third party and may be located on- premises or off-premises.
- Hybrid cloud: the cloud infrastructure is a combination of two or more clouds (private, community or public).

III. ADOPTION RATES

According to Gartner, the worldwide public cloud services market is projected to grow by 17.3% in 2019 to total $206.2 billion, up from $175.8 billion in 2018.

The growth projections are unevenly spread across SaaS, PaaS, and IaaS.

Infrastructure as a Service (IaaS) is expected to be the fastest-growing cloud services segment with forecasted growth of 27.6% in 2019 to reach $39.5 billion, up from $31 billion in 2018. Amazon is the leading vendor in the IaaS market, followed by Microsoft, Alibaba, Google, and IBM.

3.2 ADOPTION RATES BY VERTICAL.

Many organizations tend to start out with apps that could be easily migrated over to the cloud, and then transition their larger strategic systems such as their ecommerce platform, ERP and supply chain applications. These projects, tend to be integrated into their digital transformation plans.

A survey conducted by The Economist Intelligence Unit revealed the varying rate of cloud adoption across industries.

The first movers to the cloud appear to be digital "pure play" solutions that stand side-by-side with the legacy industry solutions, such as:

- ✓ Digital banking sprouting out of in-person branch banking.
- ✓ Ecommerce stores competing with brick-and-mortar retailers and shopping centers.

IV.CLOUD SECURITY RISK:

As industry trends show the ever-growing popularity and adoption of cloud technology, some organizations still seem hesitant to take the leap.
A Deloitte survey on cloud adoption showed that among a group of CIOs that have yet to implement cloud computing in their organizations, their main objections were:

- ✓ Risk of losing control and governance of data.
- ✓ Legal issues and open compliance.
- ✓ Risk of their data being exposed.
- ✓ Inadequate data security.

From the sub-group of CIOs yet to have adopted cloud technology, 78% of them, revealed that the major reason for non-adoption was their uncertainty in ecommerce security.

"The 'cloud security', is that if an organization stores their data in a third-party data center, they put themselves and their customers at risk of a data breach that will not only damage their organization's reputation but also have significant financial implications in the form loss of business and ultimately lead to penalties or fines."

V. SECURITY LAYERS IN ENTERPRISE SAAS, IAAS AND CLOUD- BASED APPLICATIONS

Cloud-based applications can be primarily categorized into two key layer:

- ✓ Layer 0, the IaaS (Infrastructure as a service) and PaaS (Platform as a service) cloud where everything else runs; typically, Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud, or Alibaba.
- ✓ Layer 1, SaaS and cloud-delivered applications that typically run on Layer 0 IaaS infrastructure.

Each layer has a set of both overlapping and distinct security considerations and standards.

5.1 LAYER 0 IAAS CLOUD SECURITY.

- ✓ The central security principle in all IaaS cloud rendered solutions is the concept of 'shared responsibility', which means two things:

- ✓ IaaS providers are responsible for the security of the cloud (e.g. global infrastructure, storage, databases, networking, and computer).
- ✓ Customers are responsible for security in the cloud (e.g. data, platforms, applications, operating systems, firewalls).

5.2 LAYER 1 SAAS CLOUD SECURITY.

- ✓ Data security should involve the use of strong encryption techniques and fine-grained authorization to control access to data.
- ✓ Achieve regulatory compliance, with the most important being
- ✓ Understand the deployment model of your SaaS vendors (i.e. if they will be using a public cloud vendor or hosting themselves).
- ✓ Availability: around the clock availability of service involves architectural changes at the application and infrastructure levels that add scalability and high availability. A load- balanced farm of application instances, running on a variable number of servers will provide resilience to denial of service attacks as well as hardware and/or software failures.
- ✓ Backups: enterprise data essentially needs to be regularly backed up to facilitate quick recovery in any event of a disaster. Strong encryption schemes need to be applied to all backup data.
- ✓ Credential Synchronization: The SaaS vendor supports replication of user account information and credentials between enterprise and SaaS application. User authentication is carried out by the SaaS vendor end using replicated credentials.

VI. SECURITY COMPLIANCE AUDITING.

Security compliance auditing is an assessment of a cloud services provider (CSP) to security- related requirements. At the very least a CSP should be able to ensure compliance with regulations and standards, as well as deploy their customers' applications and store their data securely. SaaS vendors that provide tenants with credible and trustworthy compliance information at any time hold a significant competitive advantage and are likely more reliable than others in comparison.

6.1 COMPLIANCE STANDARDS IN THE CLOUD.

There are two types of standards when ensuring compliance with different security frameworks in the cloud: vertical and horizontal. The horizontal standards may be applicable to many industries across the board, while the vertical standards are specific to each industry.

VII. BASE LEVEL SECURITY CHECKLIST OF IAAS SECURITY

✓ Asset Protection: Redundancy of IaaS Platforms

IaaS providers should guarantee that the data, and the hardware assets storing or processing it, are protected against physical tampering, loss, damage or seizure.

✓ Physical Security Mechanisms

The IaaS provider should offer an assurance that the data, disk images, and other storage, is appropriately protected – physically, logically or cryptographically. In the event that the organization is not satisfied with the protection provided by the IaaS provider, you should be able to deploy volume encryption of your data stores. Data erasure, sometimes referred to as data clearing or data wiping, allows you to completely destroy all electronic data with a software-based method that uses binary data (ones and zeros) to overwrite the data. You should verify with the IaaS provider where responsibility for erasing data lies

✓ Infrastructure security

Infrastructure security involves firewalls, robust encryption, and user authentication. Some IaaS services may directly expose client infrastructure to

public networks, such as the Internet. To establish infrastructure security, ensure that appropriate firewalls are deployed at both the infrastructure and platform level. Virtual networking can be used to separate management and back-end functionality from interfaces exposed to end-users. In situations where your IaaS provider does not offer granular interface control, virtual network security appliances may be useful. When data is intentionally shared with other users, you should have procedures in place to ensure it does not contain information which could give an attacker access to the service

VIII. CONCULSION

Data and ecommerce security is too important of a responsibility to employ alone. Plus, managing the servers and the teams that protect data can develop into a costly venture for any ecommerce business. Hosted ecommerce platforms are often more secure and don't require a high level of expertise compared to self-hosted software solutions. Each Big Commerce store is protected by multiple layers of security to prevent unauthorized access, including perimeter and server-specific firewalls, file integrity scanners, intrusion detection software, and 24/7 human monitoring. Online store data is also replicated on two data centers at a minimum, with backups hosted at a third site.

All Big Commerce plans offer HTTPS across the entire site. Shoppers can feel comfortable knowing an online store is secure from the first page they visit through the checkout process. Safeguarding data from breaches and managing all aspects of ecommerce security shouldn't strain a business. Big Commerce alleviates the pressure with unmatched security performance

IX. REFERENCES

[1]. Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," Special Publication 800-145, September 2011, pages2—3,http://csrc.nist.gov/publications/nistpubs/800-145/SP800- 145.pdf. Short NIST document defining cloud computing models and services.

[2]. NIST Cloud Computing Reference Architecture," Special Publication 500-292, September 2011,pages15-17,http://collaborate.nist.gov/twiki_090611.pdf NIST document describing security expectations in a cloud computing environment. 3 By John Panagulias, "Cloud Computing: Platform as a Service Defined", Wednesday, August 5, 2009, http://cloud.kendallsquare.com/article/cloud-computingplatform-as-a-service-defined

[3]. Ian O'Rourke,"Being Too Glib about Cloud", October, 20012, http://www.elucidateit.net/?p=608

[4]. Defense Engineering, Inc.Partnering Technology with Business Needs, "Cloud Computing, http://www.defenginc.com/solutions/cloud_computing

[5]. Cloud Computing Ireland,"Hybrid Cloud", Nov 2012, http://cloudireland.ie/?page_id=9

[6]. Pradnesh Rane, Persistent System White Paper, "Securing SaaS Applications A cloud security perspective for Application Providers"

[7]. Oracle Wiring through an Enterprise Service Bus, 2009 http://www.oracle.com/technology/tech/soa/masteringsoa-series/part2.html accessed on:19Feb February 2010

[8]. Gajek S, Liao L, Schwenk J. Breaking and fixing the inline approach. In: SWS '07, Proceedings of the ACM workshop on secure web services. New York, NY, USA: ACM; 2007. p. 37-43.

[9]. Descher M, Masser P, Feilhauer T, Tjoa AM, Huemer D. Retaining data control to the client

in infrastructure clouds. In: International conference on avail

Cite this article as :

Yamuna P, "Review on Cloud Security and Its Risk Over E-Commerce Network", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 121-126, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194722

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

On the Role of Finger Scanning in Fully Secured Online Transactions

V. Sarada Swetha[1], S. Ramu[2], U.V. Harika[3], U. V. S. Seshavatharam[4]

[1]HCL technologies, Flat No-304, Sangeeth Nagar, Kukatpally, Hyderabad, Andhra Pradesh, India

[2]SBI cards, Flat No-304, Sangeeth Nagar, Kukatpally, Hyderabad, Andhra Pradesh, India

[3] Department of ECE, S. V. Engineering College for Women, Tirupati, Andhra Pradesh, India

[4]Honorary Faculty, I-SERVE, Survey no-42, Hitech city, Hyderabad, Telangana, India

ABSTRACT

By registering user's smart phone and finger prints in the respective banks and by allowing a suitable decision making timer in online transactions - to the possible extent, online frauds can be minimized. Considering finger prints and virtual card system, online ease and security can be enhanced further.

I. INTRODUCTION

Nowadays, as smart phones are growing in number, day by day banking transaction number is also increasing. Parallel to this, online fraud activities are also increasing in number. To minimize and prevent the online fraud activities, we are working on implementing 'Online Finger Scanning' procedure.

II. Basic action plans

We propose the following action plans.

1) To register the smart phone device number [1] in the bank.
2) To register finger prints [2, 3] in the bank via the registered smart phone.
3) To initiate finger scanning for final approval of the online transactions [4, 5] through the registered mobile device.
4) To make some pre-defined and suitable time delay for each online transaction so that final online transaction approval decision can be made flexible.
5) Making debit cards and credit cards virtual.

III. Uses of the proposed action plans

With respect to the above action plans, collectively it is possible to say that,

1) User is restricted to make successful online transactions through his/her smart device only.
2) Online transactions cannot be made successful without finger prints.
3) User's credit or debit card cannot be handled by other users.
4) Even though scammers [6] are able to get one time passwords from victimized users, as the user is far away from the scammer and user finger prints are not being accepted by scammer's device, in any case, false transactions cannot be made successful.
5) In case of non-finger scanning, as there is a time

delay in finalizing any online transaction, as fraudster is supposed to wait for some time, mean while victimized user can become normal and can take a wise decision in stopping the supposed false transaction.

6) User can have a strong hold on his/her credit or debit card.
7) Apart from helping the user in activating the mobile device, finger scanner of the mobile device can be allowed to have a key role in securing the online transactions and thus finger scanner can be used to its full potential.
8) For a group of users or members of a family and joint bank account holders, with some flexibility in the above said action plans, online transactions can be made successful at their personal risk and understanding.
9) By making credit and debit cards virtual,
   a) There is no need for the user to carry any debit or credit card physically.
   b) There will be no point of damage of cards, misplacing of cards, forgetting of cards, loss of cards, thefting of cards.
   c) In case of any forced handling of any user by any scammer, it takes a long time for the scammer to find and operate the virtual card.
   d) In a phased manner, all debit and credit cards of any user can be made into a single virtual card with different set of codes.
10) Personal computers and laptops can also be equipped with finger scanning system and thereby online transactions can be made further secure and ease.
11) Switching and activating of personal computers and laptops with finger scanning helps in their secured time to time operations.
12) In a phased manner, one time password scheme can be eliminated.
13) Finger scanning can slowly be replaced with Eye scanning for ease and further secured online transactions.

IV. Mechanism

To register the smart phone IMEI number in the bank

The International Mobile Equipment Identity is generally a 15 digit code and is represented by IMEI. It is usually found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering *#06# on the dial pad or alongside other system information in the settings menu on smart phone operating systems. GSM networks use the IMEI number to identify valid devices and can stop a stolen phone from accessing the network. For example, if a mobile phone is stolen, the owner can have their network provider use the IMEI number to blacklist the phone. This renders the phone useless on that network and sometimes other networks, even if the thief changes the phone's subscriber identity module (SIM).

Devices without SIM card slot usually don't have the IMEI code. However, the IMEI only identifies the device and has no particular relationship to the subscriber. The phone identifies the subscriber by transmitting the International mobile subscriber identity (IMSI) number, which it stores on a SIM card that can, in theory, be transferred to any handset. However, the network's ability to know a subscriber's current, individual device enables many network and security features.

Many countries have acknowledged the use of the IMEI in reducing the effect of mobile phone thefts. For example, in the United Kingdom, under the Mobile Telephones (Re- programming) Act, changing the IMEI of a phone, or possessing equipment that can change it, is considered an offence under some circumstances. In the United States, changing the IMEI of a phone is not illegal. IMEI blocking is not the only way to fight phone theft. Australia was the first nation to implement IMEI blocking across all GSM networks, in 2003.

Keeping these points in view we emphasize that, based on the number of SIM(s), user must register IMEI number(s) in all of the respective banks in which user is having a valid accounts.

b) To register finger prints in the bank

A “fingerprint” is an impression left by the friction ridges of a human finger. The recovery of partial fingerprints from a crime scene is an important method of forensic science. Moisture and grease on a finger result in fingerprints on surfaces such as glass or metal. Deliberate impressions of entire fingerprints can be obtained by ink or other substances transferred from the peaks of friction ridges on the skin to a smooth surface such as paper. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers.

Human fingerprints are detailed, nearly unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity. They may be employed by police or other authorities to identify individuals who wish to conceal their identity, or to identify people who are incapacitated or deceased and thus unable to identify themselves, as in the aftermath of a natural disaster.

Since the late nineteenth century, fingerprint identification methods have been used by police agencies around the world to identify suspected criminals as well as the victims of crime. The basis of the traditional fingerprinting technique is simple. The skin on the palmar surface of the hands and feet forms ridges, so-called papillary ridges, in patterns that are unique to each individual and which do not change over time. Even identical twins who share their DNA do not have identical fingerprints. The best way to render latent fingerprints visible, so that they can be photographed, can be complex and may depend, for example, on the type of surfaces on which they have been left. It is generally necessary to use a ‘developer', usually a powder or chemical reagent, to produce a high degree of visual contrast between the ridge patterns and the surface on which a fingerprint has been deposited. The human skin itself, which is a regenerating organ until death, and environmental factors such as lotions and cosmet cs, pose challenges when fingerprinting a human.

In the Henry Classification System there are three basic finger print patterns: loop, whorl, and arch, which constitute 60–65 percent, 30– 35 percent, and 5 percent of all fingerprints respectively. There are also more complex classification systems that break down patterns even further, into plain arches or tented arches, and into loops that may be radial or ulnar, depending on the side of the hand toward which the tail points. Ulnar loops start on the pinky-side of the finger, the side closer to the ulna, the lower arm bone. Radial loops start on the thumb-side of the finger, the side closer to the radius (bone). Whorls may also have sub- group classifications including plain whorls, accidental whorls, double loop whorls, peacock's eye, composite, and central pocket loop whorls.

Fingerprint image acquisition is considered to be the most critical step in an automated fingerprint authentication system, as it determines the final fingerprint image quality, which has a drastic effect on the overall system performance. There are different types of fingerprint readers on the market, but the basic idea behind each is to measure the physical difference between ridges and valleys.

All the proposed methods can be grouped into two major families: solid-state fingerprint readers and optical fingerprint readers. The procedure for capturing a fingerprint using a sensor consists of rolling or touching with the finger onto a sensing area, which according to the physical principle in use (optical, ultrasonic, capacitive, or thermal) captures the difference between valleys and ridges. When a finger touches or rolls onto a surface, the elastic skin

deforms. The quantity and direction of the pressure applied by the user, the skin conditions and the projection of an irregular 3D object (the finger) onto a 2D flat plane introduce distortions, noise, and inconsistencies in the captured fingerprint image. These problems result in inconsistent and non-uniform irregularities in the image. During each acquisition, therefore, the results of the imaging are different and uncontrollable. The representation of the same fingerprint changes every time the finger is placed on the sensor plate, increasing the complexity of any attempt to match fingerprints, impairing the system performance and consequently, limiting the widespread use of this biometric technology.

In order to overcome these problems, as of 2010, non-contact or touchless 3D fingerprint scanners have been developed. Acquiring detailed 3D information, 3D fingerprint scanners take a digital approach to the analog process of pressing or rolling the finger. By modelling the distance between neighboring points, the fingerprint can be imaged at a resolution high enough to record all the necessary detail.

Keeping all of the above difficulties in view, we emphasize that, time to time at regular intervals, users must register and validate their finger prints in the respective banks with proper care and proper scanners to have smooth online transactions.

c) To combine the set of registered IMEI number and registered finger prints in the bank.

Since online banking transactions are being initiated and encouraged by banks, bank teams should take initiative to combine, store and process the registered IMEI number and registered finger prints of any user in order to have smooth transactions. In future with this kind of approach, one time password scheme can be eliminated.

d) To make some delay in finalizing any transaction

Users can be given a chance to set a timer for final approving of any transaction. This timer can be in between half an hour to one hour. This can be useful in judging or assessing the final transaction. As so many products are coming into market, sometimes or most of the times, users may not be having sufficient awareness or knowledge on the product and user may be in a state of confusion in purchasing the item online. The pre set timer may help in taking a firm decision in assessing the purchasing item.

Sometimes, when users are being tampered by scammers, as the pre set time is unknown to the scammer, he is forced to wait for some time. Mean while, the victimized user may come to a normal position and pre set timer allows the user to understand the scammer's cheating.

e) Virtual debit cards and credit cards

Either the bank authority or any virtual card issuing authority team can take initiative in developing and maintaining virtual credit cards and debit cards. As per the information given by bank authorities, virtual card authorities will create and maintain the user's virtual credit cards and debit cards. During online transactions, user is prompted to choose the desired card. After selecting the card, user's credit card number, expiry date and relevant information will be processed by the banking application software automatically. There is no need to enter the card information manually. After processing the card information, user is asked to confirm the same to make online payment. To have an unique identity card, virtual card issuing authority will issue a permanent physical card to the user with Aadhar number as the primary identification number. By inserting the Aadhar card in any ATM, user is asked to scan the finger and further operations can be carried out in smooth manner.

In case of loss or misplacing or forgetting the Aadhar card, at any ATM, for a very limited number of transactions in any month, user is asked to type the Aadhar number. After typing the Aadhar number, again user is asked finger scanning.

V. Discussion

As many people are not aware of the subject matter of IMEI and Finger prints, on behalf of this paper, we request Wikipedia to permit us to reproduce a part of the information for better presentation and clarity.

First four action plans seem to have some ease and control in minimizing online frauds. But coming to the 5th action plan, there seems to have security problems and needs further study.

During a journey or kidnap or any case of manhandling or threatening or at any remote ATM, there is a possibility for forced operating of all the virtual cards at a time by scammers. To avoid this, further high security action plans are required and we are working in this direction. In this context,

a) At ATMs - camera, alarm, emergency button for blocking all ATM transactions etc can be arranged.

b) Online transactions can be split into Safe mode and Unsafe mode. Unsafe mode transactions takes a minimum of 24 hours and safe mode transactions depends on pre defined delay timers.

c) Journey time transactions and other expected unsafe transactions can be put under Unsafe mode.

d) With some flexible rules, unsafe mode transactions can be converted to safe mode.

e) Long hour car driving and bike riding transactions during night and remote areas, can be put under Unsafe mode at the beginning of journey itself.

f) Security levels can be increased on roads connecting remote areas.

g) User can take the help of any call center for unexpected emergency.

VI. CONCLUSION

If banking units and smart phone manufacturing units come forward to implement the above action plans, in a phased manner, certainly online scams can be minimized, fraudsters number can be reduced, bank money can be secured, user can avail the maximum benefits of credit and debit cards without any hindrance.

VII. Acknowledgements

Authors are thankful to the conference committee for encouragement. Authors are very much thankful to their well wishers, Mr. K.V.Sripathi, Mr. K.V.Srinivas, Mr. B. Vamsi Krishna and Mr. U.V.Hareesh for their encouragement and valuable guidance.

VIII. REFERENCES

[1]. GPP TS 22.016: International Mobile Equipment Identities (IMEI)" (ZIP/DOC; 36 KB). 2009-10-01. Retrieved 2009-12-03.

[2]. Wang, Yongchang; Q. Hao; A. Fatehpuria;

[3]. D. L. Lau; L. G. Hassebrook (2009). "Data Acquisition and Quality Analysis of 3- Dimensional Fingerprints". Florida: IEEE conference on Biometrics, Identity and Security.

[4]. Fingerprint Alteration Archived June 2, 2012, at the Wayback Machine Biometrics research group, Michigan State University.

[5]. “Online Transaction Processing vs. Decision Support". Microsoft.com. Retrieved 2018-05- 07.

[6]. https://ieeexplore.ieee.org/document/7724963/authors#authors

[7]. https://en.wikipedia.org/wiki/Internet_fraud

Cite this article as : V. Sarada Swetha, S. Ramu, U.V. Harika, U. V. S. Seshavatharam, "On the Role of Finger Scanning in Fully Secured Online Transactions", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 127-131, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194723

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Security and Privacy Issues in Online Social Networking

Prof. K Adisesha*[1], Dr. Lakshma Reddy[2]
*[1]Research Scholar, Himalayan University, Karnataka, India
[2]Research Guide and Principal, SJES College of Management Studies, Bangalore, Karnataka, India

ABSTRACT

The advent of online social networks (OSN) has transformed a common passive reader into a content contributor. It has allowed users to share information and exchange opinions, and express themselves in online virtual communities to interact with other users of similar interests. However, OSN have turned the social sphere of users into the commercial sphere. This should create a privacy and security issue for OSN users. OSN service providers collect the private and sensitive data of their customers that can be misused by data collectors, third parties, or by unauthorized users. In this paper, common security and privacy issues are explained along with recommendations to OSN users to protect themselves from these issues whenever they use social media.
Keywords: OSN; security; classic privacy threats; modern threats, risk management in youth.

