Authentication Mechanisms for Preventing Cyber Crime and Providing Security in Cloud

Chaitra K.M, Soniya Tiwari, Pooja Bhardwaj, Tanvi Sharma

*Abstract— **Cloud computing has made life easier for user and business. The "cloud" is a server where data, applications and software are stored and can be accessed from any device as long as we have internet connection. Nowadays, security is the main issue in the cloud computing environment because cyber crime is increasing abruptly. The main motive of this paper is to reduce the cyber crime in cloud computing. Cyber crime is the phenomenon which interrupts the privacy and security for data storage, to overcome this cyber security is introduced. Cyber security is protection from unauthorized access that aimed to exploitation from attackers which destroys information system. The inference of this paper is to focus on authentication mechanisms for providing security and preventing cyber crime activities in the cloud.***

Keywords — Authentication, Security, Encryption , Cyber Crime, Deep Fake, Forensics

I. INTRODUCTION

A. Cybercrime

Cloud is a metaphor for internet. Since from the past years, one of the trending and emerging field in technology is cloud computing. It is defined as a practice of storing, accessing data and application using internet. Nowadays, organization and digital transmission in business without cloud computing is impossible. It was estimated that by the end of 2025, atleast one cloud service will had adopted 75% of business around the world.

Cloud computing provides better flexibility and a good functionality to organizations. The increase in number of cybercrimes and to overcome from this is a challenge to the cloud. The data stored in cloud is attacked by the criminals in business platform and to mount attacks like DOS, DDOS, cloud as a platform for employee misuse, etc. The modern attackers are cyber spies that use traditional Spespionage tactics and distruptive malware to bypass passive defence based on security measure. Cyberattack like the Wannacry/Notepetya Pendemic in the extra ordinary growth of Ransomware are launched by attacker. To detect such attacks, security must transform itself into an active profile hunts. Today's attacks are increasing as aggressively as it predicts the threats for tomorrow. To predict and detect attacks, security must be provided to the cloud.

Cloud security must create a collaborative approach that analyze the normal events stream and abnormal activities across users to built a global threat to monitoring system. This technology connects and analyze unfiltered endpoint data using the power of cloud to make prediction and protect against unknown attacks. Intrusion detection system is implemented for monitoring purpose. There is a new approach in cloud security i.e. predictive security. It works like a Counter Intelligence agency that hunts the species before their attacks.

B. Authentication

- Aadhaar

Aadhaar is a unique identity number of twelve digit that is obtained by residents of India made on the basis of their biometrics and demographic data. Cloud sign provides authentication on Aadhaar to eliminate the remembering password and accessing the utility on websites. Some passwords are simple to guess or broken easily. Whenever puzzling passwords are difficult to create and remember then cloud sign provides authentication to give OTP from Unique Identification Authority of India (UIDAI) server as a support of your password. This OTP is used to eliminate the saved password or verify key whenever we access the cloud sign service. Cloud sign is a private cloud digital signature service for organization to digitally verify, sign and share documents [1].

SHA-512 is used for data integrity, non-repudiation, confidentiality and digital signature algorithm per hybrid cryptography through RSA and AES algorithm. It is built by Hadoop framework in java for data store. It supports all file types containing Docx, Doc, XIs, rtf and pdf [1].

When cloud sign converts any file as a pdf which is 25 mb restricted. Cloud computing perform all computation by online technology to provide confidentiality, integrity, availability and non-repudiation. To verify the person's identity Aadhaar authentication can be done by Demographic details i.e. name, address, gender, date of birth along with Aadhaar number, Biometric details i.e. fingerprint, palmprint and iris with One Time Password along with Aadhaar number received on registered phone number [1].

Revised Manuscript Received on April 12, 2019.

Chaitra K.M., Assistant Professor, CSE, JSSATEN, Noida. India. (chaitrakm1987@gmail.com)

Soniya Tiwari, (M.Tech), CSE, JSSATEN, Noida. India (tiwarisoniya7777@gmail.com)

Pooja Bhardwaj, (M.Tech),CSE