I. INTRODUCTION

Social media are a source of communication between the data owner (data generator) and viewers (end users) for online communications that create virtual communities using online social networks (OSN). A social network is a social graph that represents a relationship among users, organizations, and their social activities. These users, organizations, groups, etc., are the nodes, and the relationships between the users, organizations, groups are the edges of the graph. An OSN is an online platform used by end users to create social networks or relationships with other people that have similar views, interests, activities, and/or real-life connections. A large number of different types of social-networking services are available in the current online space.

Figure 1: Usage of social-networking sites

The following are some of the common features in social-networking sites:

- All current online social-networking services are web-based, using an Internet connection. Contents are stored on cloud storage through a centralized access management system. These contents can be accessed from anywhere using an Internet connection and web browsers.
- OSN users need to create a public profile for social-network sites as per their predefined format. This profile information is primarily used for the

authentication process to log into the social-networking site.

- Almost all existing social-networking services facilitate users in developing their social relations with other users by connecting a user's profile with others having similar profile information.
- One interesting feature of the existing OSNs is that contents on these sites are user-generated, while OSNs use these contents for business purposes.

The main goal of OSNs is to share contents with maximum users. Users utilize OSNs, such as Facebook, Twitter, and LinkedIn, to publish their routine activities. Sometimes, OSN users share information about themselves and their lives with friends and colleagues. However, in these published data, some of the revealed contents through the OSN are private and therefore should not be published at all. Typically, users share some parts of their daily life routine through status updates or the sharing of photographs and videos. Currently, various OSN users utilize smartphones to take pictures and make videos for sharing through OSNs. These data can have location information and some metadata embedded in it. OSN service providers collect a range of data about their users to offer personalized services, but it could be used for commercial purposes. In addition, users' data may also be provided to third parties, which lead to privacy leakages. It also offers a set of techniques to an organization for data analysis and making decisions based on this retrieved information. Data privacy protects information from unauthorized and malicious access that discloses, modifies, attacks, or destroys the data stored or shared online.

For example, researchers related to information retrieval sometimes do not consider privacy issues while designing solutions for information retrieval and management. On the other hand, researchers who work on data privacy usually restrict information-retrieval techniques to protect sensitive data from adversaries who seek personal information.

With the emergence of social media and the growing popularity of online communication using OSNs, more sensitive information about individuals is available online. Though much of the data that are shared through OSNs are not sensitive, some users publish their personal information. Thus, the availability of publicly accessible sensitive data can lead to the disclosure of user privacy.

The privacy of users is at more risk when publicly available data can be traced, and their activities can be connected with these data for mining and extracting sensitive information from it.

Privacy has different meanings in different situations, and the intensity of privacy depends upon the context of shared contents. Information gathered from social media for analysis purposes is generally unintended and often irrelevant. However, it may be related to the private activities of a person, for example, religion or political affiliations.

The main focus of the paper is to point out that privacy and security issues related to OSN, and educate ordinary users on how to protect themselves from these security and privacy issues. Privacy is the right of someone to keep information to themselves or at least share it only with relevant people. Privacy-preservation and -protection terms are used to keep private information away from irrelevant users.

II. Objective

The objective behind this work is to give a brief overview of raised privacy and security issues due to the use of OSNs. This is a fact that is necessary for everyone to use one a technological acility for smooth and fast communication. Social media are one type of these communications that have both negative and positive effects to their users. OSNs make information sharing more convenient and rapid than real-life communications. They make globalization a reality

and provide a chance to their users to express themselves. OSNs are also a new way for international relationships, whether the relationship is related to business or social interactions. It is easy for people to interact with each other using OSNs anytime and anywhere in the world. Along with these advantages, social media have disadvantages, one of which being the issue of privacy and security. In this paper, the issues that can harm OSN users are discussed, in addition to giving them recommendations on how to protect their privacy while using OSNs. The rest of the paper is organized as follows. Section 3gives an overview of the privacy and security threats in OSNs. Section 4 gives about different privacy and security treats for youth in OSNs.

III. Privacy and Security Threats in OSNs

User-generated content on social media may include users' experiences, opinions, and knowledge. In addition, it may also include private data, for example, name, gender, location, and private photos. Online-shared information is electronically stored and is therefore permanent, replicable, and rechargeable. OSN users generally face the challenges of managing their social identity while compromising their social privacy. The popularity of social media is such that worldwide active users of social media are expected to reach around 2.95 billion by 2020, which is about one third of the world's entire population.

The total active users accessing different popular social media networks are presented in figure 2. Popular Online Social Networks (OSNs) and their total active users in millions.

Figure 2 : Frequency of Social Media Usage

Taking into account this global number of users, privacy is one of the obvious and critical issues regarding OSNs. Various privacy issues are fostered because of OSNs, such as surveillance, in which the social sphere of OSNs changes to a commercial sphere and OSN service providers supervise user actions for market force access control. Standard OSNs share users' personal data with third parties for advertisement purposes that may be exploited. Likewise, OSN users leave digital imprints when they browse OSN sites, and therefore are targeted as data sources for commercial uses and user profiling.

In India, the number of internet users stood 296.6 million when compared to 2015 and 2016 where the increase rate is relatively lower as compared to the growth ranging from 142.23 million to 168.1 million. Nevertheless, the number of Social Media users in our country are expected to cross over 450 million by 2023 as shown in the figure 3. The most popular social media site in the year 2017 was Facebook, and later WhatsApp and Instagram remained the popular choice among the social media platforms.

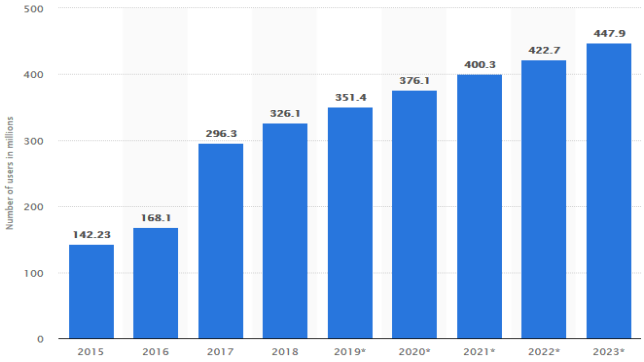


Figure 3 : Social network users in India from 2015 to 2023 (in millions)

Social-networking tools have changed the way we interact in our personal and professional lives.

Although they play a significant role in our social and business lives, at the same time they bring

about high risks concerning privacy and security. As hundreds of thousands of users use OSNs on a regular

basis, they have attracted the attention of attackers more than any other target in recent years. Because of the high usage of social media, online users have been exposed to privacy and security threats. These threats can be categorized into classic and modern threats. Classic threats are online threats that not only make OSN users vulnerable, but also other online users who do not use any OSN. The second type of threats is modern threats, which are related to OSN users only because of the OSN infrastructure that can compromise user privacy and security. The report states that social media are not included in the risk-evaluation scoring system but they are one of the top types of platform for cybersecurity.

Classification of Threats in social Media are:

3.1. Classic Threats

Classic threats have been an issue ever since the development of the Internet. These threats are spam, malware, phishing, or cross-site scripting (XSS) attacks. Although researchers and industries have addressed these threats in the past with the invention of OSNs, they can spread in a new way and more quickly than ever before. Classic threats are used to extract the personal information of users, which are shared through an OSN, not only to attack the target users but also their peers by adjusting the threat to correlate to users' private attributes.

3.1.1. Malware

Malware stands for malicious software. It is a generic term that refers to intrusive software.

It is developed with the intention to log into someone's computer and access their private contents. A malware attack on social networks is easier as compared to other online services because of the structure of an OSN and the interactions among users. The worst malware case is to access users' credentials and impersonate them to send messages to their peers. For example, the Koobface malware was spread through OSNs such as MySpace, Facebook, and Twitter. It was used to collect login credentials and make the target-infected computer a part of a botnet. An OSN has a vital role for various purposes, for example, marketing and entertainment. However, it has opened up its users to harmful activities. Committing fraud and propagating malware are criminal actions wherein users are engaged to access a URL and run a malicious code on the computer of an OSN user.

3.1.2. Phishing Attacks

Phishing is another type of fraudulent attack in which the intruder acquires the user's personal information by masquerading as a trustworthy third party through either a fake or stolen identity.

For example, during an attack that was attributed to intelligence by the Chinese government, senior U.K. and U.S. military officials were tricked into becoming Facebook 'friends' with someone impersonating the U.S. Navy Admiral James Stavridis. Similarly, social media were used in many places by phishers posing as other persons.

3.1.3. Spam Attacks

Spam messages are unwanted messages. In OSNs, spam comes as a wall post or a spam instant message. Spam in OSNs is more dangerous as compared to traditional email spam because users spend more time on OSNs. Spam messages normally contain advertisements or malicious links that can lead to phishing or malware sites. Generally, spam comes from fake profiles or spam applications. In case of a fake profile, it is normally spread from a profile created in the name of a popular person. Spam messages normally come from compromised accounts and spamming bots. However, the majority of spam spreads from compromised accounts. Spam-filtering approaches are used to detect a malicious message or URL in a message and filter it before delivering it to the target system.

3.1.4. Cross-Site Scripting

XSS is a vulnerable attack on web-based applications. It is one of the most common and serious security problems that drastically affect web applications. An XSS attack allows an intruder to run malicious code on the targeted user's web browser that results in compromised data, theft of data stored in the form of cookies, and saving passwords and credit-card numbers. Furthermore, an attacker can use XSS with a social-network infrastructure and develop an XSS worm that can be virally spread on OSNs.

3.2. Modern Threats

These threats are typically related to OSNs. Normally, the focus of modern threats is to obtain the private information of users and their friends, for example, an attacker wishes to know about a user's current employer information. If users have their privacy setting on their Facebook account as public, they can be easily viewed. However, if they have the customized privacy setting, then it is viewable to their friends only. In this situation, the attacker can create a Facebook profile and send a friend request to targeted users. Upon acceptance of the friendship request, details are disclosed to the attacker. Similarly, the intruder can employ an inference attack to collect users' personal information from their peers' publicly available contents.

3.2.1. Clickjacking

Clickjacking is also known as a user-interface redress attack, wherein a malicious technique is used to make online users click on something that is not the same for which they intend to click. In clickjacking attacks, an attacker can manipulate OSN users into posting spam posts on their timeline and asks for 'likes' to links unknowingly. With a clickjacking attack, attackers can even use the hardware of user computers, for example, a microphone and camera, to record their activities.

3.2.2. De-anonymization Attacks

De-anonymization is a strategy based on data-mining techniques, wherein unidentified information is cross-referenced with public and known data sources to re identify an individual in the anonymous dataset. OSNs provide strong means of data sharing, content searching, and contacts. Since the data shared through OSNs are public by default, they are an easy target for deanonymization attacks. In existing online services, pseudonyms are used for data anonymity to make the data publicly available.

3.2.3. Fake Profiles

A typical attack in most of the social networks is a fake-profile attack. In this kind of attack, an attacker creates an account with fake credentials on a social network and sends messages to legitimate users. After receiving friendship responses from users, it sends spam to them. Usually, fake profiles are automated or semi-automated and mimic a human. The goal of the fake profile is to collect the private information of users from the OSN, which is accessible only to friends, and spread it as a spam. The fake-profile attack is also a problem for the OSN service providers because it misuses their bandwidth.

3.2.4. Identity Clone Attacks

An attacker using theft credentials from an already existing profile, creating a new fake profile while using stolen private information, can perform Profile cloning. These attacks are known as identity clone attacks (ICAs). The stolen credentials can be used within the same network or across different networks. The attacker can use the trust of the cloned user to collect contents from their peers or perform different types of online fraud.

IV. Social Media Privacy & Security Risks for Youth

Let's find out what are the privacy & security risks the youth generation is facing from social media. In

addition, we will try to find out how to access the risks and what are the options to prevent those:

4.1.1. Profile Hacking:

Profile hacking is the most common issue in social media scam lists. Hacking one's social media account is not a difficult task for hackers. It takes just minutes for them to do it. Cracking the passwords of social media user accounts is the most common way to hack one's profile. These hackers include mostly the ones who are technically sound in computing.

4.1.2. Fake Apps and Malicious Links

There are many fake apps and links, which attain all your personal information including mobile numbers, email ids, passwords, residential addresses, and other personal details. With the help of these details, one can be easily prone to fraudulent situations; maybe a life of unwanted and unfortunate disturbances. All these apps and links have been deleted from the web network. However, there are still many people who are trying to get into it by creating more new things to carry out frauds.

4.1.3. Fake offers & schemes:

It is often observed that young people have a tendency to do shopping through several e-commerce platforms or online portals. They often get to see advertisements regarding their recent searches on social media platforms. Almost all of them get tempted to click on those links to check out recent offers on their favorite items. Hackers are taking advantage of this eagerness amongst young users. They are creating fake offers on expensive products; thereby encouraging them to click on those links and piercing into the system of users.

4.1.4. Login to social media channels through other networks:

As most of the young adults don't have premium smartphones or laptops, they try to serve their needs by using devices of their friends or cyber café. They often tempted to access their social media profiles through strange devices and even forget to log-off in rush. This may put them in serious risks of account privacy. An unknown person can access their social media profile and make changes to it according to their wish.

4.1.5. Fake Gaming software and apps:

Young adults spend maximum time of their day on playing games. They either prefer to play these games online or tempted to download and install gaming software to play it offline. Hackers are very much aware of this fact. They create several fake online and offline games that help them to sneak into the system of young users without even giving them a slight hint. Downloading any unknown or new game also put users in the high risk of downloading viruses or dangerous malware.

4.2. Risk Assessment

If you clicked on any link through your social media profile but observed that you are directed to some other websites which are not even close to what you were looking for then it's time to get alert. Most of the fake websites even make it hard for you to take an exit. They want you to spend maximum time on their platform; thereby they force you to share your personal details with them.

Most of the fake websites persuade you to check on their 'allow' notification bar. It thereby sending a lot of spam messages to your email id or social media profile. If you are getting constant emails or notifications on your social media profile from the

website to which you have never subscribed before then take it as a threat signal.

Following are some prevention methods.

4.2.1. Think twice before clicking any links:

There are many malicious links presents on social media nowadays which are meant for making cyber frauds. These lead to unwanted viruses or maybe one might create the links to attain the address of the social media users who click the links. These things further lead to undesirable and much devastating issues. So, think twice before you click any link!

4.2.2. Identifying Fake Apps before installation

As mentioned above, there are many applications in the market of social media which gains almost all the confidential information of social media users (that should not be shared by any means), and this information is proven to be helpful for the cybercriminals to make cybercrimes at a greater level.

4.2.3. Think before you share:

Every social media user is eager to share what he/she is doing currently or has visited new places with their friends and family. So, before you share anything on the web, just make sure that you do not tag your mates and share much of the information (as of location), which may lead to unwanted issues in your life.

4.2.4. Get accustomed to your network:

It is very necessary to make yourself well acquainted with your friend circle and people in your network. Avoid accepting friend requests or prevent chatting with people that you don't know in real life. Most of the hackers try to get familiar with young adults who are new on social media. Once they create rapport with you, they will start asking your personal details. So, it is always recommended to stay away from such people.

4.2.5. Avoid participating in surveys or questionnaire:

As young people have a habit of spending a significant amount of their daily internet time on entertaining activities, they often receive messages regarding contests, winning jackpots; online quiz competition and much more. It is always recommended to stay away from such contests. Most of them will not only waste your valuable time. They will also ask you to share your personal details to claim the award. This is a very common trick followed by hackers; you should not participate in such competition unless you verify the details of the competition.

4.2.6. Protect your location privacy:

Young adults tend to personalize their social media profile by updating the live location from their Smartphone device. They find it quite interesting to tag images or posts with a live location displayed to the public. This can be good if they are attending an educational event or corporate conference. But in other scenarios, if you follow to avoid sharing your location details to everyone. You can customize your settings or uncheck the box while installing a new app that asks your permission to access location details.

V. Conclusion

Social media is considered as a most lucrative and effective way to engage new users and develop communities online. However, in order to be successful with your diverse strategies on various social media platforms you need to identify, monitor and manage the risk associated in it as a part of your governance plan. Operating any of the social media channels without following preventive measures may put you into serious jeopardy. It will create harm to your personal or company image in the long term.

Social media is a want of life for everyone, without which no one can live. Every person is present on the web eagerly, and some are prone to unwanted risks and issues. The dangers can be avoided by following the simple steps mentioned above. So, simply follow the steps, stay alert from hackers and fake account users. Enjoy a social media life free from frauds.

VI. REFERENCES

[1]. International Journal Paper Publication "A Survey on Security and Privacy Challenges in Internet of Things (IoT)." By Prof. K. Adisesha, and Prof. Praveen Moses, in International Journal of International Journal of Business and Administration Research Review (IJBARR), Vol.6, Issue.2, April-June 2019, Pg. No. 06-13, E-ISSN -2347-856X, Impact Factor- 5.494

[2]. International Journal Paper Publication "Usage of Machine Learning and Hadoop Usage in Social Media Analytics" By Prof. K. Adisesha & Prof. Praveen Moses in GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES (GJESR), volume 4 Issue 5, January 2017 Pg. No. 53 to 59, ISSN: 2348 – 8034, Impact Factor-4.022.

[3]. National Journal Paper Publication "Security Issues in Mobile Payment" By Prof. K. Adisesha in Parivriddhi: A National Reference Journal of Multidisciplinary, Volume 2, August 2016 Pg. No. 70 to 78, ISSN: 2394 – 9112.

Cite this article as :

Prof. K Adisesha, Dr. Lakshma Reddy, "Security and Privacy Issues in Online Social Networking", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 132-139, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194724

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

A Survey on Network Security

Rachana R, Vinay N
UG Scholar, KLE S. Nijalingappa College, Rajajinagar, Bangalore, Karnataka, India

ABSTRACT

Computer networks are an essential part of our life by which we can share the information through different technologies like wired or wireless networks. Nowadays wireless technologies are adopted because of its advantages and secured information transmission. This article includes definition of network, network security and their working process on information security.

Keywords : Network, DoS, Attacks, Security, Encryption

I. INTRODUCTION

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse , modification , or denial of a computer network and network accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the administrator. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among business, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access.

NETWORK

A network is an interconnection of autonomous computers. Two computers are said to be interconnected if they are capable of exchanging the information. Central to this definition is the fact that the computers are autonomous. This means that no computers on the network can start, stop or control another.

NETWORKING SECURITY

The networking offers endless possibilities and opportunities to every user of it, alone with convince. But this convinces endless benefits are not free from risks as there are many risks in network security. While ensuring network security, the concerns are to make sure that only legal or authorized user and programs gain access to information resources like databases.

NEED OF NETWORKING

- ✓ File sharing provides sharing and grouping of data files over the network.
- ✓ Print sharing of computer resources such as hard disk and printers etc.,
- ✓ Email tools for communication with the email address.
- ✓ Remote access able to access data and information, around the globe.
- ✓ Sharing database to multiple users at the same time by ensuring the integrity.

APPLICATIONS IN NETWORKING

• SMS(Short Message Service)

It is the transmission of short text messages to and from a mobile phone, fax machine and/or IP address. Messages must be no longer than some fixed number of alpha-numeric characters and contain no images or graphics.

• Chat

Chatting is the most fantastic thing on internet. Chatting is like a text phone. In telephone conversations, you say something, people hear it and respond , and one can hear their responses on the spot and can reply instantly.

The problems encountered under network security are as follows:

• Physical Security Holes

When individuals gain unauthorized physical access to a computer and temper with files. Hackers do it by guessing passwords of various users and then gaining access to the network systems.

• Software Security Holes

When badly written programs or 'privileged ' software are compromised into doing things that they should not be doing.

• Inconsistent Usage Holes

When a system administrator assembles a combination of hardware and software such that the system is seriously flawed from a security point of view.

SECURITY MANAGEMENT

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming. In order to minimize susceptibility to malicious attacks from external threats to the network, corporations often employ tools which carry out network security verifications.

TYPES OF NETWORK SECURITY

A. Distributed Denial of Service (DDoS)
B. Intrusion Prevention / Detection System (IPS/IDS)
C. Security Information and Event Management (SIEM)
D. Network Access Control (NAC)
E. Virtual Private Networks (VPNs)

TYPES OF ATTACKS

Network are subject to attacks from malicious sources. Attacks can be from two categories : "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation or to conduct reconnaissance and lateral movement to find and gain access to assets available via the network.

Types of attacks include

• Passive
• Network
• Wiretapping
• Port scanner
• Idle scan
• Encryption
• Traffic analysis II.
• Virus
• Eavesdropping
• Data modification
• Denial-of-service attack
• DNS spoofing
• Man in the middle
• ARP poisoning
• VLAN hopping
• Smurf attack
• Buffer overflow
• Cyber-attack

WIRETAPPING

Wiretapping is the monitor of telephone and internet based conversations by a third party.

ENCRYPTION

The translation of data into a secret code. Encryption is the process of encoding a message or information in such a way that only authorized parties can access it.

VIRUSES

Computer virus is a malicious program that requires a host and is designed to make a system sick, just like a real virus. Viruses can spread from computer to computer and they can replicate themselves. Some viruses are categorized as harmless pranks, while others are far more malicious.

PROTECTION METHODS

I. Authorization
It determines whether the service provider has granted access to the web service to the requestor. Authorization is performed by asking the user a legal login ID. If the user is able to provide a legal login ID, he/she is considered as authorized user.
II. Authentication
Authentication also termed as password protection as the authorized user is asked to provide a valid password and if he or she is able to do this, he or she considered to be an authentic user.
III. Encrypted Smart Cards
An encrypted smart card is a hand held smart card that can generate a token that a computer system can recognize. Every time a new and different token is generated, which even though cracked or hacked, cannot be used later.
IV. Bio Metric Systems
They form the most secure level of authorization. The Biometric systems involve some unique aspects of a person's body such as finger prints, retinal patterns, etc to establish his/her identity. V. Firewall
A system designed to prevent unauthorized access to or from a private network is called firewall. They can be implemented in both hardware and software or a combination of both.
Types of firewall techniques are:
- Packet Filter
- Application gateway
- Circuit level gateway
- Proxy server

II. CONCLUSION

Network security is an important field that is getting more and more attention as the internet expands. This field concentrates on protecting the data from the unauthorized users. This security technology consists of mostly software and even certain hardware devices too. Network security plays an important role in authorizing the users so that they can secure their data from the hacker or unauthorized users. An effective network security plan can be developed to manage the understanding of security issues, potential attackers, needed levels of security and the factors that makes the network to attack. In addition to protect the network systems from the other external threats or failures, the network security is used. It can be stated that, using Network Security data transmission can be the safer mode of transmission with very less possible interruption to the any particular system.

Cite this article as :

Rachana R, Vinay N, "A Survey on Network Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 140-142, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194725

National Conference on Communication Technology & Network Security In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Image Processing Techniques and It's Applications-Review

Harshapradha D, Damini D H, Dr.Kavitha
Department of Computer Applications, Dayananda Sagar College of Arts, Science & Commerce, Bangalore, Karnataka, India

ABSTRACT

Current era of image processing the field of computer science, digital image processing and so on the use of computer is major and the computer algorithm to perform the given tasks the cost of the processing is high computer equipments of those era the work of processing digital image processing is the use of computer algorithm computer algorithm to perform image processing on digital image it follows range of algorithm to be applied to the data and can avoid problems as the The build-up of noise and signal of noise and signal during processing does signal image processing and GIS of Remote sensing it is the one of the famous moving processing and technique in the present and front 5 it's the main process of creating the program image processing method to perform some operations on an image point in our research research paper we have done the process where, how it is introduced and what are the components of it, how are the process accept and, the usage of the image processing and comma the all serving of the computer details studied and gone through the research, are all the major technique and Technology used in the image processing. The usage of these technology technology these technology technology is commercial 18% industrial 32%, hospitality 75%, usage and public 43%.

Keywords : Image Processing , GIS, Remote sensing

I. INTRODUCTION

IMAGE PROCESSING

This is a method in which we perform operations on an image, in order to get some useful information. In this process we put some useful image as input and we may get image as output or else we may get some useful characteristics features which are related to image[1], now a days this process is becoming vast and it is becoming a core research area for upcoming computer science students.

Basically it includes three steps.

1. Importing image by image acquisition tools.
2. Manipulating image and analysing the image.
3. Output in which result can be altered image or report that is based on image analysis.

The two types of image processing are Analog image processing and Digital image processing

Analog image processing can be used for the hard copies like printouts and photographs. Example for Analog image processing are television broadcasting in older days through dish antenna systems .

Digital image processing techniques help in manipulation of the digital images by using computers .example image data stored in digital logic gates.

II. PHASES OF IMAGE PROCESSING

a. ACQUISITION – It is a simple process in which a image is given out which is in Digital form. The main

work involves scaling and color conversion[2] (RGB to GRAY or vice- versa)

b. IMAGE ENHANCEMENT-This phase is also simplest and most approaching area of image processing it is used extract some hidden details from an image.

c. IMAGE RESTORATION –It is an objective of restoration on mathematical or probabilistic model of image processing.

d. COLOR IMAGE PROCESSING –This process deals with pseudo color and full color.

e. WAVELETS AND MULTI – RESOLUTION PROCESSING – In this phase various degrees of images is represented.

f. IMAGE COMPRESSION- In this phase, it develops some functions to perform operation which mainly deals with image size or image resolution.

g. MORPHOLOGICAL PROCESSING- It extract image components which is useful in representing and descripting shapes.

h. SEGMENTATION PROCEDURE- This process divides the image into different parts or objects and this is the most difficult task performed in image processing.

i. REPRESENTATION AND DESCRIPTION- Choosing the output of segmentation stage representation is only the part of solution for altering raw data into a processed data.

j. OBJECT DETECTION AND RECOGNITION- It is a process in which gives a label to an object based on its description.

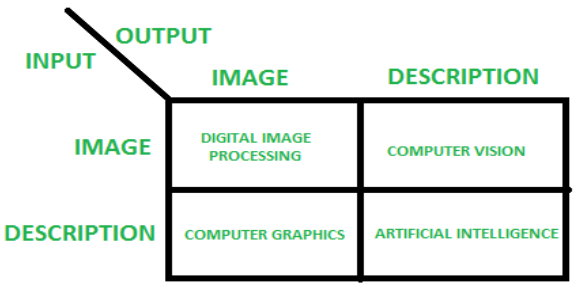


Fig.1. Overlapping Fields with Image Processing

DISCRIPTION

From the above image we can see four visions.

ACCORDING TO BLOCK 1-The input of an image is given and the output will be in the form of image and this is termed as digital image processing.

ACCORDING TO BLOCK 2- In this the input of an image is given and we get output in the form of description or information. This is termed as computer vision.

ACCORDING TO BLOCK 3- Input is given in the form of code or description and we get an image as output and this can be termed as computer graphics.

ACCORDING TO BLOCK 4- Input is in the form of keywords or code and we get keywords or some description as an output then it is termed as artificial intelligence.

III. ANALOG IMAGE PROCESSING

We can use analog image processing to take hard copies like for ex: printouts and photographs. Analysts of image use different basic interpretation[3] while usingthe visual techniques. Analog image processing is the image processing which is based on two dimensional analog signals by analog means. Fundamentally any information can be shown in two ways mainly named as:

1.) Analogue
2.) Digital

The analog wave which is represented in the form of pictures is called as analog image. For ex: television broadcasting system in older daysthrough the dish antenna system. The analogue image processing is applied on analogue signals. Analogue signal is time-varying signals so the image formed under analogue image processing is a slower and costlier process.

Analogue signal is real-world but not good quality of images. It is usually continuous and should not be broken into tiny pieces.

IV. DIGITAL IMAGE PROCESSING

Digital images processed methods helps manipulation of the digital image by using computer. The 3 basic stages that all types of information will have to undergo while using digital technique, they are pre-processing, enhancement, display, information extraction. It is also used to enhance the images to get some important information from it.

For example: Adobe Photoshop, MATLAB, Computer graphics, Signals, Photography, Camera Mechanism, Pixels, etc.

It is used in the conversion of signals from an image[4] sensor into digital images. A certain number of algorithms are used in image enhancing, processing of analog and digital signals, image signals, voice signals etc.

Types of digital image processing formats:

TIFF (Tagged Image File Format) : This format can be called as lossy or lossless. It is a very flexible format, a part of files are included by the details of the image storage algorithm. There is no compression at all in lossless image storage format and this is exclusive. They have a quite[5] big file sizes. (LZW is also one of the names used for lossless compression algorithm but universally it is not supported.)

PNG (Portable Network Graphics): In contrast with usage of common TIFF, lossless storage is also a format. To compress

File size it looks for patterns in the image which can be compressed it is exactly a reversible compression by this the image is exactly recovered.

GIF (Graphics Interchange Format): From a pool of 16 million colours it creates a table of 256 colours. Exactly the image can be rendered by GIF if the image has fewer than 256 colours.

JPG (Joint Photographic Experts Group): Very high image quality is maintained by achieving astounding compression ratios contains many colours for the tone of the image optimized for photographs. It works by discarding information that is least likely noticed by the eye analysing images.

RAW (Research and Analysis Wing): The better digital cameras has a raw images output. It is three or two times smaller than TIFF files. RAW formats can read some manufacturers graphic applications.

BMP (Bitmap): This format has no reason to be used. Microsoft has invented this uncompressed proprietary format called BMP.

PSD (Phot Shop Document): This format is called as working format. PSP image are profiles of paint shops used PSP and PSD extensions are used in photo shop's files. These images are used in all web pages but TIFF is not supported by web browsers.

Digital Image Processing allows users the following tasks:

- **Image sharpening and restoration:** The common applications of Image sharpening and restoration are zooming, blurring, sharpening, grey scale conversion, edges detecting, image recognition, and image retrieval etc.
- **Medical field:** The common applications of medical field are Gamma-ray imaging, PET scan, X-Ray imaging, Medical CT, UV imaging, etc.
- **Remote sensing:** It is the process of scanning the earth by the use of satellite and acknowledges all activities of space.
- **Machine/Robot vision:** It works on the vision of robots so that they can see things, identify them,etc.

Characteristics of Digital Image Processing

- It uses software, and some free of cost.
- It provides clear images.
- Digital Image Processing do image enhancement to recollect the data through images.
- It is used widely everywhere in many fields.

- It reduces the complexity of digital image processing.
- It is used to support a better experience of life.

Advantages of Digital Images Processing

- Image reconstruction (CT, MRI, SPECT, PET)
- Image reformatting (Multi-plane, multi-view reconstructions)
- Fast image storage and retrieval
- Fast and high-quality image distribution.
- Controlled viewing (windowing, zooming)

Disadvantages of Digital Image Processing

- It is very much time-consuming.
- It is very much costly depending on the particular system.
- Qualified persons can be used.

V. Applications of Digital Image Processing

Almost in every field, digital image processing puts a live effect on things and is growing with time to time and with new technologies.

1) Image sharpening and restoration

It refers to the process in which we can modify the look and feel of an image. It basically manipulates the images and achieves the desired output. It includes conversation, sharpening, blurring, detecting edges, retrieval, and recognition of images.

Fig.2.Image sharpening

2) Medical Field

There are several applictions under medical field which depends on the fuctioning of digital image processing.

With a general use of digital imaging processing data in the hospitals, the size repository of medical image is increasing very instantly. This source of difficulty in managing & querying vast databases that leads to the content based on medical image retrieval (CBMIR) systems.The main challenge[6] is CBMIR system was that a sematic gap that is there between the low level visual data captured by image device & high level sematic data which is retrieved by human. Efficiency of such systems those are more difficult terms in feature representation which can characterize the high-level information wholly. By using deep convolutional neural network (CNN), in this paper we can clearly tell the framework of deep learning for CBMIR. This is trained for classification of medical image. The 24 classes and 5 modalities are used to train the network which is present in intermodal dataset. The strategized features and thedifferentclassification with results are needed to retrieve images of medical field. When we need best results of retrieved images, class based predictions are used. For retrieval task to be successful we need average classification of 99.77% and mean average precision of 0.69% have to be achieved. For different body organs the methods best suited to retrieve multimodal medical images are:

a) Gamma-ray imaging
b) PET scan
c) X-Ray Imaging
d) Medical CT scan
e) UV imaging

3) Robot Vision

There are several robotic machines which work on the digital image processing. Through image processing

technique robot finds their ways, for example, hurdle detection root and line follower robot.

Fig.4.Image of Robot vision

4) Pattern recognition

It involves the study of image processing, it is also combined with artificial intelligence such that computer-aided diagnosis, handwriting recognition and images recognition can be easily implemented.

Now a days, image processing is used for pattern recognition.

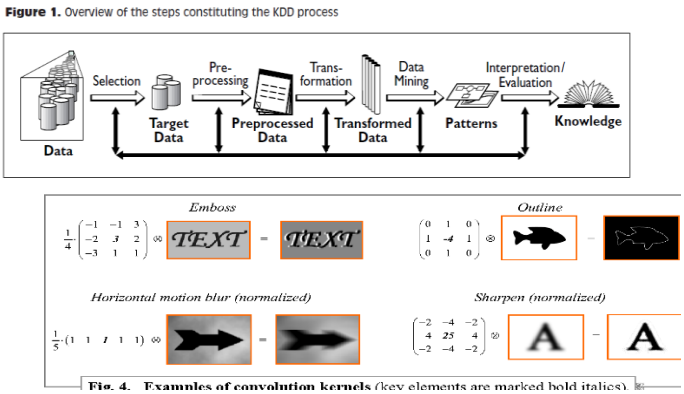


Fig.5.Image for pattern recognition

5) Vedio processing

It is also one of the applications of digital image processing. A collection of frames or pictures are arranged in such a way that it makes the fast movement of pictures. It involves frame rate conversion, motion dectection, reduction of noise and colour space conversion etc.

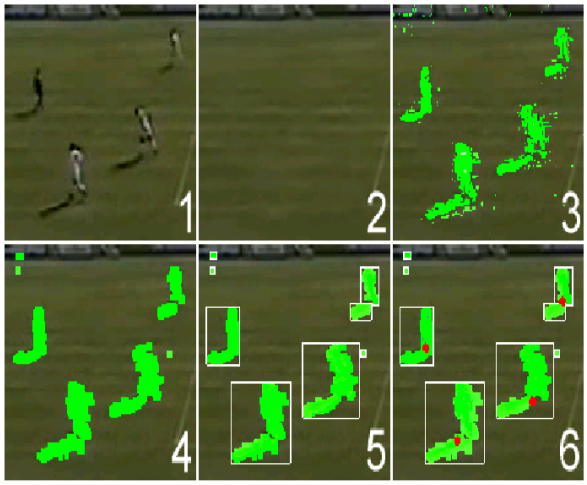


Fig.6.Image of how the vedio is processed

Conversion of the analog signal to a digital signal by digital image processing

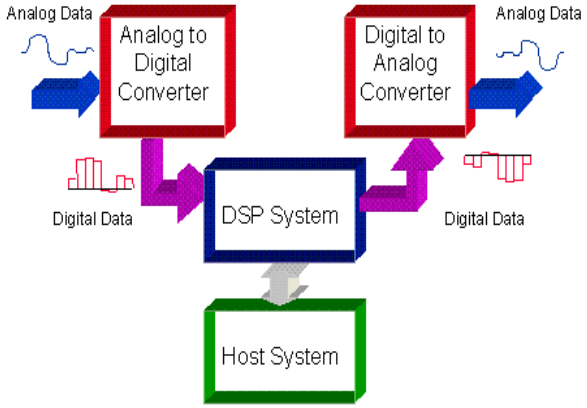


Fig.7 Image of converting analog signal to digital signal

Digital signal processing is all about processing analog signal or real-world signals which humans interact, for example, speech. DSP syatem coverts digital signal to analog signal or vice-versa by the use of converters.

VI. CONCLUSION

Hence we conclude that it is very useful to understand the concept of the image processing in these days. Earlier people used to think that all image processing uses pattern recognition technology. These days many new technology came which uses the system of image processing like iris recognition, face recognition, biometric recognition.

VII. REFERENCES

[1]. https://sisu.ut.ee/imageprocessing/book/1. Klipi teostus: Gholamreza Anbarjafari
[2]. https://www.geeksforgeeks.org/digital-image-processing-basics/. Rafael c. gonzalez
[3]. https://en.wikipedia.org/wiki/Analog_image_processing. free encyclopedia. This page was last edited on 17 September 2018 https://www.javatpoint.com/analog-image-processing-vs-digital-image-processing
[4]. https://www.javatpoint.com/digital-image-processing-tutorial
[5]. https://www.ivanexpert.com › blog › 2010/05 › the-5-types-of-digital-ima...
[6]. https://www.javatpoint.com/applications-of-digital-image-processing. https://www.sciencedirect.com/science/articale/pii/S0925231217308444

Cite this article as :

Harshapradha D, Damini D H, Dr. Kavitha, "Image Processing Techniques and It's Applications - Review", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 143-148, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194726

National Conference on Communication Technology & Network Security In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Challenges in Implementing NGN

Pavithra D. R.
Assistant Professor, BMS College for Women, Bangalore University, Bangalore, Karnataka, India

ABSTRACT
The telecommunication industry started to focus on a "next generation" of network that would replace the current telephone network . The technological advancements in telecommunications is leading towards the trend of unification of networks and services and Next Generation Networks are rapidly growing and developing globally. NGN being an IP based network enables customers to receive voice, data and video over the same network. NGN offers reduced network and operational complexity resulting in better and reliable service. It offers unrestricted access by users to different service providers also supporting generalized mobility. In the course of transition from the legacy PSTN to an IP based NGN there are many issues which need to be addressed. In this paper some of them is been defined.

Keywords : Next Generation Network (NGN), Dynamic Topology, Heterogeneity, Soft switch, Wavelength Division Multiplexing

I. INTRODUCTION

Communications technologies are evolving fast, demand for more and newer services anywhere and at any time. The drivers for this trend come from the economy, military defense,health and education fields, and match the request for more efficiency, and more comfortable and safe daily life. As a rule, new technologies are put into use as soon as they are available.

Communication networks have become a key economic and social infrastructure in world economies. The network infrastructure supports all economic sectors, and is therefore crucial to the national and international exchange of goods and services.

II. OVERVIEW OF NGN

In this section, we present the definition of Next Generation Network (NGN) along with its architecture and principles.

2.1 Definition of NGN

NGN is a packet-based network to support the transfer of mixed traffic types such as voice, video, and data. It is expected to integrate services offered by traditional networks and new innovative IP services into a single service platform. The key foundation of the NGN is the separation of services and transport networks, which provides QoS-enabled transport technologies and servicerelated functions independent from underlying transport technologies. The service network is composed of various servers such as Web Server, Authentication, Authorization and Accounting (AAA), SIP Proxy Server and LDAP Server etc. The service network is only responsible for providing services and applications for NGN users.

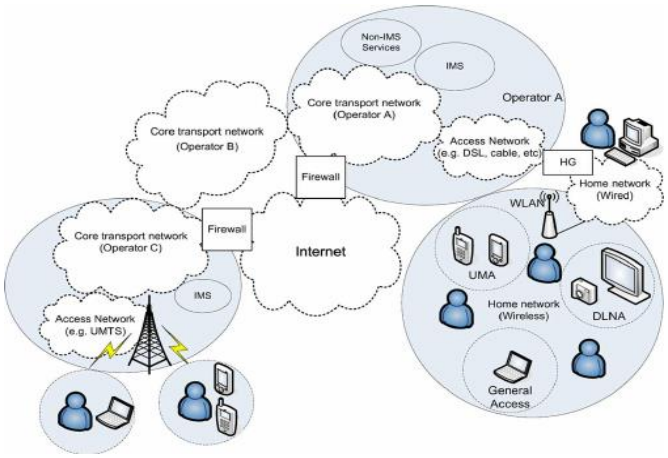


Fig. 1 shows typical NGN components

The connection between the service network and the core network can be implemented via gateways. The core network in NGN represents the transportation backbone in traditional networks, which is concerned with the transfer of information between peer entities. Besides the transfer of packets, control and management functions are also implemented in the core network. The access network in NGN is derived from the existing access technologies. To accommodate various access media, the access network is separated from the core network of NGN, which serves as an intermediate between user equipments and core network

2.2 NGN Functional Architecture

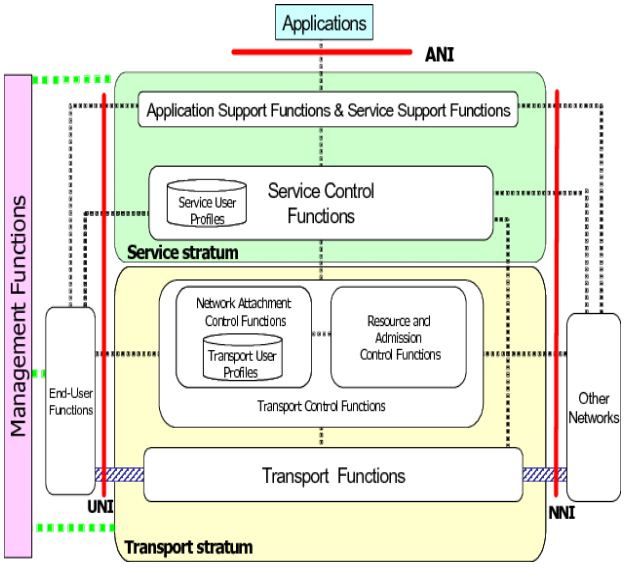


Fig. 2 shows an overview of the NGN functional architecture.

The NGN architecture needs to offer the configuration flexibility to support multiple access technologies. It also needs to support a distributed and open control mechanism, which provides a separated service provisioning from transport network operation and speeds up the provision of diversified NGN services The NGN functions are divided into service and transport strata.The service stratum functions provide session-based and non-session-based services, including subscribe/notify for presence information and a messaging method for instant message exchange .End-user functions are connected to the NGN by user-to network interface (UNI), while other networks are interconnected through the network-to-network interface (NNI). The application-to-network interface (ANI) provides a channel for interactions and exchanges between applications and NGN elements.

2.3 Core NGN Technologies Required

.Now NGN is not only a concept on the paper; its commercial implementations are already realized on a large scale. Appropriate technologies are significant for the accomplishment of the functions and abilities promised by NGN. In fact, any technologies which satisfy the NGN requirements could label themselves as NGN; some industry-wide accepted and practice-proved core NGN technologies are listed below:

Soft-switch: NGN provides PSTN/ISDN emulation and simulation services, which are used to enable end-users to use their legacy terminals with NGN continuously and have similar experience to the legacy system in an NGN environment.

MPLS (Multi-Protocol Label Switching): MPLS and its subsequent development (Generalized Multi-Protocol Label Switching or GMPLS for short) are virtual circuit switching protocols, and were designed to carry data for both circuit switching nodes and packet switching nodes. MPLS is an important element enabling NGN services by providing IP based

networks with basic traffic engineering ability such as CoS (Class of Service) and packet priority.

Core Transport Technology: IP over ASON over OTN: Wavelength Division Multiplexing (WDM) technology is widely used in the telecommunication backbone/core transport networks to provide solid transport services due to its tremendous line rates. Furthermore, IP is the virtually dominant network protocol now in the world to carry a variety of services and applications. Therefore, IP, ASON and OTN compose the best technical solution for an NGN transport network at the present time.

Moreover, a full NGN deployment requires cooperation among a number of technologies to realize the promised services and functions, such as new last-mile broadband technology, and mobile IP technology.

2.4 The Need for an NGN

Over the last decade the explosion of data traffic in telecommunication networks has been impressive. The shift from simple voice communication to rich content interactions (video and image) over the Internet, even in terms of the simple voice communication, voice carried by packets over mobile networks and the Internet has seen a dramatic increase while the voice traffic over conventional PSTN has dropped in recent years.

As stated the deployment of NGN is mainly driven by the desires of cost reduction and product differentiation from network companies (network carriers and service providers); however those network companies have a huge investment in the existing network infrastructure, and therefore a balance point between retaining current value and investing for the future must be taken into account.

On the other hand, from a users' point of view, the services of current networks have done quite well in teams of service quality, fulfilling the demands of enabling people to communicate geographically. However, from a network carriers' point of view, the existing network architecture has some significant drawbacks, it is too complicated and uneconomical to handle the possible traffic explosion in the future on a large scale and therefore it cannot meet the constantly increasing demands of the market. A new network infrastructure is required to handle the increasing data traffic in a cost-effective way and NGN was conceived due to this purpose.

III. Challenges in Future

Although NGN will derive greatly from the current telecommunications networks and IP-based infrastructure, its control and management architecture is likely to be radically different from both, and will be anchored on a clean separation between a QoS-enabled transport/network domain and an object-oriented service/application domain, with a distributed processing environment . The pressure arising from deregulation, competition and rapid technology development together with the fresh vision of NGN would generate significant challenges in terms of operation, administration and maintenance of networks and services.

Generation with the basic understanding of the concepts mentioned above, the challenges faced by next can be investigated.

A. Energy Efficiency, Maintaining Friendly Outlook.

Due to the rapid increase of number of people networks, a lot of the spectrum is being consumed. But the amount of spectrum being used is nowhere near the total available bandwidth. Even so, we are facing shortage of bandwidth due to wastages and inefficient usage of the spectrum. This has happened due to overcrowding of the spectrum by various wireless systems and services. The greater the spectrum being used, the more expensive it gets to keep the services running. Thus next networks will face a challenge in

keeping the service running at an economical rate.One such method to utilize the complete spectrum efficiently is cognitive radio. The cognitive radio as described looks for spectrum holes which are not being used. Once it finds such spectrum holes, it checks capacity to carry the load and then uses that spectrum band to run services. In Dynamic Power Scaling, the amount of energy spent is based on the network requirements. On the other hand, if the load on the network is very less, then only certain parts of the network are active and the others are in stand-by mode, which saves energy.

B. Dynamic Topology

In NGN, it is reasonable to expect that devices,especially high-end routers and switches, will become increasingly programmable, and that it will become possible to execute more control software directly on the devices . As a result, network topology of common networks of NGN can change occasionally. In addition, the collaboration between disparate network domains or between different service providers will increase to a great extent. Dynamic configuration and topology of NGN will challenge the traditional configuration management approaches,which are often inefficient and involve too many human efforts. In NGN, a quick-response and network-wide configuration capability is required to manage the changing network topology which may be composed of thousands of distributed nodes.

C. Heterogeneity

The NGN will not only contain the legacy components from traditional PSTN, but also some "brand new" components from the development of up-to-date technologies, e.g. Multi-protocol Label Switching (MPLS). Meanwhile, the flexibility based on trust negotiation among disparate domains is required in the pervasive computing environments of NGN. The interoperability among heterogeneous entities will become critical important for NGN. For these reasons, different vendors' platforms / technologies have to be "converged" and managed on a common platform in order to support and improve NGN services. Both CMIP and SNMP can be the candidates for the next-generation network management protocols. Limited by the multi-vendor capability and other weaknesses of current approaches how to deal with heterogeneous resources in a cost-effective manner thus becomes the big challenge for NGN.

D. Multiple Services (Traffic Considerations)

The NGN is packet-based, and responsible for carrying multiple services over the single IP-based transport network, ranging from traditional telephony voice to data, video and multimedia applications.

E. Security Issues

The next-generation-networks will be using a lot moresoftware (like SDN) than previous generations. This opens it up to a lot of security concerns. Whenever there is software involved, there are also security concerns. Security risks may arise as a result of a voluntary attack or software bug that occurs naturally.Jamming and spoofing are examples of voluntary attack on software and hardware.

F. Quality of Service (QoS) Challenge

QoS is extremely important for the next-generation of Internet applications such as VoIP, video-on-demand and several other consumer services. Some older networking technologies such as Ethernet were not designed or meant to support prioritized traffic which offer guaranteed performance levels. This makes it extremely difficult to implement QoS across the current infrastructure of the internet.

Data networks were not designed to carry voice, but the next-generation-networks will need to carry data and voice simultaneously. To make this possible, the network must be able to carry voice as a series of data packets. But the individual data packets experience different transmission delays and hence there might be overlapping of voice or cracking of voice at the receiver end. This is one of the main challenges faced by next-generation-networks. The solution to this would be to use RTP (Real-time Transport Protocol). RTP gives a way in which the timestamps and the

sequence numbers of data packets can be used to reconstitute a message signal even if individual data packets have different transition delays.

G.Reliability

As a network grows, there are more and more aspects that come into the picture. A large network will have thousands of software/hardware components, even if one of these components fail, there may be a drop in quality of service or a total disruption in service. This is obviously unacceptable. For example, a small network, say, servicing about a 100 people can be regularly checked and maintained to ensure100% uptime Therefore, with growing networks, reliability is going to be a big issue. But this can be addressed with the use In the SDN, a controller has the overview of the entire network and hence can find and correct faults in a short period of time.Best-effort approach in the current Internet, the NGN is optimized for differentiated services where QoS and reliability of services will be engineered and guaranteed. Accordingly, the traffic management capability for differentiated NGN services and traffic has to be provided so as to monitor and control any concerned service. In the traditional TMN framework,traffic management has not been addressed clearly since all network connections are at fixed rate. In NGN, the fine-grained controlling and monitoring of traffic pattern will become an important consideration for NGN service providers and network operators.

H. Standardization

For any service provider or network operator in NGN, the biggest motivation for adopting new operations support system (OSS) is to maximize Return On Investment (ROI). Besides taking advantage of new technologies coping with issues such as multiple services, other industry trends have to be considered, such as the trend towards commercial off-the-shelf (COTS) components and systems promising seamless integration (plug-and-play). Most important of all, the fundamental management architecture for NGN shall be considered. In the TMN architecture of the ITU-T, no further decomposition of the proposed layers into specific functions is proposed.

Although ITU-T's NGN Management Focus Group is emerging for necessary management standards, standardization in the area of network management for NGN is still fragmented at many different standards bodies.

IV. CONCLUSION

In conclusion, in the current telecommunication market, a new phenomenon can be observed: an ongoing rapid shift from traditional voice traffic to IP traffic, and a move from service-specific networks towards a common network infrastructure where all services are supported. Following the trends above, NGN is envisioned as a network infrastructure designed to cover the shortcomings of current networks. variety of challenges in NGN make current management approaches not applicable in the future. Some foreseeable challenges have been discussed in this paper, combined with the characteristics and services of NGN. Furthermore, promising evolutionary and revolutionary approaches were presented to illuminate emerging technical trends in the network management development of NGN.

V. REFERENCES

[1]. IEEE Network, New Books & Multimedia Column, November 2002)December 2, 2008,

[2]. ICT papers from http://www.newport-networks.com/cust-docs/89-ECH.pdf

[3]. Nightingale, S., Montgomery, D., Frankel, S., & Carson, M. (2007). A Profile for IPv6 in the U.S. Government. Retrieved December 2, 2008, from http://www.antd.nist.gov/usgv6-v1-draft.pdf

[4]. Olszewski, C., Labourdette, J., Huang, F., Charies, D., & Pendaradis, D. (2003). Network Migration: Evolution from Ring to Mesh. Proceedings of the National Fiber Optics Engineers Conference. Retrieved December 2,

2008, from http://www-ee.ccny.cuny.edu/www/web/ellinas/network-migration_NFOEC2003.pdf

[5]. Ponterotto J. G., (2005). Qualitative Research in Counselling Psychology: A Primer on Research Paradigms and Philosophy of Science. Journal of Counselling Psychology, 52(2), 126-136.

[6]. Pullar, T. (2007). Telecom's NGN will make old phones obsolete. Retrieved 2 December, 2008 from: http://www.stuff.co.nz/4178345a28.html

Cite this article as :

Pavithra D. R. , "Challenges in Implementing NGN", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 149-154, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194727

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Data Security and Privacy in Cloud Computing Environment

Ganga Gudi
Department of Computer Science, KLE's S. Nijalingappa College, Bangalore, Karnataka, India

ABSTRACT

Cloud computing is an upcoming paradigm that offers tremendous advantages in economical aspects, such as reduced time to market, flexible computing capabilities, and limitless computing power. To use the full potential of cloud computing, data is transferred, processed and stored by external cloud providers. However, data owners are very skeptical to place their data outside their own control sphere. Cloud Computing is a combination of existing technologies that make a paradigm shift in building and maintaining distributed computing systems. The large improvements in processors, virtualization technology, data storage and networking have combined to make the cloud computing a more compelling paradigm.

Keywords : Cloud Computing, Security Controls

I. INTRODUCTION

Cloud Computing is a new computing paradigm in which the Internet is used to deliver reliable IT services to customers. The amount of service can be scaled up and down based on the customer needs. This flexibility, combined with the potential of a "pay-per-use" model makes the cloud attractive solution to enterprises, where the capital expenses are heavily reduced. Cloud Computing is a combination of existing technologies that make a paradigm shift in building and maintaining distributed computing systems. The large improvements in processors, virtualization technology, data storage and networking have combined to make the cloud computing a more compelling paradigm. The cloud computing service model is "X-as-a- service" where X includes IT functions. The above definition is supported by five key *cloud characteristics*, three *delivery models* and four *deployment models.*

a) Characteristics

Cloud computing has a variety of characteristics:

Shared Infrastructure: Uses a virtualized software model, enabling the sharing of physical services, storage, and networking capabilities. The cloud infrastructure, regardless of deployment model, seeks to make the most of the available infrastructure across a number of users.

Dynamic Provisioning: Allows for the provision of services based on current demand requirements. This is done automatically using software automation, enabling the expansion and contraction of service capability, as needed.

Network Access: Needs to be accessed across the internet from a broad range of devices such as PCs, laptops, and mobile devices, using standards-based APIs.

Managed Metering: It manages and optimizes the service and provide reporting and billing information. In this way, consumers are billed for services according to how much they have actually used during the billing period.

b) Service Models

Software-as-a-Service (SaaS): The SaaS service model offers the services as applications to the consumer,

using standardized interfaces. The services run on top of a cloud infrastructure, which is invisible for the consumer. The consumer can only control some of the user-specific application configuration settings.

Platform-as-a-Service (PaaS): The PaaS service model offers the services as operation and development platforms to the consumer. The consumer can use the platform to develop and run his own applications, supported by a cloud based infrastructure.

Infrastructure-as-a-Service (IaaS): The IaaS service model is the lowest service model in the technology stack, offering infrastructure resources as a service, such as raw data storage, processing power and network capacity. The consumer can use the IaaS based service offerings to deploy his own operating systems and applications.

c) Deployment Models

There are four deployment models:

Public clouds: Public cloud computing is based on massive scale offerings to the general public. The infrastructure is located on the premises of the provider, who also owns and manages the cloud infrastructure.

Private clouds: Private clouds run in service of a single organization, where resources are not shared by other entities. The physical infrastructure may be owned by organization's datacenters. Private cloud users are considered as trusted by the organization, in which they are either employees, or have contractual agreements with the organization.

Community clouds: Community clouds run in service of a community of organizations, having the same deployment characteristics as private clouds. Community users are also considered as trusted by the organizations that are part of the community.

Hybrid clouds: Hybrid clouds are a combination of public, private, and community clouds. Each part of a hybrid cloud is connected to the other by a gateway, controlling the applications and data that flow from each part to the other. The private and community clouds are managed, owned, and located on either organization or third party provider side as per characteristic.

II. PROBLEM STATEMENT

There is a lack of knowledge on how cloud computing impacts the confidentiality of data stored, processed and transmitted in cloud computing environments. In this paper we concentrate on the security controls which protect the most sensitive data in private cloud computing architectures. With cloud computing, organizations can use services and store data outside their own control. This development raises security questions and should induce a degree of skepticism before using cloud services which points out five areas of security issues in cloud computing.

- **Privileged user access**

Data stored and processed outside the enterprises direct control, brings "an inherent level of risk, because outsourced services bypass the physical, logical and personnel controls IT shops exert over in-house programs".

- **Data location**

The exact location of data in the cloud is often unknown. Data may be located in systems in other countries, which may be in conflict with regulations prohibiting data to leave a country or union.

- **Recovery**

Cloud providers should have recovery mechanisms in place in case of a disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure".

- **Regulatory compliance**

Data owners are responsible for the integrity and confidentiality of their data, even when the data is outside their direct control, which is the case with external service providers such as cloud providers.

- **Data Lock-in**

Availability of customer's data may be at risk if a cloud provider goes broke or is acquired by another

organization. Providers should provide procedures on how customers can retrieve their data when needed.

III. SYSTEM SECURITY CONTROL SELECTION

It describes the security controls classes and to which families they are. Then we will describe the control selection process, presenting a recommended baseline of controls for each impact level of an information system. We will also show how this baseline can be refined to match the specific requirements of an organization. The result will be a list of required technical controls to match the security requirements of an information system. Security controls can be placed into three classes:

- **Technical security controls**

Technical controls can be used to protect against specific types of threats. These controls can range from simple to complex measures and consist of a mix of software, hardware and firmware.

- **Management security controls**

Management security controls are implemented to manage and reduce risks for the organization. Management security controls can be considered as the highest level, which focuses on the stipulation of policies, standards and guidelines.

- **Operational security controls**

It is used to correct operational deficiencies that might be exploited by potential attackers. Physical protection procedures and mechanisms are examples of operational security controls.

a) Procedure for selection process

When organizations start the selection process, there are three steps to be executed:

Selecting the initial security control baseline

The selection process begins with a baseline of controls, which are later on tailored and supplemented when the need arises.

Tailoring the security control baseline

After selecting the initial security control set, the organization continues the selection process by tailoring this baseline to their specific business conditions. Tailoring a baseline consists of two steps.

- Policy & regulatory related considerations
- Public access related considerations

Supplementing the tailored security controls

The tailored security control baseline acts as the starting point for determining whether or not this selection of controls provides enough security for the information system. This is done by comparing the organizations assessment of risk and what is required to sufficiently mitigate the risks to the organization. Two approaches can be taken to identify which additional controls and control enhancements must be included in the final agreed-upon set of controls:

- **Requirements definition approach**: In this approach the organization investigates possible threats and acquire specific information about what adversaries may be capable of, and what damage human errors may inflict. With this assessment of possible threats, additional security can be obtained by adding control enhancements.
- **Gap analysis approach:** It begins with an assessment of the current security capabilities, followed by a determination of what threats can be expected. This approach identifies the gap between the current security capabilities and selects additional controls enhancements.

b) Cloud Control limitations

In this, five properties influence the applicability of a security control, depending on the deployment of the information system and inherently, the deployment of the control itself.

IV. CLOUD SECURITY SOLUTIONS

The goal of this section is to describe the solutions and choices available to either counter these limitations,

or accept the limitations. When an organization considers a cloud service offering as operational environment for the information system in question, both parties can perform a gap analysis to determine which security controls are required for the information system, and which security controls the cloud service provider supports. The difference between the required controls and the supported controls is called the security gap. To reduce the organizational risk that the security gap imposes, the NIST recommends the following three options:

1. Use the existing contractual vehicle to require the external provider to meet the additional security control requirements established by the organization.
2. Negotiate with the provider for additional security controls if the existing contractual vehicle does not provide for such added requirements.
3. Employ alternative risk mitigation measures within the organizational information system when a contract either does not exist or the contract does not provide the necessary leverage for the organization to obtain needed security controls.

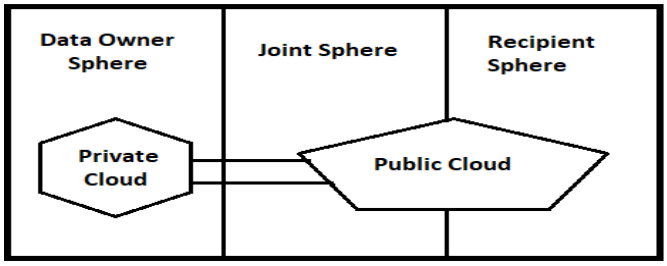


Fig 1. Hybrid cloud computing; the combination of clouds in multiple control spheres

V. CONCLUSION

The usage of cloud computing as a computing environment for information systems and data can place data outside the data owner's control. The amount of protection needed to secure data is directly proportional to the value of the data. When the value of data increases, the number and extensiveness of needed security controls also increase. It could be a problem if these security controls are not supported by the cloud provider. The uncertainty of how security can be guaranteed in external computing environments raises several security questions concerning the availability, integrity, and confidentiality of data in these cloud computing environments. We have focused on the confidentiality issues in cloud computing environments and proposed hybrid cloud computing is a very promising cloud deployment model that can cope with the security limitations occurring in a public cloud environment, while still being able to support many of the economical advantages of public cloud computing. Hybrid clouds depend heavily on the gateway between the private part of the hybrid cloud and the public part of the hybrid cloud. The gateway between the private and public parts of a hybrid cloud is an interesting point for research.

VI. REFERENCES

[1]. http://www.infoworld.com.
[2]. http://www.thestandard.com/article/0,1902,5466,00.html.
[3]. An example of a 'Cloud Platform' for building applications.
[4]. Klein, D. A. Data security for digital data storage
[5]. Mell, P., Grance, T. The nist definition of cloud computing National Institute of Standards and Technology 2009
[6]. Cloud Security Alliance. http://www.cloudsecurityalliance.org.

Cite this article as : Ganga Gudi, "Data Security and Privacy in Cloud Computing Environment", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 155-158, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194728

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Cloud Security - Hybrid Storage Model

UMA S
Assistant Professor in Computer Science, Nagarjuna Degree College, Ramahondanahalli, Yelahanka
Bangalore, Karnataka, India

ABSTRACT

Cloud storage / Virtual Cloud providers in today's world have multiple users and multiple servers sharing multiple data spread across the world. Massive servers where data is stored are often referred to as "server farms "which run 24*7*365. Cloud companies tend to outsource their "server farms" to different satellite locations for reducing the cost incurred, and also replicate and store data at various servers. Cloud computing is an IT paradigm that enables access to shared pools of configurable system resources and higher-level services over Internet. This paper provides an insight on whether the data generated locally must be stored within the country or exported cross-border. This abstract is to find the issues in existing solution and to find out whether to Nationalized or Globalize cloud storage.

Keywords : CC- Cloud Computing, AI- Artificial intelligent, IOT-Internet of things, CIFS-.Common Internet file system, NFS – Network file system, IT-Information technology

I. INTRODUCTION

Internet has brought a new revolution in Information technology, industries has been steadily moving away from Local storage to remote, server based storage and processing - "Cloud".

Figure 1. Global data center locations

Cloud computing is an on-demand service that stores and enables us to access data and services over internet. Cloud storage providers Such has Dropbox, Gmail, Facebook, Amazon web services and citizen services are increasing daily.

Objectives

With growing E-commerce and emerging Mobile apps, documents and media files are kept in cloud making it 'Digital assets'.

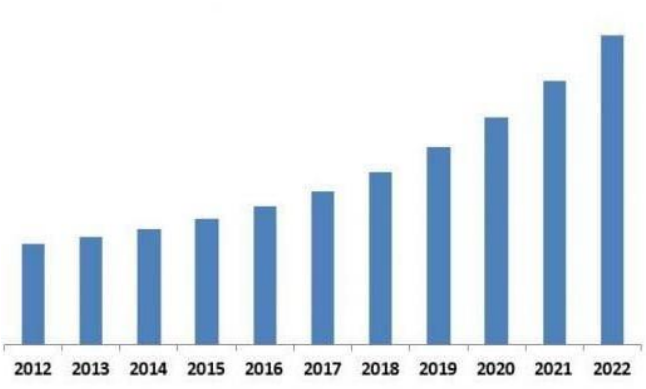


Figure 2. Data asset increase chart

With increase in digital payment and e-commerce the bigger concern is that if we put data into global cloud, security risk are heightened and it effects on our growth since we rely on foreign countries Data centers.

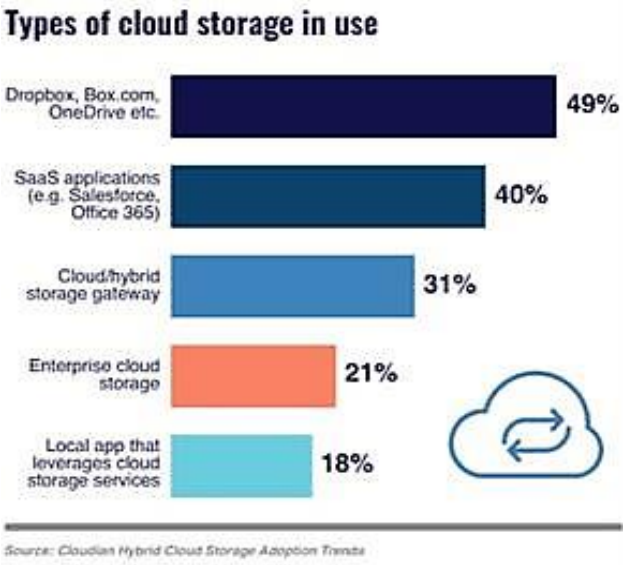
The objective is to provide a Make in India version of AI Local Data centers within Indian territory instead of Global storage which helps to boost the Indian IT industry. With recent Cambridge Analytica's misuse of Facebook user data there is an urgent need for the Customers awareness of the fact about the storage they are using.

II. METHODS AND MATERIAL

Cloud Computing is implemented using Virtualization technology; dynamic virtual

Figure 3. Cloud Companies

Cloud companies have varied customers and provide different type of storage space like Personal cloud (individual), Public cloud (social media), Private cloud(Enterprises) and Hybrid cloud (combination of Public and Private cloud).



Cloud companies outsource there Data centers to different satellite locations, and they usually replicate the data multiple times on various servers so as to ensure data safety in the event of some catastrophe (natural disaster, fire etc.).

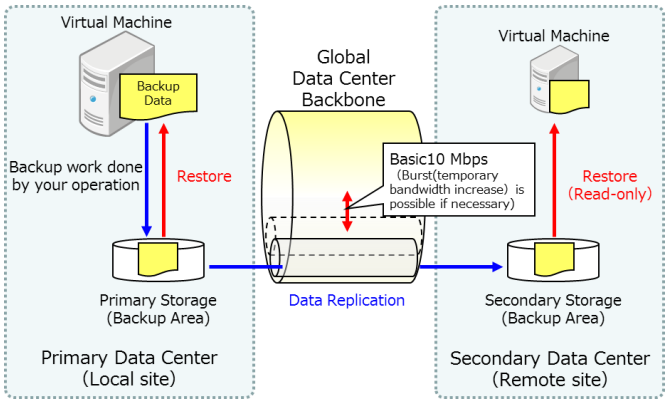


Figure 4. Global data storage

Need for Study

- ✓ Storage gateways are necessary to ensure that data stored in local Data centers infrastructures are optimized according to established standards, manage traffic and storage space.

- ✓ Implementation of new local Data Centers within Indian territory instead of outsourcing data created within India will give a boost to the Indian IT industry creating Employment, incresing innovation, results in revenue, protect national autonomy and positon India better in the IT sector.
- ✓ Countries such as Russia, Germany, France, We need to design, construct and manage these data centers. Well designed services don't upload entire files everytime they change. They just upload the changes, saving connection bandwidth. The cost of setting up data centers is far less than the revenue generatee by global companies in India.
- ✓ Indonesia, vietnam, Australia, Europe nd certin united states federal agencies have mandated via their strict data sovereignty laws that citizens data to be stored on physical servers within country's physical borders.

Figure 5. Data centers

Already paytm has powered AI cloud computing platforms in India. Paytm AI cloud process, stores all consumer data locally in servers located in India

III. Issues and challenges

- ✓ Several global companies already exist in Indian market, it might be hard to completely store data locally.
- ✓ A major issue is whether data localization limit the access to any global network or does it reduce the ability of citizens and consumers to access and contribute to online resources and opportunities globally.
- ✓ Data localization potentially burden relations between India and other countries.
- ✓ AI and IOT concepts in Cloud computing may be a major challenge since our local data server need to compete with the new inventions in AI and IOT.

Findings

A hybrid model – meaning a combination of both AI based local data centers and global data centers would be a better option to store the Digital assets.

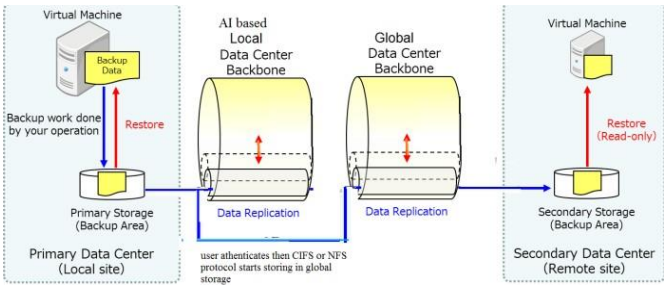


Figure 6. Hybrid Cloud storage

Further, only when customer authenticates then CIFS or NFS protocol should start storing data into global data centers otherwise data can be stored in local Data centers.

Conclusions

The Indian government's data localization push and with tremendous increase in data, creating a digital ecosystem " hybrid-cloud" , which combines Local and Global cloud storage will facilitates and supports the needs of multinational companies across industries and customers.

IV. REFERENCES

[1]. http:// sdtimes.com
[2]. http://www.esasd.net
[3]. www.opensourceforu.com
[4]. www.maropost.com

[5]. www.enterprisestorageforum.com
[6]. www.recuters.com
[7]. https://retail.economictimes.indiatimes.com
[8]. www.reviews.com
[9]. https:// www.ibm.com/cloud-computing
[10]. www.google.com

Cite this article as :

UMA S, "Cloud Security - Hybrid Storage Model", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 159-162, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194729

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Can We Digitalise Performance.....? – A Study

Amarnath Ramachandra[1], Sushmitha[2]
[1]St Annes College, Bengaluru, Karnataka, India
[2]Sri Krishna Degree College, Bengaluru, Karnataka, India

ABSTRACT

In the present era everything is being digitalised. So my question is can we digitalise performance? It is the pursuit of human mind that computer itself possess human mind and guide us in our day to day ventures. So this paper of ours is a small attempt in that direction. We feel that the Computer possesing human mind is a blur margin between fact and fiction but nevertheless the Question is can my research paper answer to the Question that - "is it possible for the technology to guide us in our everyday life?...."

Keywords : Digitalise, Digital Technology, Digital Devices , Academic Toppers, Digitalised

I. INTRODUCTION

The foundation of the research paper is the survey we did over 21 class toppers who are either doing their PG or UG courses. When the survey was made a common pattern evolved in the day to day life style of these class toppers. And we found that this comon pattern can indeed be adapted in the digital technology. Once this common pattern can be adapted in the digital technology then it is not tough task to make the digital devices to warn us if we sway away too much from this established pattern. Hence the digital devices will make sure that we follow this common pattern which itself is being followed by the academic toppers and the same digital devices when they track our day to day life they can accurately predict the probability of us getting top result in a class.

II. The Survey

A survey was done over 21 class toppers who are either doing their PG or UG courses it also included those candidates who had passed in net exams.

A common pattern was observed In their day to day training

Those points are mentioned as below.

1.A life changing incident happened in their life because of which to "become the topper of the class became the paramount importance in there life"

2.The zeal to become the topper of the class was so strong in them that hunger, Leisure or other performance hindering activities took 2nd priority in them Working hard to achieve topper position became the paramount importance to them

3.Every topper selected a place to sit and study, which the topper found it very comfortable to sit and study.

4.The topper begin to sit in that comfort place everyday without fail for a minimum of 2 hours 30 minutes to study this ritual was practiced come rain or shine ,sickness or boredom.

5.They practiced sitting in that comfortable place for a minimum of 2.5 to 3 months..

III. The challenge to track our day to day activities

What if our smart watch ensures we are spending 2.30 hrs to 3 hrs Sitting on our comfortable place each and

everyday and if we fail to do so the smart watch will give an alarm beep!!!!!
This is the challenge we faced!!!

Why Smart watch why not smart phone to track our Activities

Smart phone we don't carry always but smart watch will be with us till we go to bed hence the smart watch will locate whether we are at our study place and if we are indeed at our study place it ensures whether we are sitting their for a duration of 2.30 hrs to 3 hrs without walking around too much.

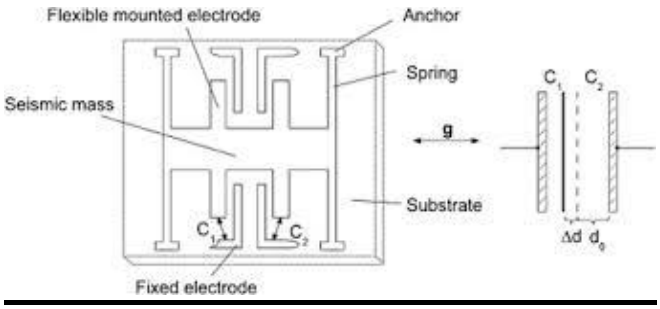
If we walk around too much it gives a warning beep that the walking around will hinder your performance And it will warn us too if we fall asleep at our study desk!!!!!

To invent this App is the goal of this research paper.

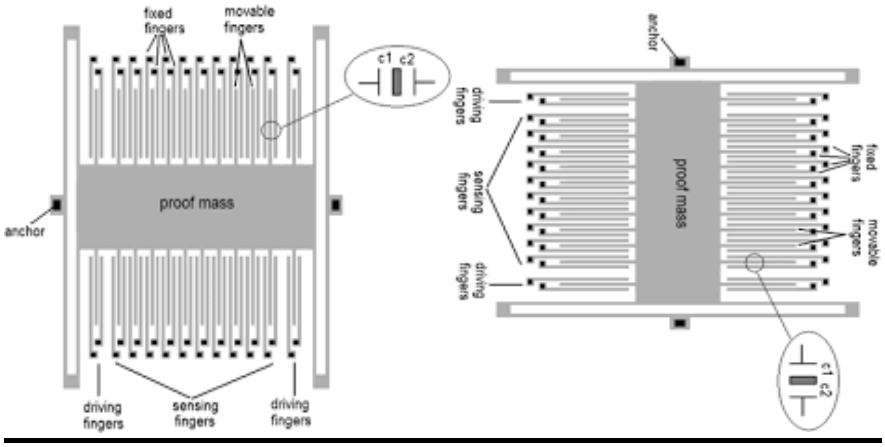
IV. A Real Life Scenario

So the candidate has sat in his place how to track he is not walking around too much?!!!.....
This can be done by pedometer

Cite this article as : Amarnath Ramachandra, Sushmitha, "Can We Digitalise Performance ? A Study", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 163-164, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194730



**Every time the hand swings the distance between the capacitor plate widens which increases the electric charge stored between the capacitor plates.
This increase of electric charge is considered as hand movement**



X-axis

Which senses the horizontal movement of our hand which happens while walking and every horizontal swinging of our hand is considered as walking

Y- Axis

Which senses the vertical movement of our hand which happens in any other movement other than walking.

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

A Survey on Image Encryption Techniques

Vishwas C.G.M[1], Dr. R Sanjeev Kunte[2]
[1]Assistant Professor Department of IS&E, J.N.N College of Engineering, Shivamogga, Karnataka, India
[2]Professor, Department of CS & E, J.N.N College of Engineering, Shivamogga, Karnataka, India

ABSTRACT
Security of data/images is one of the important aspects and it is still an expanding domain of digital transfer. Encryption of images is one of the well known mechanisms to preserve the secrecy of images over the Internet. This medium is vulnerable to attacks and hence efficient encryption algorithms are necessary for securely transmitting the data. Various techniques have been proposed in literature to cope up the ever growing need of security. This paper is an effort to compare the most popular techniques available for image encryption.
Keywords : Encryption, Decryption, Cryptography.

I. INTRODUCTION

With the increasing growth of multimedia applications, security is an important issue in transmission of multimedia data. The main aim of image encryption is to transmit the image securely over the network so that no unauthorized user can be able to decrypt the image. Therefore the information has to be protected while transmitting it. Important information such as credit cards and banking transactions need to be secured. For this reason, many techniques exist which are Image encryption, video encryption, chaos based encryption that have their have applications in many fields including the medical imaging, internet communication, transmission, military communication, tele-medicine etc. Encryption techniques are very useful tools to protect secret information. In this paper we survey on different techniques for image encryption.

This paper is organized as follows. In Section 1; we present general guide line about cryptography. In

We Survey on already existing work. Finally, we conclude in section 3.

Encryption is defined as the conversion of plain text into a form called a cipher text that cannot be read by others without decrypting the encrypted text. Decryption is the reverse process of encryption which is the process of converting the cipher text into its original plain text, so that it can be read [1]. In order to fulfill such a task, many image encryption methods have been proposed in the literature.

There are two main types of cryptography: 1.Secret key cryptography and 2.Public key cryptography. Secret key cryptography is also known as symmetric key cryptography. Here, both the sender and the receiver have the information regarding the same secret key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

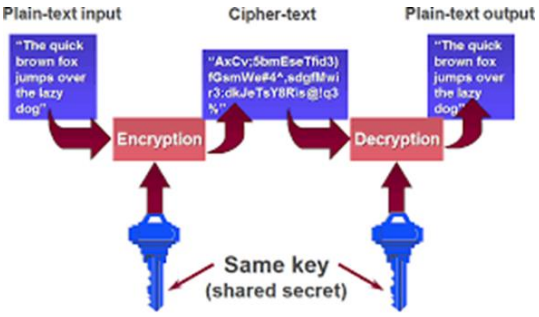


Fig 1. A simple model of symmetric key encryption

Fig 1 shows the process of symmetric cryptography. Both parties agree on the secret key that both of them will use in this connection. Sender starts sending its data encrypted with the shared key. On the other hand, receiver uses the same key to decrypt the encrypted message.

Public key cryptography, also called asymmetric key cryptography, uses a pair of keys for encryption and decryption as shown in Fig. 2. Where as in public key cryptography, keys work in pairs of matched public and private keys.

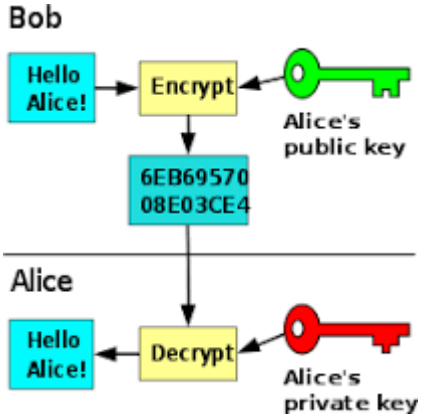


Fig 2. Asymmetric encryption

Nowadays when sensitive information is stored on computers and transmitted over the Internet, safety and security of information must be ensured. Considering this, image is also an important part of information. Therefore it is very important to protect the image from unauthorized access.

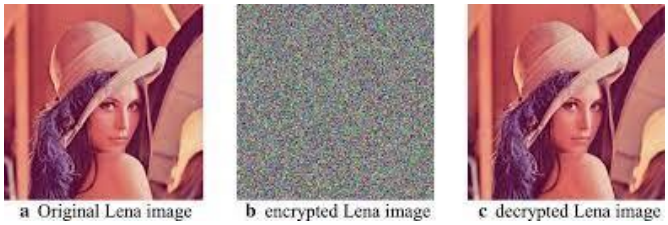


Fig 3. Image encryption process

Fig 3 shows a general image encryption process using any image encryption algorithm and the resultant encrypted image. Decryption is the reverse process of encryption which gives back the original image. There exists many algorithms in the literature to protect image from unauthorized access which is described in the next section.

II. LITERATURE SURVEY

Aloka Sinha and Kehar Singh [2] proposed the digital signature based image encryption scheme. First the original image is encoded and digital signature is added to the original image. Bose- Chaudhuri Hochquenghem (BCH) type of code is used for encoding of the image. After the decryption of the image, digital signature is used for authentication of the image and digital signatures are created and verified by means of cryptography. One-way hash function was used to produce the digital signature of an image. Standard digital image algorithms were used to convert a message of any length into a fixed length message digest which is usually 128 bits long. MD2, MD4, MD5 and Secure Hash Algorithm (SHA) are the standard techniques for creating hash. This encryption technique provides three layers of security.

S.Vani Kumari and G.Neelima [3] proposed the image encryption by using Chaotic Logistic Map and Arnold Cat Map. In this scheme, first block based shuffling is performed using Arnold cat transformation. After block based shuffling, pixel shuffling is performed by using certain number of iterations of Arnold cat map. The Arnold cat map is used to change the positions of the blocks/pixel values of the original image. The shuffled image contain the same pixel values as that of the original image. To encrypt the pixels of an image, eight different types of operations are used and which operation should be used is decided by the logistic map. It is concluded that chaos-based image encryption technology is very useful for real-time secure image.

Mohammad Ali Bani Younes and Arnan Jantan [4] proposed an image encryption using block-based transformation algorithm. A block-based transformation algorithm along with blowfish algorithm is used for encryption and decryption. First the original image is divided into blocks and then it is rearranged into a transformed image using a transformation algorithm. Later, blowfish algorithm is used for encryption. It is observed that increasing the

number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy. Experimental results showed that a direct relationship exists between number of blocks and entropy. And an inverse relationship exists between number of blocks and correlation.

A Combination of Permutation Technique for image encryption was proposed by Mohammad Ali Bani Younes and Aman Jantan [5]. This approach depends on the concept that, in natural images the values of the neighboring pixels are strongly correlated. This means that the value of any given pixel can be reasonably predicted from the values of its neighbors. It is necessary to disturb the high correlation among image pixels to increase the security level of the encrypted images. Here, a new permutation technique is introduced based on the combination of image permutation and an encryption algorithm called RijnDael. Here the original image is divided into 4 pixels × 4 pixels blocks, which are then rearranged into a permuted image by using a permutation process. The permutation process is defined as the operation of dividing and replacing an arrangement of the original image. The results show that the correlation between image elements is significantly decreased by using the combination technique which leads to higher entropy. This technique enhances the security level of the encrypted images by reducing the correlation among image elements and increasing its entropy value by decreasing the mutual information among the encrypted image variables.

Bibhudendra Acharya et.al.[6] proposed an Image encryption using Advanced Hill Cipher Algorithm. The available Hill cipher algorithm is classified as a symmetric key algorithm. The proposed advanced Hill (AdvHill) encryption technique uses an involuntary key matrix which overcomes the problem of encrypting the images with homogeneous background. It also overcomes the drawback of using a random key matrix in Hill cipher algorithm for encryption, where if the key matrix is not invertible then it may not be possible to decrypt the encrypted message. Also, as it is not required to find inverse of the matrix for decryption, the computational complexity can be reduced.

Sesha Pallavi Indrakanti and P.S.Avadhani [7] proposed Permutation based Image Encryption Technique in which image encryption based on random pixel permutation exists. In this technique, first for image encryption, image is split into blocks, later permutation is applied based on random number. Next, in the key generation phase, a key is built by using the values used in the encryption process. The last stage is where the identification process is involved in the numbering of the shares which are generated from the secret image. These shares and the key are then sent to the receiver. The key is generated with valid information about the values used in the encryption process which is a unique one from others. A new image encryption technique based on a new chaotic system by adding two chaotic systems: the Lorenz chaotic system and the Rössler chaotic system was proposed by Qais H. Alsafasfeh and Aouda A. Arfoa [8]. The main strength of this technique is that it provides stronger security. Data encryption standard (DES) is not useful for image encryption because of the special storage characteristics of an image. Experimental analysis shows that the image encryption algorithm has the advantages of high speed, large key space, high- level security and high obscure level.

Ibrahim S I Abuhaiba and Maaly A S Hassan [9] describe an Image Encryption using Differential Evolution Approach in Frequency Domain. This scheme employs magnitude and phase manipulation using Differential Evolution (DE) approach. First the two dimensional keyed discrete Fourier transform is performed on the original image. Then Crossover is performed between two components of the encrypted image, which are selected based on Linear Feedback

Shift Register (LFSR) index generator. Keyed mutation will be performed on the real parts of a certain components selected based on LFSR index generator. In this process, shuffling of the positions of image pixels is done. Final encrypted image is found to be fully distorted increasing the robustness of the said scheme.

Nidhal Khdhair El Abbadi et.al., [10] proposed new image encryption algorithm based on Diffie- Hellman and Singular Value Decomposition. In the proposed work, they have suggested a new way to encrypt image based on three main steps: the first one aims to scrambling the image values by using Fibonacci transform. The second step focuses on generating public and private key based on Diffie - Hellman Key Exchange which are used encrypt the diagonal matrix that is created by Singular Value
Decomposition (SVD) in third step. The experimental results show that the proposed image encryption system has a very large key space. Also the proposed image encryption algorithm analysis proves better in case of the security, robustness, correctness and effectiveness.

S.S. Maniccam and N.G. Bourbakis [11] have presented a novel approach which based on two works: lossless compression and encryption of binary and gray-scale pictures. The compression and encryption methods are based on the SCAN methodology which is a formal language-based 2D spatial-accessing methodologies that generate a wide range of scanning paths or space filling curves.

Chang-Mok Shin et.al.,[12] proposed an algorithm which was multilevel form of image encryption using binary phase exclusive OR operation and image dividing technique. The same grey level multi-level image is divided into binary images. Then binary pictures are regenerated to binary phase encoding.Then these images are encrypt with binary random phase images by binary phase XOR operation.

Huang-PeiXiao and Guo-ji Zang [13] describe an algorithm using two chaotic systems . One chaotic system generates a chaotic sequence, which changes into a binary stream using a threshold function. The other chaotic system is used to construct a permutation matrix. Firstly, using the binary stream as a key stream, randomly the pixel values of the images is modified. Then, the modified image is encrypted again by the permutation matrix.

Amitava Nag et.al, [14] introduced a novel approach using affine transform which is based on shuffling the image pixels. This method is a two phase encryption decryption algorithm. Firstly using XOR operation, the image is encrypted. Then, the pixel values are redistributed to different locations with 4 bit keys using the affine transformation. The transformed image is then divided into 2 pixels x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The result proves that the correlation between pixel values was significantly decreased after the affine transform.

A mirror like algorithm is presented by Jiun-In Guo and Jui-Cheng Yen [15]. There are 7 steps in this algorithm. At first, 1-D chaotic system is determined and its initial point x (0) and set k = 0. Then, from the chaotic system, the chaotic sequence is generated. After that, the binary sequence is generated from chaotic system. Image pixels are rearranged in the last four stages using swap function according to the binary sequence.

Seyed Mohammad Seyedzade, et.al., [16] proposed a novel algorithm based on SHA-512 hash function. The algorithm had two sections. Firstly, it does pre-processing operation to shuffle one half of image. Then the hash function is applied to generate a random number mask. Then, the mask is XORed with the other part of the image that is to be encrypted.

Ismail Amr Ismail et.al.,[17] proposed a chaos- based stream cipher which composes of two chaotic logistic maps and it also consists of an external secret key for encryption of image. In this scheme, an external secret key of 104 bit and two chaotic logistic maps are used to differentiate between the plain image and the encrypted image. Further, the secret key is modified after encrypting of each pixel of the plain image which makes the encrypted image more robust in nature. There is also a feedback mechanism which increases the robustness of the said scheme.

Rasul Enayatifar and Abdul Hanan Abdullah [18] proposed a novel scheme for image encryption based on a hybrid model composed of a chaotic function and a genetic algorithm. In this scheme, with the help of the chaotic function, first a number of encrypted images are constructed using the original image. In the next stage, these encrypted images are employed as the initial population for starting the operation of the genetic algorithm. Then, as much as possible, the genetic algorithm is used to optimize the encrypted images. In the end, the best cipher-image is selected as the final encryption image.

Kuldeep Singh and Komalpreet Kaur [19] compared four chaotic maps i.e., Henon, Logistic, Cross chaotic and Ikeda map and noise effects are observed on the image. First, the image encryption algorithm is used to convert the given original image to encrypted image. Then they apply noise on the encrypted image and then decrypt cipher image with noise back to original image. The conclusion is that the cross chaotic map shows best results than the other three chaotic maps.

III. CONCLUSION

In today's digital world, the security of digital images has become more important. In this paper, we have surveyed existing work on image encryption. We also give the general guide line about cryptography. The techniques that are described in this paper can provide security functions which might be suitable in some applications so that no one can carry unauthorized access on the image while transferring the image on the open network. In general, a well-suited, fast and secure conventional cryptosystem should be chosen so as to provide high security.

IV. REFERENCES

[1]. John Justin M, Manimurugan S, "A Survey on Various Encryption Techniques", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[2]. Aloka Sinha and Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203), 229- 234.

[3]. S. Vani Kumari and G. Neelima, "An efficient Image Cryptographic Technique By Applying Chaotic Logistic Map and Arnold Cat Map", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 9, 2013.

[4]. Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, 35, 2008.

[5]. Mohammad Ali Bani Younes and Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique

[6]. Followed by Encryption", IJCSNS International Journal of Computer Science and Network Security, VOL.8 , April 2008.

[7]. Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", International Journal of Recent Trend in Engineering, Vol. 1, No. 1, May 2009.

[8]. Sesha Pallavi Indrakanti, P.S.Avadhani, "Permutation based Image Encryption Technique", International Journal of Computer

Applications (0975 – 8887) Volume 28– No.8, 2011.

[9]. Qais H. Alsafasfeh , Aouda A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems", Journal of Signal and Information Processing, 2011.

[10]. Ibrahim S I Abuhaiba , Maaly A S Hassan, "Image Encryption Using Differential Evolution Approach In Frequency Domain" Signal & Image Processing: An International Journal(SIPIJ) Vol.2, No.1, March 2011.

[11]. Nidhal Khdhair El Abbadi, Samer Thaaban Abaas, Ali Abd Alaziz "New Image Encryption Algorithm Based on Diffie-Hellman and Singular Value Decomposition", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016, pages: 197-201.

[12]. S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34(6): 1229-1245 2001.

[13]. Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, "Multilevel Image Encryption by Binary Phase XOR Operations", IEEE Proceedings, 2003.

[14]. Huang-Pei Xiao Guo-Ji Zhang, "An Image Encryption Scheme Based On Chaotic Systems", IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006.

[15]. Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, "Image Encryption Using Affine Transform and XOR Operation ",International Conference on Signal

[16]. Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).

[17]. Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryption algorithm and its VLSI architecture", Pattern Recognition and Image Analysis, vol.10, No.2, pp.236-247, 2000.

[18]. Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, "A Novel Image Encryption Algorithm Based on Hash Function", 6th Iranian Conference on Machine Vision and Image Processing, 2010.

[19]. Ismail Amr Ismail, Mohammed Amin, Hossam Diab ,"A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps", International Journal of Network Security, Vol.11, No.1, pp.1 -10, July 2010.

[20]. Rasul Enayatifar , Abdul Hanan Abdullah, "Image Security via Genetic Algorithm", International Conference on Computer and Software Modeling IPCSIT Vol.14, 2011.

[21]. Kuldeep Singh, Komalpreet Kaur, "Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it", International Journal of Computer Applications (0975 – 8887) Volume 23– No.6, June 2011.

Cite this article as :

Vishwas C.G.M, Dr. R Sanjeev Kunte, "A Survey on Image Encryption Techniques", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 165-170, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194731

National Conference on Communication Technology & Network Security In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

CASB - Cloud Access Security Broker

Jyoti Bolannavar
Asst. Professor, Department of Computer Science, Govt. First Grade College, Naregal, Tq: Ron Dist: Gadag, State: Karnataka, India

ABSTRACT

With cloud technology becoming a larger and more important part of running a digital business, cloud computing platforms are rapidly limiting the effectiveness of the traditional security model. The cloud has required organizations to rethink security. Since data and applications in the cloud reside outside the old enterprise boundaries, they must now be protected in new ways. As more and more users connect directly to public cloud applications, and as workloads continue to shift to leverage Infrastructure-as-a-Service and Platform-as-a-Service capabilities from providers, a category of products called Cloud Access Security Brokers (CASB) has emerged to prominence and has become the go-to solution to address challenges in cloud security. Over the years, CASBs have evolved to keep pace with the rapid cloud adoption trends. This paper is an attempt to define some of the key capabilities that organizations look for in a CASB solution.

I. INTRODUCTION

Cloud computing has brought a variety of services to potential consumers. Many companies typically access around 600 services, mostly of the SaaS type. Those companies also have internal resources and governing access to external and internal resources can be a complex logistic problem in that access to those services need to be controlled because they may provide access to highly sensitive enterprise data. Although the service provider (SP) may have a strong security infrastructure, it does not understand the semantics of the applications running on it and the consumer must control access to its sensitive information. A new type of system software has recently appeared that can organize the management of these applications; this is the Cloud Access Security Broker (CASB). A CASB becomes a key part of the IT governance structure of the institution. Access to the company resources may come from portable devices such as smartphones, tablets, and laptops, and there is also a need to grant some user's temporary access to cloud applications; all this variety can be conveniently handled by CASBs. A CASB is also an important part of cloud ecosystems. An ecosystem is the expansion of a software product line architecture to include systems outside the product which interact with the product.

What is CASB?

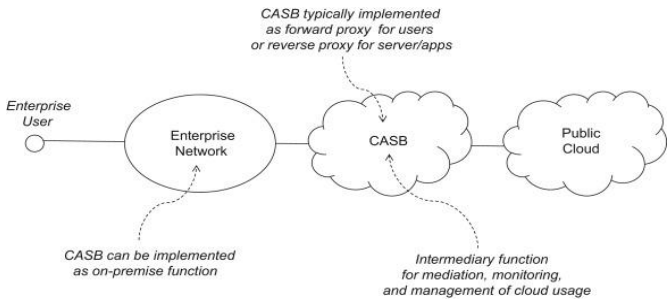
A cloud access security broker (CASB) is a software tool or service that sits between an organization's on-premises infrastructure and a cloud provider's infrastructure. A CASB acts as a gatekeeper, allowing the organization to extend the reach of their security policies beyond their own infrastructure.

CASBs typically offer the following:

- **Firewalls:** to identify malware and prevent it from entering the enterprise network.

- **Authentication:** to checks users' credentials and ensure they only access appropriate company resources.
- **Web application firewalls (WAFs):** to thwart malware designed to breach security at the application level, rather than at the network level.
- **Data loss prevention (DLP):** to ensure that users cannot transmit sensitive information outside of the corporation.

Architecture of CASB and working of CASB



How CASBs work

There are two key ways that a CASB can work. It can be set up as a proxy — either a forward or a reverse proxy — or it can work in API mode, using cloud providers' APIs to control cloud access and apply corporate security policies. Increasingly CASBs are becoming "mixed mode" or "multi-mode," using both proxying and API technology. That's because each approach offers pros and cons.

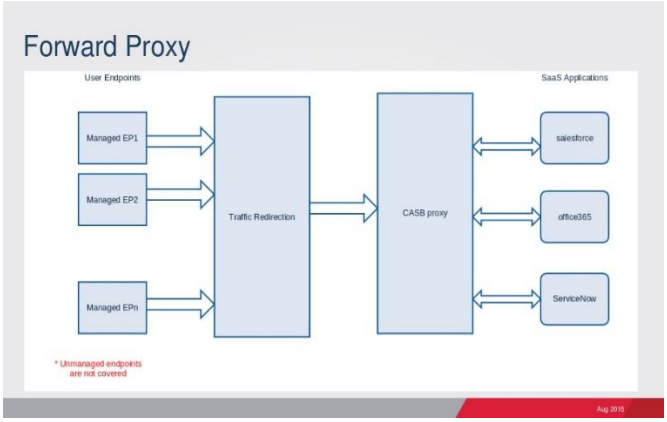
Proxy mode

A CASB deployed in proxy mode is “inline”; network traffic between users and cloud applications flows through the CASB proxy.

This is achieved in one of two ways:

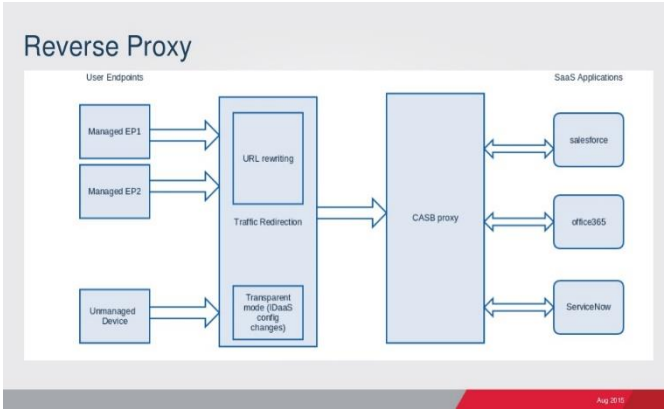
Forward proxy

For example, a forward proxy can be used for all types of cloud applications and all data passes through the proxy, but to use a forward proxy you need to install self-signed certificates on every single device that accesses the proxy. This can be difficult to deploy in a distributed environment or one with a large number of employee-owned mobile devices.



Reverse proxy

A reverse proxy system is easier in that respect because it is accessible from any device, anywhere, without the need for special configuration or certificate installation. The drawback is that a reverse proxy can't work with client-server type apps, which have hard-coded hostnames.



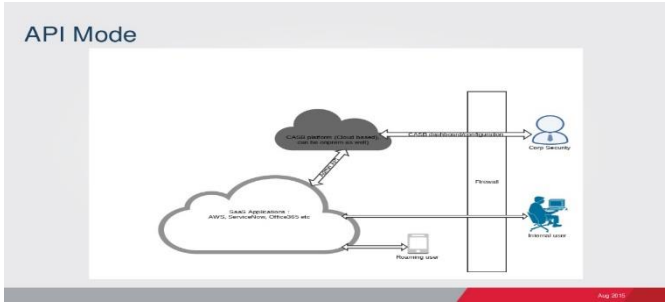
Proxy mode allows CASBs to implement very granular access controls. Proxy mode also gives the CASB visibility into data in motion and allows it to enforce policies in real time. For example, the CASB can ensure that files being uploaded are encrypted, and can block the download of sensitive files to noncompliant devices. It can also generate alerts in real time, allowing security teams to react

immediately to security incidents, policy violations, and anomalous behaviours.

However, proxy mode takes longer to implement. To route traffic to the CASB proxy, changes need to be made to network devices and endpoints (for forward proxy), or to applications (for reverse proxy). Also, some implementations of forward proxies require the installation of software agents on endpoint devices, which may be impossible with unmanaged devices. Further, some reverse proxies can break application functionality

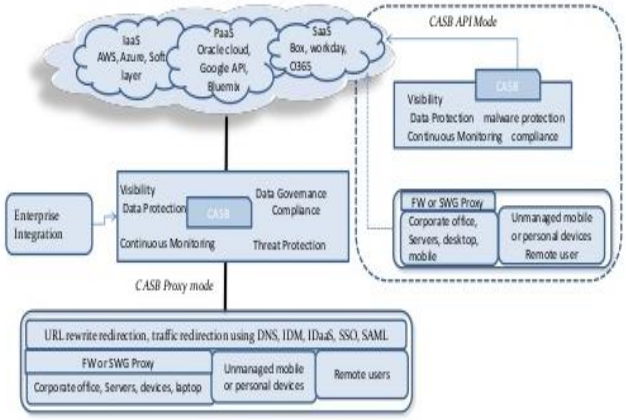
API mode

A CASB deployed in API mode is "out of band"; users communicate directly with cloud applications, and the CASB obtains data from the applications through their APIs. This approach provides very detailed visibility into data at rest and user activities, including logins and logouts, file uploads and downloads, information sharing, and administrative actions. CASBs deployed in API mode can also perform administrative tasks and enforce governance policies. For example, if a user violates policies by publicly sharing files containing sensitive information, administrators can use the CASB to change the access permissions on the files, or to take file ownership away from the offending user. A major advantage of API mode is speed: a CASB can be implemented literally in minutes because no changes to networks, endpoint devices, or applications are needed.



Hybrid mode

Some CASBs offer a hybrid mode that combines API mode and proxy mode. This allows the CASB to support a wide range of use cases with visibility, policy enforcement, and ways to deal with unmanaged devices.



Key CASB capabilities

- **Discovery, visibility and security across all cloud applications and resources** A CASB solution must provide a complete view into cloud access, irrespective of where users are located.

The solution should streamline security assessment across your cloud ecosystem:

- SaaS apps in use
- IaaS and PaaS providers your business relies on.

It should enable a security-first approach to compliance with support for pre-built and customizable compliance reports. It needs to provide means to remediate risks as they arise. Proactive monitoring of the entire cloud stack is an important consideration.

Most organizations today have adopted the cloud, and a majority of them have adopted a multi-cloud strategy. While BYOD policy at these organizations have increased productivity and lowered costs, Infrastructure-as-a-Service (IaaS) services and Software-as-a-Service (SaaS) apps need cloud app security to prevent threats, protect sensitive data and meet regulatory compliance needs. A Cloud Access Security Broker (CASB) solution must provide cloud security with visibility and control over sanctioned

and unsanctioned cloud services to enable safe and productive use. In addition, any CASB should be able to ensure that the initial or discovered state of the cloud service meets all the requirements of the organization to achieve the minimum acceptable security posture and standards.

- **Continuous Security Assessment for IaaS, SaaS & PaaS** The growth and rapid adoption of Infrastructure-as-a-Service (IaaS) has introduced the need for a Cloud Security solution to also cover the same. A Cloud Access Security Broker solution must be able to provide protection and security for all cloud use, whether SaaS, IaaS or PaaS, specifically by continuously monitoring security configuration for these environments, CASB should ensure that the services are configured appropriately and any change in configuration that results in a state change of the cloud service is captured and appropriate users are alerted. A CASB may also provide sensitive data discovery, protection and cloud Data Loss Prevention capabilities. Additionally, as the number of cloud services increase, it is very difficult to identify and manage the ongoing configuration changes that the service provider makes. Getting specific talent to manage these complexities are not easy either. A good CASB solution should provide a rich set of policies out of the box that will help organizations get an assured security posture right away, without the dependence on service expertise. For example, as enterprises adopt IaaS services, they need to have the expertise to understand not just the IaaS provider's compute, network, storage and security capabilities, but also need to understand the underlying infrastructure components and configuration. Not doing so may result in accidentally opening up the infrastructure to vulnerabilities. Ideally a CASB solution should have readily deployable security policies across cloud services that will reduce the barrier to adoption, improve time to value and enhance the overall security posture.
- **User & Entity Behaviour Analytics (UEBA) with Machine Learning & Threat Protection** By their very nature, cloud services, particularly the control plane of these services, are accessible via the internet. It is not only necessary to understand who is using these services but also to ensure that the vast threat surface opened up as a result is constantly monitored. That is where UEBA brings profiling and anomaly detection based on machine learning to security. UEBA essentially maps what legitimate processes look like when they take place in an enterprise and learns how to distinguish and stop threats. A CASB solution must incorporate UEBA to deliver actionable intelligence and provide protection against internal and external threats. The solution should be able to detect unusual user activity and data movement and compromised credentials that could indicate internal or external threat to a cloud environment.
- **Integration with Identity and Access Management** **Identity and Access Management** is a key element in the security of an operating cloud and is usually the first level in a defence-in-depth strategy of an organization. Understanding and defining user authentication and authorization among cloud actors is an important aspect of cloud security. A CASB solution as an open platform must provide seamless and standards-based integration with existing Identity and Access Management solutions or Identity-as-a-Service solutions.
- **Data Security and Application Security** typically covers integration aspect with SaaS applications. Risks to data security is the exposure of data at rest and data in motion. A CASB solution should be able to address Data Security for the cloud. Further, any CASB must provide cloud service specific insights, this includes the risk posture of the app, usage patterns and risky behaviour within the apps. While multi-modal CASBs support the

use of proxies, introduction of such infrastructure components complicate the deployment and increase adoption time.

- **Cloud Delivered – Responsive & Reliable For businesses,** the increasing sophistication of attacks means traditional approaches to security no longer provide adequate protection. Many organizations have now started to agree that cloud security as-a-service offerings can provide better security than on premise hardware or software security offerings. A CASB solution must be fast, responsive and highly reliable.
- **Non-Intrusive & Frictionless User Experience** A CASB solution must provide bullet-proof security without impacting productivity. It must provide required protection without causing slowdown and without affecting device performance. Additionally, the CASB solution should have sufficient APIs to integrate with other security solutions to facilitate remediation. Ideally, a CASB solution should be agentless hence reducing any friction to adoption by users.

Advantages of CASB include:

- Policy-based services--consumers can define security policies, e.g., RBAC, to apply to the services they use in order to restrict the access of their employees and customers to cloud data.
- Secure channel—the channel to access cloud services can be encrypted. Data encryption—CASBs can let consumers encrypt their data using their own keys.
- Compliance—consumers can demonstrate compliance with specific regulations because CASBs normally include security loggers/auditors.
- Discovery—users at the company are able to find out what services they have available through the CASB.
- Transparency—security is transparent to the application consumers when they use the CASB, they would only know about the CASB if an attempted access is rejected.
- Access unification—Consumers do not need to deal with a variety of credential types and protocols.
- Heterogeneity—access to the cloud can be made from any type of device.
- Malware detection—access to the cloud application through a CASB can guarantee that no malware will be found in the accessed service.
- Logging/auditing—the CASB keeps logs for security and compliance reasons; these can be later audited.
- Identity—the CASB can provide identification services.

Liabilities of CASB include:

- Complexity due to using different types of credentials. It can be fixed by using some standard such as SAML for all the credentials.
- If the consumers encrypt their data with their own keys, the SP cannot search that data and cannot apply its procedures to it.
- The CASB may incur in possible privacy violations, but careful use of its security controls can improve users' privacy.

II. Conclusion

In this paper we have presented the know-how about the Cloud Access Security Broker (CASB), which the ongoing and a go to market solution for protection of sensitive data being hosted by different vendors' trough cloud applications on different cloud platforms. And we also discussed about working modes of CASB along with its capabilities, advantages and disadvantages.

III. REFERENCES

[1]. [Sky14] Skyhigh Networks, "What is a cloud access security broker?",2014 http://www.skyhighnetworks.com/cloud-

university/what-is-cloud-access-security-broker/

[2]. [McV13] Lori McVittie, “The mounting case for cloud access brokers”, Virtualization Journal, Feb. 8, 2013.

[3]. https://pdfs.semanticscholar.org/fecb/163673cb5f87a40826dec5b1b4a796b60e8a.pdf

[4]. https://4b0e0ccff07a2960f53e707fda739cd414d8753e03d02c531a72.ssl.cf5.rackcdn.com/w-content/uploads/2015/12/Definitive-Guide-to-CASB_HPE-eBook.pdf

[5]. https://blog.cloudsecurityalliance.org/2016/08/11/api-vs-proxy-get-best-protection-casb/

[6]. https://www.slideshare.net/cisoplatform7/workshop-on-casb-part-2

Cite this article as :

Jyoti Bolannavar, "CASB - Cloud Access Security Broker", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 171-176, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194732

National Conference on Communication Technology & Network Security In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Human Security in Information and Cyber Era

Madhumita[1], Kavya V[2], Nair Rathish[2]

[1]Assistant Professor Department of Computer Application Soundarya Institute of Management and Science, Soundarya Nagar, Bangalore, Karnataka, India

[2]Department of Computer Application Soundarya Institute of Management and Science, Soundarya Nagar, Bangalore, Karnataka, India

ABSTRACT

This case studies brief note on aspect of human security in today's world. The role of social media, cybersecurity and cyberterrorism are playing high role in society and influencing forth destruction of human security. We are witnessing a technological revolution wherein in the tip fingerbone can know from present Government status to the thought so fin decidual people over networking. Social media is a great facilitator, which has not only brought people together but has bought much more worries too. It was revealed that Social networking sites permit for information to spread very quickly amongst the public. The biggest threat in technological era is no one can predict the time and source of brutal activities. Though Government is taking initiative to spend more and protect their data from cyberhackers or terrorists it has been highly difficult to disclose it. Social media, wiki leaks etc. are making Government efforts ruin. These are imposing threat to human security, and there is a need for greater Government security and awareness amongst citizens to safeguard their information.

Keywords : Cybercrime, Identity theft, Human Security, Privacy issues, Cyber Security

I. INTRODUCTION

Cyberwriters imaginary space, which is created when the electronic devices communicate, like network of computers. Cybercrime refers to anything done in the cyberspace with a criminal intent. Computer fraud can be an untrustworthy misrepresentation of the fact proposed to prompt another to abstain from doing something that causes loss. Computer crime can be summarized as a criminal activity which involves information technology infrastructure, in addition to unauthorized access, illegal interception, any data interference, computer or systems interference, abusage of devices, forgery, blackmail, embezzlement, and some electronic fraud s. Cybercrime can cause harm to any organisation.

To fight the fast-spreading cybercrime, governments and businesses must have collaboration globallybasicallyto develop any impressive model that somehow controls the threat. The internet is basically used for the betterment of life, to make people aware of world- wide activities, enhances the speed of life as well and makes users technically strong and up-to-the- mark. Asther use technology's increasing day-by-day, the crime is also increasing gradually. It covers all the formsofcrimesand thefts related to computer networks. Some of the criminals are technically expert and educated having deeper and remarkable knowledge regarding the technology

The purpose orthopaedist Understanding Cybercrime its Phenomena, Challenges and Legal Response is to assist everyone in understanding the legal aspects of cybersecurity and to help harmonize legal frameworks.

As such, it aims to help better understand the national and international implications of growing cyberthreats, to assess the requirementsofexisting national, Regional and international instruments, and to assist in establishing a sound legal foundation. It provides comprehensive overview of the most relevant topics linked to the legal aspects of Cybercrime and focuses on the demandsofdeveloping countries. Due to the transnational dimension of Cybercrime, the legal instruments are the same for developing and developed countries.

Cybercrime

Cybercrime is an activity done using computers and internet. We can say that it is an unlawful act wherein the computeractsaseithera tool or target or both. Computer crime, cybercrime, electronic crime orchid-tech crime basically criminal activity where a network or computerise target, source, or place of the crime. Network crime encloses wide range of illegally potential active activities. Whenever a person tries to steal information, or cause damage to computer network, this is assumed to be entirely virtual in which the particular information exists in digital form but the damage caused is real, which ceases the machine and has no physical consequence. A computer may act as a source of evidence, even though not directly or completely used for the criminal purposes, it acts as an excellent device for keeping the record and has given the in charge to encrypt data. If the evidences are obtained and decrypted, it will be assumed to have a greater value to the criminal investigators.

Cybercrime can be basically categorized in two ways: -

Computershare

Busing a computer to attack other computers, through network.

E.g. Hacking, Virus/worms, Do attack, etc.

Computerasweapon

Using a computer to commit real world crime.

E.g. Cyberterrorism, Credit card fraud etc

Varioustypesofcybercrimes There are several types of cybercrimes that are occurring in the networking world some of these are as written below

1. Financial fraud
2. Sabotage of data and other networks
3. Theft ofproprietaryinformation
4. System penetration from outside
5. Denial of service
6. Unauthorised accessbyinsiders
7. Employee use of internet service privileges
8. Viruses

Here the picture depicts the top countries having threat foyer crime

Threats to be aware of: -

Hacking

Hacking is a term used to describe actions taken by someone to gain unauthorized access to a computer. The availability of information online on the tools, techniques, and malware makes it easier for even non-technical people to undertake malicious activities. The process by which cybercriminals gain access to your computer. In hacking, the criminal uses variety of software to enter person's computer and the person may not be aware that his computer is being accessed from a remote location. This is a type of crime wherein a person's counterstroke into so that his personal or sensitive information can be accessed. Find weaknesses in your securitysettingsand exploit them in order to access your information. Install a Trojan horse, providing a back door for hackers to enter and search foryourinformation.

Phishing

Phishing is a crime mostly used by the criminals because it is one of the easiest ways to execute and it can produce the outcome sorresultsthey're looking for with less effort.

Websites, text messages, and fake emails are created to look as if they are from some authentic companies. Basically, these are sent by some criminals to steal and

acquire some personal and the financial information from you. This may also know as “Spoofing”.

Phishing is used by the strangers to "fish" or steal for information about you basically those that you would not disclose to a stranger, like your bank details, PIN, and some other personal details. What it does: Trick you into giving them information by asking you to update, validate or confirm your account. It is often presented in a manner than seems official and intimidating, to encourage you to take action. Provides cyber criminals with your username and passwords so that they can access your accounts and steal your credit card numbers.

Malware

Malware is the most common way to infiltrate or harm your computer. The term malware is nothing more than “malicious software”. Different malwares are Trojan, key loggers, spyware.

1) Alterfilesordelete them.
2) Intimidate you with scare ware.
3) Reformat hard drive causing you to lose all the useful information.
4) Steal some sensitive information.
5) Send emails using your identity.
6) Take charge ofyoursystem.

Computer Vandalism

Damaging or destroying data rather than stealing or misusing them is called cybervandals. These are program that attach themselves to a file and then circulate.

Cyber Terrorism

Terrorist attacks on the Internet are by distributed denial of service attacks, hate websites and hate E-mails, attacks on service network etc.

Software Piracy

Theft of software through the illegal copying of genuine progressors counterfeiting and distribution of products intended to passport original.

CYBER SECURITY

A branch of technology basically known as cybersecurity or information security applied to networks and computers, the objective carries protection of data or information and the property from the thefts, natural disaster, or corruption, and allowing the property and information to remain productive and accessible to its users. The Cybersecurityimpliesto the processes and the technologies which are designed to protect networks, computers and the data from the unauthorized access, attacks, and vulnerabilities delivered via the Internet bycyber criminals.

In countersecurity threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.

Example: malware, virus, spam’s, spywares

Who is Cyber Security Hacker?

A securityhackerisa person who seeks and exploits weaknesses in a computer system or computer network. Hackers maybe motivated bay multitude of reasons, e.g.: profit, protest, challenge, enjoyment, grudges or revenges.

Hotdishes hacker communicate with target?

Using targeted email

Fake emails

Fake website

Malicious web-link address in your email or social media

e.g.: Facebook, WhatsApp

Challengesovercybercrime occurrence:

Capacity to store data in comparatively small space as there is need to be right memory space to store. Also, if insist access like passwords such as individual name, mobile number, date of birth etc which is predictable. Complex and negligence of data may lead to leakage ofdata or piracy. Loss of evidence leads to cybercrime and human security issues.

Example: Receiving a text from an unknown number saying you have won and that you need to claim money/prize.

Prevention tipsforcybercrime:

1. Update firewalls (infrastructure defence systems) up to date.
2. Make sure that system is configured safely and securely.
3. Always choose strong passwords and securitychecksfor social networking sites, email boxes, and for systems.
4. Do not respond to unfamiliar mails.
5. Protect system with some best security software.
6. Shield or protect personal information from unknown people or strangers.
7. Safe browsing, and do maintain some good system hygiene.
8. Keep updating passwords, and login id's at least once or twice in one or two months and make them strong.
9. Do protect data and personal information and avoid being scammed.
10. Never send personal information and data via mail or anetodermas.
11. Make system clean time to time and review social media sites as well.
12. Do not respond to any spam email and be cautious
13. Do not visit / link to unknown and dangerous website.
14. All external drives must be scanned.
15. Be aware of surroundings– never reuse a password.
16. Do not connect to public free WI-FI network using company laptop.

Conclusion

In this modern era of technology, the role and usage of internet is increasing worldwide rapidly, therefore it becomes easy for cybercrime in also access any data and information with the help of their knowledge and their expertise. The cybercrime as a whole refers to Offences that are committed against individuals or groupsofindividualswith a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directlyorindirectly, using modern telecommunication networks such as Internet and mobile phone. Such crimes may threaten a nation'ssecurityand financial health too. Issues surrounding this type of crime have become high-profile, particularly those surrounding cracking and child grooming. A computer can be a source of evidence. Even when a computer is not directly used for criminal purposes, may contain records of value to criminal investigators. So, the network must be secure as no one can access the information of the computer by providing the necessary security.

Cybercrime is an awful act that needs to be tackled firmly and effectivelyeitherbywell known people or Government. There is a need to create more awareness among the people and basically usersofinternet about cyber space, cybercrime and some more aspects. So, it is seriously advised to take some previous precautions while operating the internet before attaining loss. Security nowadaysisbecoming a prominent and major concern hence it's always best to take care of the networks which is being used and must be provided with assured security. Itsalwaysbetterto take certain precaution while operating the net.

Future Scope

Human securitise main aim ofurace study and hence it is more concerned over it. Basically, this paper demon tradeshow ignorant we are in the security purpose and ways to keep secure and cope up with the threats that may occur. The new implementations that can be done overtire Biometric system, in future Retina detection i.e., Iris detection can be a revolutionary system. As fingerprint also being done forgery's threat to rely on it. A lot of research is still going on in this area to build a more secure system despite offal disadvantages.

Example: According to our opinion using smart card with fingerprint detection makes system more secure. Thus, combination of

II. REFERENCES

[1]. Biometric with technologies makeshighlyeffective in security.

[2]. To conclude, the usage of biometric systemsmainlyiris detection will increase a lot more securityto humansin upcoming dayswith the support ofstable technologiesand more cost effectiveness.

Cite this article as:

Madhumita, Kavya V, Nair Rathish, "Human Security in Information and Cyber Era", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 177-181, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194733

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Mail Bucket

Prof. Shreedhara N Hegde, Prof. Manjula T.
Seshadripuram Degree College Tumakur, Karnataka, India

ABSTRACT

The Mail Bucket application is being developed to transfer the files between the cloud services. It helps in storing, grouping, managing and transferring of files from one service provider to the other. The files can also be downloaded when the user is offline and it helps in backing up the files easily. Various kinds of the documents are being synced with the help of service providers like Gmail, yahoo, OneDrive etc. The documents can be synced based on the various categories of the documents which are available. The users need not upload or download the document in order sync the files to the application. There is no existing system application where we can find all the documents in one single application. The application also helps in improving memory allocation for Various Service providers. Our application also improves the consistency with respect to security and portability.

Keywords : Admin, User, Service providers, Cloud Providers.

I. INTRODUCTION

The application helps us in grouping, storing, managing and transferring of files from one application to the other. This is a best application in transferring the files between the cloud services.

The application connects to the cloud and qualifies you in firmly accessing all your files that saves all kinds of documents at one place, images, audio, video etc. which can found beneath the virtual roof. It helps the users to arrange, manage, transfer, correct and share files between multiple service providers like Dropbox, Google Drive, and OneDrive etc.

Through this application we can also download the files required when offline. . It is a web- based application that helps in transferring the files across cloud services and permits users to correct, take backup of their files.

The major users of the application are Admin, User and the Service Providers

Admin is responsible in managing and planning all the activities that are being distributed in the application. He has the authority of receiving all the major access points of the users who is registered to the application. He will receive the count of number of files and applications that are synced from different Service providers.

He authenticates the users by notifying a confirmation mail to the users account before the user receives his credentials.

User must get registered to the application in order to access the application and to store all his files in a single application.

The user will upload , download and syncing the files from the various cloud providers and he will use this

account to view all his documents that is saved in a single application. He can integrate files from various clouds by just choosing the files which are to be integrated.

Service Providers are nothing but the Gmail, GDrive, Dropbox, Outlook, OneDrive etc., which are different types of cloud storages used by many users to store their documents.

These are the various service providers which helps in storing, managing and updating the files that are stored only in their boundaries. Here we cannot integrate our files which are stored in the application directly. But the application being developed helps us in syncing the files from these Service providers where many of the users important documents are being shuffled which will be in need of time.

There is no need of downloading the required documents and later uploading it to the application. It is just one click by which we can integrate the necessary documents from these service providers to our application.

Tools and Technologies Used:

Application Environment are being used in order to develop the application which makes the design look more effective and attractive. The technologies used are secure, reliable and robust. Below are the description of the technologies used in developing the application.

HTML5

- The properties and the behaviours of the 5th version of the HTML are being defined which helps in designing of the web pages
- Structure of the document is being written mainly.
- Html has its own new and latest set of elements which is being introduced in the new and the stable version and it is also being more complicated to know about the large set f API's designed.
- Basic concepts and the events used in html are to be learned initially which helps in developing the application
- Html is being used by most of the people and it is being a very sophisticated language across.

CSS3

- The design and the presentation of the web pages with its styles, colors, font families, font –size, layouts etc are being defined in the style sheets.
- The css can be used to design a responsive web page which adjusts in all kind of multi - media devices.
- The css is being compatible with both the older and the new versions of the languages which are being used today.
- The maintenance of the websites become much easier, its look and feel are being more flexible and can be conveniently used by the users.
- Various dynamic and websites templates are easily handled and created with the help of css.

BOOTSTRAP

- It is a front end open source framework of the combination of html, css and js.
- Responsive web applications can be easily created with the help of the classes that are being used in the language.
- Various templates like tables, flex, buttons, forms, navigations, carousels are all being designed
- The ability of creating easy and responsive designs for the web applications can be done using this framework

JAVASCRIPT

- JS helps in designing the custom client side scripts which helps in creating interactive and dynamic web applications.
- Dynamic functionalities can be implemented for the static pages with the help of javascript.

- JS is available in all the main browsers both in client & the server environment.
- JS displays the data based on the users' requirements.
- Various inbuilt functions and events are being used in the content of html in order to provide the dynamic functionality when the functions are executed.

ASP.NET

It is a computer side framework application for web which runs on windows.

Asp.net core is the new version of asp.net which runs on every platform including windows, mac and Linux. The major benefits of the application are its high speed, lower cost with a huge & vast support of most considerable languages.

Asp.net makes use of the most important and popular database like Microsoft sql server, mysql, Maria DB and mongo DB.

It is a great framework which helps in developing websites and web applications.

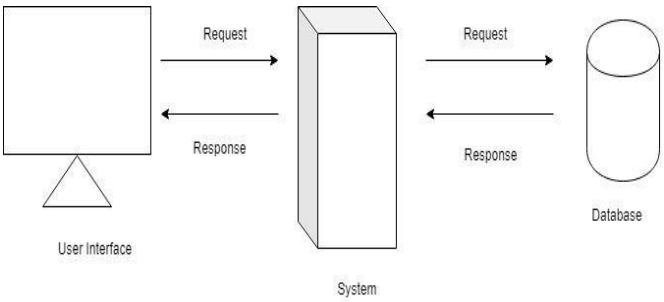
SQL Server 2008

A back end tool which is used in storing and accessing of data Embedded and web applications are most commonly used in SQL Server.

It is a popular and an alternative database which is being used based on its reliability & speed.
Including windows and Linux it can be used for any web servers which essentially works on all major platforms.

The data stored in the tables in the database are similar to the excel spreadsheets, where the database helps the user in accessing and managing the data from the database.

Detail Design:



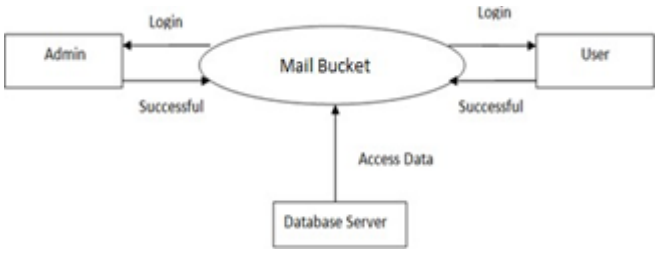
System Perspective Diagram

The architecture diagram can be described as external level, conceptual level and database level.

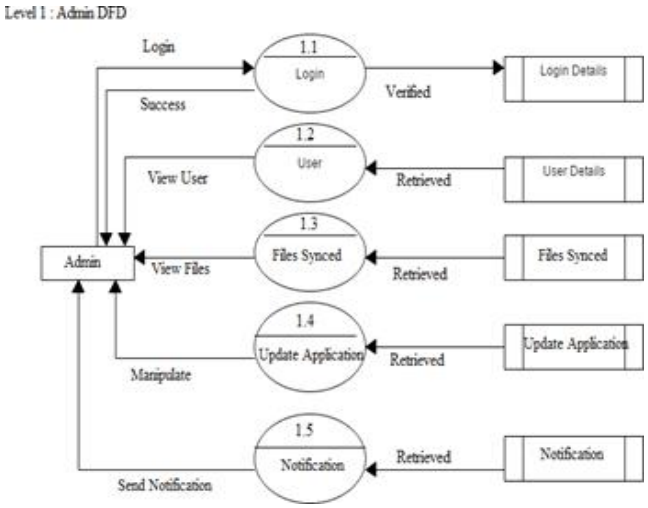
The external level displays the data in the user interface which is also known as physical level.

The conceptual level includes the logics written in order to develop the application.

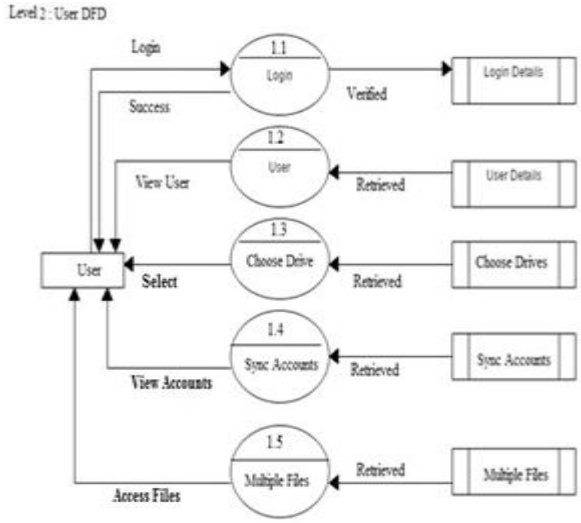
Physical level is the internal level where the database comes into picture and all the data of the application is stored in the database.



Context Diagram of Admin Level 0



Admin Data Flow Diagram Level 1



User Data Flow Diagram of Level 2 Implementation

Implementation is that phase of the project where the abstract plan is cut into a working entity.

The process of implementation should be precisely composed and planned so that there is no ambiguity which may mislead the users.

Implementation includes all those actions that makes the system to be modified and updated compared to the old system.

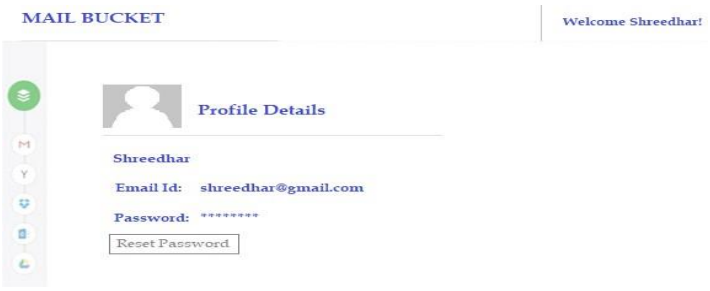
The new system which is being implemented replaces the existing system with more efficiency and reliable according to the users requirements.

The process of establishing a developed system into its actual use is called as System Implementation. The system is being implemented only after the complete testing done on the system so that it is working according to the users requirements.

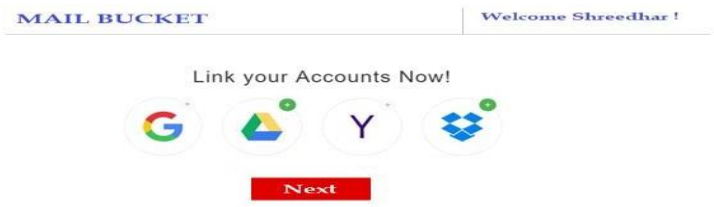
The most important phase of the implementation is producing the new successful structure of the project and providing confidence of the new system for the user which will work effectively and efficiently.

It involves proper planning, the review of the present system that is implemented, its constraints on implementation and design that is implemented.

Registration Form



Profile details



Linking your Accounts.

Syncing your files from other Service Providers

II. CONCLUSION

Having control on the memory of an application is a vital functionality which provides the proper and complete details of the efficient usage and proper file management can be tracked easily. This helps in improving the entire business for storing and managing memory. There are very new and refined techniques in order to maximize the customer service. The application developed is just a short initiation to

handle the memory management and security which can be made better in the future by implementing new functionalities where the application can perform better. The application developed is truly effective which would reduce the complexities of the activities involved in planning, controlling and tracking the details of the files and documents are stored in respective service providers.

III. REFERENCES

[1]. Steven Holzoner "The complete Reference ASP.NET" Indian Edition, Tata McGraw-Hill, 2007.
[2]. Chris Bates "Web programming building internet Application", 3rd edition, Pearson Education, 2008.
[3]. http://www.w3schools.com

Cite this article as :

Prof. Shreedhara N Hegde, Prof. Manjula T. , "Mail Bucket", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 182-186, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194734

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Detection of Attacks in Online Social Networks (OSN)

Prof. Rajesh R M[1], Prof. Prathibha S. B.[2]
[1]Seshadripuram Degree College Tumkur, Karnataka, India
[2]Assistant Professor and HOD Seshadripuram Degree College Tumkur, Karnataka, India

ABSTRACT

Online Social Networks (OSN) attacks are most prevalent and practical attack that cannot be prevented easily. Due to increase in OSN population many users are exposed to many attacks. Attacker uses social media as a channel to launch the attacks. Due to this it is necessary to develop some mechanism to avoid the attacks. So it is essential to do the risk assessment in OSN by assigning the Risk Score to each user in OSN. Risk Score assignment is carried out in two ways. (i) One Phase Risk Assessment based on Group Identification features (ii) Two Phase Risk Assessment based on behaviour features mapping. After calculating the risk score users are categorized as below average (below normal), average (normal), and above average (Malicious) user.

Keywords : OSN Online Social Networks, Risk Assessment, Attacks.

I. INTRODUCTION

Online Social Networks (OSN) is growing field in computer world, it is growing like anything, and it allows users to create accounts in OSN and to share information to other users in the network around the world. OSN also allow user to create both private and public profile encouraging to post the images, videos etc. [1]. The first decade of the twenty first century has witnessed a tremendous growth in the field of communication and information technology, and the penetration of Internet in almost all aspect of our daily life. Within four decades of its introduction in a very crude form called UseNet in 1979, -the Internet has become an integral part of the modern society.

Though there are several popular applications on the web such as E-mail, games, videos, etc., none of these applications make users interested with the Internet the way social media do. The popularity of social media such as Facebook and Twitter has increased several folds in recent years. Social networking sites are attracting a large number of visitors. According to a report, by the Shareaholic website [2], the two social networking sites Facebook and Pinterest attracted over 20% of overall traffic over the Internet, where approximately 73% of adult Internet users access social networking sites as reported in September 2013 (https://blog.shareaholic.com/socialmedia- traffic-trends-01-2014/), and (http://www.pewinternet.org/fact- sheets/social-networkingfact-sheet/).

On social media sites such as Facebook and Twitter some of the users post or tweet and other users, whether- friends or followers may respond to posts by commenting, sharing or re-tweeting, which may be followed by others along the network. These activities constitute online user behaviour and generate a huge amount of data which may be useful in learning models of user behaviour, identifying communities of like-minded users, developing models to understand users' attitudes and predicting future activities of the same set of users. With the ever- increasing popularity of social media, better understanding of users' online

behaviour has become critical for the success of many application development and business houses.

As the number of users on social networking sites is increasing rapidly, the amount of data generated by them are also growing very fast. The large amount of highly unstructured data generated by social media poses several challenges to research community in terms of storage, retrieval and mainly analysis. The analysis of user behaviour can be useful to all stakeholders of network traffic; for example, -to ISP providers in optimizing the traffic pattern, to social media sites to create applications as per user behaviour, and to users to understand the behaviour of normal users and malicious users. In order to design an effective model for using social media in teaching and education in general, this paper aims to analyse and model the user behaviour on social media.

In other words, social media is an online interactive platform where users can make online social networks, create contents, discuss and share views. As it is clear from the definition of the social media, users can express their views in different forms and formats. Accordingly, social media can be classified into different categories as described below:

Social Networks: Social network sites can be defined as web-based services that allow individuals to construct a public or semi- public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system [3].

Thus the social network websites allow users to connect with friends, colleagues and other users in order to share media, content and communications. Examples of social networks include Facebook, LinkedIn, and Myspace.

As a result, compromised accounts in Online Social Networks (OSNs) are more favourable than Sybil accounts to spammers and other malicious OSN attackers. Malicious parties exploit the well-established connections and trust relationships between the legitimate account owners and their friends, and efficiently distribute spam ads, phishing links, or malware, while avoiding being blocked by the service providers. Offline analyses of tweets and Facebook posts [4], [5] reveal that most spam are distributed via compromised accounts, instead of dedicated spam accounts.

Online social networks like Facebook, LinkedIn, Orkut and such others are vulnerable to various networking threats. One of the majors is Sybil attack, where attackers create and maintain many fake accounts, called Sybils to inject malwares. Since decade, many social- graph-based Sybil defences have been extensively discussed and proposed in the research community. The social-graph- based Sybil defences rely on multiple assumptions but the underlined truth lays strictly on the limited social connections known as attack edges which form between Sybil and non-sybil users. Here, upper bound of Sybil acceptance still depends on the total number of attack edges which shows that if there is increase in the attack edges then it will evade the Sybil detection. As a result, Sybils may be able to develop many attack edges to real users especially because of those few promiscuous non- sybils who are careless to befriending even with strangers. Existing social graph based detection schemes may show major performance drop while dealing with such kind of situation. To overcome such limitation of social graph based Sybil detection, here proposed its extension version by incorporating user behavioural aspects behaviour profile.

People using such services share tremendous amount of personal and sensitive information on such sites. As a result, these services become vulnerable to different kinds of privacy breaches and attacks where a malicious entity tries to steal user's sensitive information or tries to hack into such services and disrupt its normal working. It has been reported that around 10% of total users registered on popular social networking website Facebook are fake users which amounts to approximately 100 million registered

profiles [6]. Also, news has emerged that millions of registered fake accounts were on sale in the market [7]. Rest of Paper is organised as follows. In module 2 discussed the work related to Attack detection techniques based on social graph and user profile behaviour and the attacks related to OSN. In module 3 proposed design is explained in detail. Module 4 discussed the design technique. In module 5 the evaluation factors are discussed.

II. LITERATURE SURVEY

Online Social Networks (OSNs) allow users to create a Public or private profile, encourage sharing information and interests with other users and communicating with Each other. As a result, today's social networks are exposed to many types of privacy and security attacks. Social media are computer-mediated technologies that allow the creating and sharing of information, ideas, career interests and other forms of expression via virtual communities and networks. The variety of stand-alone and built-in social media services currently available introduces challenges of definition. However, there are some common features. [11]

1. Social media are interactive Web
2. Internet-based applications.[12]
2. User-generated content, such as text posts or comments, digital photos or videos, and data generated through all online interactions, are the lifeblood of social media.[12]
3. Users create service-specific profiles for the website or app that are designed and maintained by the social media organization. [11] [12]
4. Social media facilitate the development of online social networks by connecting a user's profile with those of other individuals and/or groups. [13]

Although there is a dramatic increase in OSN usage – Facebook, for instance, has now 1.55 billion monthly active users, 1.31 billion mobile users, and 1.01 billion daily users1 there are also a lot of security/privacy concerns. One of the main sources of these concerns is that OSN users establish new relationships with unknown people with the result of exposure of a huge amount of personal data [14]. Unfortunately, very often users are not aware of this exposure as well as the serious consequences this might have. Also, some users are less concerned about information privacy; therefore, they post more sensitive information on their profiles without specifying appropriate privacy settings and this can lead to security risks [15].

As a result, today's social networks are exposed to many types of privacy and security attacks. These attacks exploit the OSN infrastructures to collect and expose personal information about their users, by, as an example, successfully convincing them to click on specific malicious links with the aim of propagating these links in the network [15]. These attacks can either target user's personal information as well as the personal information of their friends. Another widely used attack is the generation of fake profiles, which are generated with the sole purpose of spreading malicious Content. In addition, there is a growing underground market on OSNs for malicious activities in that, for just a few cents, you can buy Facebook likes, share, Twitter followers, and fake accounts. Although many solutions, targeting one specific kind of attacks, have been recently proposed, having a more general solution that can cope with the main privacy/security attacks that can be perpetrated using the social network graph is missing.

2.1 Types of Attacks

- Sybil attacks.
- Identity clone attacks.
- Compromised accounts attacks.
- Socware attacks.
- Creepers attacks.
- Cyberbullying attacks.
- Clickjacking attacks.

Sybil attacks: - To launch a Sybil attack, a malicious user has to create multiple fake identities.

Identity clone attacks: - In this type of attack, malicious user creates similar or even identical profiles to impersonate victims in an OSN.

Compromised accounts attacks: - Compromised Accounts Are accounts where legitimate users have lost complete or partial control of their login credentials.

Socware attacks: - In this type of attack, an adversary creates malware items, called Socware, in the form of applications, Pages or events containing malicious links to be propagated in the OSN.

Creepers attacks: - Creepers are real users they might send friend requests to many strangers or posting spammy advertisements by selling the accounts temporarily.

Cyberbullying attacks: - Attackers harass their Victims (usually children and teenagers) by posting sexual Remarks, threats, or repeated hurtful messages.

Clickjacking attacks: - In this kind of attacks, attackers. Trick users into clicking some items different from what they intended to click. Then, the attacker can manage the User's account by posting spam messages and performing Likes on some items.

III. DESIGN TECHNIQUE

We recall that the aim of the first.

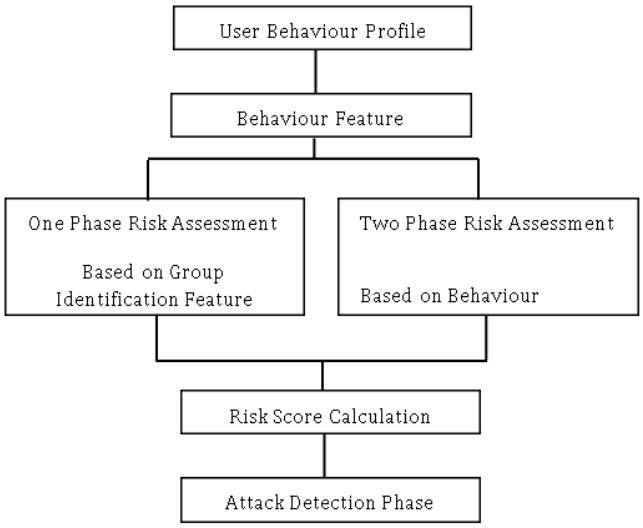


Fig: 3.1 Architecture for Attack Detection Phase

Clustering is to group users for which similar behaviours are expected. At this purpose, group identification (GI) features should be those that are greatly discriminating, likes age, gender, but also those that impact the possible users' behaviours, like, education and nationality. In addition to these features, we have to take into account that even if in the real world people with similar background usually behave in similar way, in an OSN this might be impacted by the users' attitude towards online social networks that might be different even for similar users. For this reason, in addition to profile information (i.e., age, gender, education, nationality), in order to measure users' attitude in online socialization, GI features also include the following:

Fig 3.1 shows the Architecture of the proposed system, input for the system is the Behaviour Profile, based on this the Behaviour Features (BF) are calculated after this BFs are used to do the Risk Assessment. Here Risk Assessment is carried out in two phases. One Phase Risk Assessment and Two Phase Risk Assessment. Based on this output the attacks are categorized and in attack detection phase attacks are detected and reported to Admin.

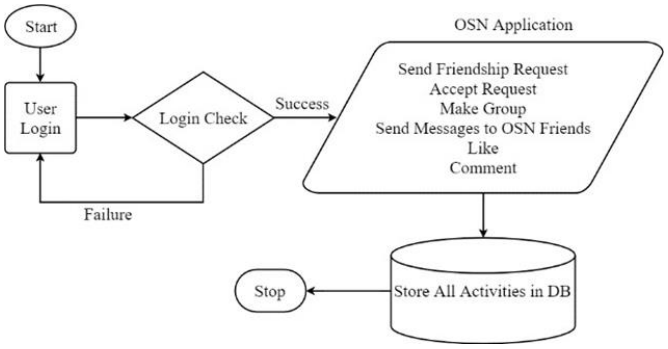


Fig 3.2 User activity Flow Diagram

Figure 3.2 shows the A flowchart is a graphic illustration showing the flow of stages in a program, individuals in an Organization. A flowchart specifies arrangements and choice points as well as initial and ending points. Meanwhile it is easier to hold associations in a pictorial form than in a verbal picture, flowcharts can avoid the oversight of stages in a procedure. Flowcharts are predominantly useful for instructional designers who are beginner or infrequent programmers.

In this application user login to the application first if it is success OSN allow user to do the activities such as user can send Friendship request, accept request, like, comment, post the images, create groups, send messages and do replay to the messages. All these activities are recorded in the database.

3.1 ONE PHASE RISK ASSESSMENT

In One Phase Risk Assessment Phase the Group Identification (GI) Features are considered to detect the attacks in the OSN. GI feature includes the following

• Number of Friends: Here the popular user is accepting request form strangers than the normal or private user. This is one of the features that can be considered in attack detection phase.

• Activity Level: This activity features like, comment and posts by the user and other item for which this user does like, comment and sharing of the posts.

• Percentage of Public item in OSN: Some posts in the OSN are public items. These items can be accessed by anyone in the OSN, so attacker makes use of this thing to propagate the malicious items. So that we need to consider these items too.

3.2 TWO PHASE RISK ASSESSMENT

In Two Phase Risk Assessment Phase Behaviour Feature mapping is done based on the attacks. In this phase I considering the attacks so that need to map the Behaviour Features to the Sybils attacks. The BF's that are to be considered for mapping in done in two ways

• Attack Detection (Dense Graph) in this the Behaviour Features like Comment Rate, Started Comments, Post Rate, Post Propagation Speed, Like Propagation Speed, Comment Feedback Ratio, Post Feedback Ratio, Out In Ratio, Like Rate Like Propagation Ratio and Post Rate Post Propagation are considered to calculate the risk score.

• Attack Detection (Sparse Graph) Group Identification Features, Friendship Ratio, Mutual Friend Ratio, Comment Rate,

Started Comments, Post Rate, Post Propagation Speed, Like Propagation Speed, Comment Feedback Ratio, Post Feedback Ratio, Out In Ratio, Like Rate Like Propagation Ratio and Post Rate Post Propagation are considered to calculate the User risk score.

3.3 Calculation of risk score

This section aimed with some significant procedures of spreading such as mean deviation, variance etc., of the user in the OSN and finally analysis of frequency distributions.

Mean deviation for ungrouped data: For n observation of user u1, u2,..un, the mean deviation about their mean of user u is given by

$$\text{M.D}(\bar{u}) = \frac{\sum |ui - \bar{u}|}{n} \qquad (1)$$

Mean deviation about their median M is given by

$$\text{M.D}(\text{M}) = \frac{\sum |ui - M|}{n} \qquad (2)$$

Mean deviation for discrete frequency distribution Let the given data consist of discrete observations u1, u2... un occurring with frequencies f 1, f 2 , ... , fn , respectively.

$$\text{M.D (M)} = \frac{\sum fi\,|ui-\overline{u}\,|}{\sum fi} = \frac{\sum fi\,|ui-\overline{u}\,|}{n}$$

$$\text{M.D (M)} = \frac{\sum fi|ui-M\,|}{n} \qquad (3)$$

Once the mean, median, and deviation is obtained the risk score is calculated as shown below.

3.4 Clustering of Users.

An Expectation-Maximization (EM) algorithm is an iterative method for finding maximum likelihood or maximum a posteriori (MAP) estimates of parameters in statistical models, where the model depends on unobserved latent variables. The EM iteration alternates between performing an expectation (E) step, which creates a function for the expectation of the log-likelihood evaluated using the current estimate for the parameters, and a maximization (M) step, which computes parameters maximizing the expected log-likelihood found on the E step. These parameter-estimates are then used to determine the distribution of the latent variables in the next E step. Filtering and smoothing EM algorithms arise by repeating the following two-step procedure.

E-Step

Operate a minimum-variance smoother designed with current parameter estimates to obtain updated state estimates i.e. the mean and variance of the obtained value is given as input.

M-Step

Use the filtered or smoothed state estimates within maximum-likelihood calculations to obtain updated parameter estimates.

3.5 Gaussian Mixture Model

A Gaussian Mixture Model (GMM) is a parametric probability density function represented as a weighted sum of Gaussian component densities. GMMs are commonly used as a parametric model of the probability distribution of continuous measurements or features in the Risk Assessment Phase. The below formula is used to calculate the risk score i.e. the probability value using the below formula.

$$p(x) = \sum_{i=0}^{k} \pi_i f_i(x)$$

Where p(x) is the probability value is called the risk score of a user.

After calculation of the user risk score the user are clustered, clustering means users are grouped together based on their risk score. In order to do this the threshold value is fixed to do clustering. If the user is below the threshold value, they are called below average user if value is above threshold value users are grouped as a malicious user in case of One Phase Clustering. In Two phase clustering Behaviour Features are mapped to calculate the Risk Score. If the score obtained above the threshold, then it is considered that Sybil attacks may be launched by the user. Here everything is based on the user behaviour profile. The input is the user risk score and output is the detection alert to the admin. Once the attack is detected the admin will take an action.

IV.CONCLUSION

In this paper, One Phase Risk Assessment and Two Phase Risk Assessment is discussed. These approaches are based on risk estimation of the user based on the User Behaviour Features in the OSN by calculating risk score to each user in the network. If the user behaviours are diverged from normal behaviour it is grouped as below average, normal, and abnormal behaviour based on the threshold value.

V. REFERENCES

[1]. N. Laleh, B. Carminati, and E. Ferrari, “Risk assessment in social networks based on user anomalous behaviour,” IEEE Transactions on Dependable and Secure Com- puting, 2016.

[2]. A. M. Kaplan and M. Haenlein, Users of the world, unite! the challenges and opportunities of social media," Business horizons, vol. 53, no. 1, pp. 59-68, 2010}.

[3]. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, Detecting and char- acterizing social spam campaigns," in Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, pp. 35-47, ACM, 2010.

[4]. C. Grier, K. Thomas, V. Paxson, and M. Zhang, @ spam: the underground on 140 characters or less," in Proceedings of the 17th ACM conference on Computer and communications security, pp. 27-37, ACM, 2010.

[5]. J. Jiang, C. Wilson, X. Wang, W. Sha, P. Huang, Y. Dai, and B. Y. Zhao, “Under- standing latent interactions in online social networks,” ACM Transactions on the Web (TWEB), vol. 7, no. 4, p. 18, 2013.

[6]. J. R. Douceur, The sybil attack," in International Workshop on Peer-to-Peer Systems, pp. 251-260, Springer, 2002.

[7]. H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, “Sybilguard: defending against sybil attacks via social networks,” in ACM SIGCOMM Computer Communication Review, vol. 36, pp. 267- 278, ACM, 2006.

[8]. H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, Sybillimit: A near-optimal social network defense against sybil attacks," in Security and Privacy, 2008. SP 2008. IEEE Symposium on, pp. 3,17, IEEE, 2008.

[9]. D. N. Tran, B. Min, J. Li, and L. Subramanian, “Sybil-resilient online content voting.," in NSDI, vol. 9, pp. 15-28, 2009.

[10]. G. Danezis and P. Mittal, “Sybilinfer: Detecting sybil nodes using social networks”, in NDSS, San Diego, CA, 2009.

[11]. L. Jin, X. Long, H. Takabi, and J. Joshi, “Sybil attacks vs identity clone attacks in online social networks,” Pittsburgh: University of Pittsburgh, 2012. international conference on World wide web, pp. 551-560, ACM, 2009.

[12]. M. Fire, R. Goldschmidt, and Y. Elovici, “Online social networks: threats and solutions” IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2019, 2036, 2014.

[13]. L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, “All your contacts are belong to us: automated identity theft attacks on social networks,” in Proceedings of the 18th

[14]. B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, “An analysis of social network-based sybil defenses,” ACM SIGCOMM Computer Communication Review, vol. 40, no. 4, pp. 363{374, 2010.

[15]. V. Dave, S. Guha, and Y. Zhang, “Catching click-spam in search ad net- works,” in Proceedings of the 2013 ACM SIGSAC conference on Computer & com- munications security, pp. 765{776, ACM, 2013.

Cite this Article

Prof. Rajesh R M, Prof. Prathibha S. B., "Detection of Attacks in Online Social Networks (OSN)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 187-193, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194735

National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Survey on E-Voting Protocol with Decentralisation and Voter Privacy

Prof. Pushpanjali C H, Prof. Anuradha K N
Seshadripuram Degree College Tumkur, Karnataka, India

ABSTRACT

Technology has positive impacts on many aspects of our social life. Designing a 24 hour globally connected architecture enables ease of access to a variety of resources and services. Furthermore, technology like the Internet has been a fertile ground for innovation and creativity. One such disruptive innovation is blockchain – a keystone of cryptocurrencies. The blockchain technology is presented as a game changer for many of the existing and emerging technologies/services. With its immutability property and decentralised architecture, it is taking centre stage in many services as an equalisation factor to the current parity between consumers and large corporations/governments. One potential application of the blockchain is in e-voting schemes. The objective of such a scheme would be to provide a decentralised architecture to run and support a voting scheme that is open, fair, and independently verifiable. In this paper, we propose a potential new e-voting protocol that utilises the blockchain as a transparent ballot box. The protocol has been designed to adhere to fundamental e-voting properties as well as offer a degree of decentralisation and allow for the voter to change/update their vote (within the permissible voting period). This paper highlights the pros and cons of using blockchain for such a proposal from a practical point view in both development/deployment and usage contexts. Concluding the paper is a potential roadmap for blockchain technology to be able to support complex applications.

Keywords : E-Voting, Decentralisation, Voter Privacy, Equalisation

I. INTRODUCTION

Voting, whether traditional ballet based or electronic voting (e-voting), is what modern democracies are built upon. In recent years voter apathy has been increasing, especially among the younger computer/tech savvy generation [1]. E-voting is pushed as a potential solution to attract young voters [2, 3]. For a robust e-voting scheme, a number of functional and security requirements are specified [4]–[6] including transparency, accuracy, auditability, system and data integrity, secrecy/privacy, availability, and distribution of authority. Blockchain technology is supported by a distributed network consisting of a large number of interconnected nodes. Each of these nodes have their own copy of the distributed ledger that contains the full history of all transactions the network has processed. There is no single authority that controls the network. If the majority of the nodes agree, they accept a transaction. This network allows users to remain anonymous. A basic analysis of the blockchain technology (including smart contracts) suggests that it is a suitable basis for e-voting and, moreover, it could have the potential to make e-voting more acceptable and reliable. There are number of papers that have explored this idea [7]–[9] including now this one.

Obvious advantages of e-voting using blockchains includes:

i) greater transparency due to open and distributed ledgers,
ii) inherent anonymity ,
iii) security and reliability (especially against Denial of Service Attacks)
iv) immutability (strong integrity for the voting scheme and individual votes).

Existing works explore how blockchains can be used to improve the evoting schemes or provide some strong guarantees of the above listed requirements. However, these papers do not discuss the implementation challenges and limitations of the blockchain (and smart contract) technologies at their current state to fully support a large scale voting scheme. In this paper we explore both the possibilities of an e-voting scheme, along with the challenges and limitation of the blockchain technology in the e-voting context. A. Contribution of the Paper Contributions of the paper can be summed up as below:
1) The paper proposes an e-voting scheme based on blockchain technology that meets the fundamental e-voting properties whilst, at the same time, provides a degree of decentralisation and places as much control of the process in the hands of the voters as was deemed possible.
2) Discussion on the implementation challenges and underlying platform's (blockchain and smart contracts) limitation to support the e-voting proposal.

II. PROPOSED PROTOCOL

The motivation behind the proposed e-voting protocol, is to have a blockchain based scheme that meets the above stated goals. In addition to those properties the protocol must allow for a voter to change one's mind and cancel one's vote, replacing it with another. As a secondary goal, it has been actively pursued to provide the maximum degree of decentralisation and to create a protocol which the voters control as a network of peers. After careful consideration, however, it was decided that a certain degree of centralisation is necessary to reach the primary goal. This is because when using the blockchain, one is unable to store secret information in the public ledger without the use of external oracles that maintain such information. So if the identity of the voters is to remain secret, whilst at the same time permitting only eligible voters to participate in the elections, a Central Authority needs to be introduced that acts as a trusted third party.

The proposed voting protocol utilises the blockchain to store the cast ballots, therefore in this context the blockchain acts as a transparent ballot box. The main reason for using the blockchain in an e-voting protocol is to take advantage of the fact that it enables a group of people to maintain a public database, that is owned, updated, and maintained by every user, but controlled by no one. Since the protocol is based on the blockchain, it will be realised as a network of peers. Each voter will be a peer i.e. a node in a network of equals. Every voter will be responsible for making sure that fraudulent votes are rejected, hence that consensus is maintained according to the election rules. The blockchain also has the additional advantage of being increasingly well-known and well-trusted to operate as intended, as evidenced by the sheer size of the cryptocurrency market.

III. CONCLUSION

E-voting, as discussed in the paper, is a potential solution to the lack of interest in voting amongst the young tech savvy population. For e-voting to become more open, transparent, and independently auditable, a potential solution would be base it on blockchain technology. This paper explores the potential of the blockchain technology and its usefulness in the e-voting scheme. The paper proposes an e-voting scheme, which is then implemented. The implementation and related performance measurements are given in the paper along with the challenges presented by the blockchain platform to develop a complex application like e-voting. The paper

highlights some shortcomings and presents two potential paths forward to improve the underlying platform (blockchain technology) to support e-voting and other similar applications. Blockchain technology has a lot of promise; however, in its current state it might not reach its full potential. There needs to be concerted effort in the core blockchain technology research to improve is features and support for complex applications that can execute within the blockchain network.

IV. REFERENCES

[1]. L. C. Schaupp and L. Carter, "E-voting: from apathy to adoption," Journal of Enterprise Information Management, vol. 18, no. 5, pp. 586–601, 2005.

[2]. W. D. Eggers, Government 2.0: Using technology to improve education, cut red tape, reduce gridlock, and enhance democracy. Rowman & Littlefield, 2007.

[3]. T. M. Harrison, T. A. Pardo, and M. Cook, "Creating open government ecosystems: A research and development agenda," Future Internet, vol. 4, no. 4, pp. 900–928, 2012.

[4]. K.-H. Wang, S. K. Mondal, K. Chan, and X. Xie, "A review of contemporary e-voting: Requirements, technology, systems and usability," Data Science and Pattern Recognition, vol. 1, no. 1, pp. 31–47, 2017.

[5]. D. A. Gritzalis, "Principles and requirements for a secure e-voting system," Computers & Security, vol. 21, no. 6, pp. 539–556, 2002.

[6]. R. Anane, R. Freeland, and G. Theodoropoulos, "E-voting requirements and implementation," in The 9th IEEE CEC/EEE 2007. IEEE, 2007, pp. 382–392.

[7]. T. Moura and A. Gomes, "Blockchain voting and its effects on election transparency and voter confidence," in Proceedings of the 18th Annual International Conference on Digital Government Research, ser. dg.o '17. New York, NY, USA: ACM, 2017, pp. 574–575. Online]. Available: http://doi.acm.org/10.1145/3085228.3085263

8A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," International Journal of Network Security & Its Applications, vol. 9, no. 3, 2017.

[8]. P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 357–375.

[9]. BitCongress. Control the world from your phone. Online]. Available: http://www.bitcongress.org/BitCongress Whitepaper.pdf

[10]. FollowMyVote.com, Tech. Rep., 2017. Online]. Available: https: //followmyvote.com 12"Tivi

Cite this Article

Prof. Pushpanjali C H, Prof. Anuradha K N, "Survey on E-Voting Protocol with Decentralisation and Voter Privacy", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. , September-October 2019.

Journal URL : http://ijsrcseit.com/CSEIT194736

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 Communication Technology & Network Security (NCCTNS-2019)

Organised by
Bachelor of Computer Application,
KLE Society's S.Nijalingappa College,
Rajajinagar, Bengaluru,, Karnataka, India

Email: editor@ijsrcseit.com, ijsrcseit@gmail.com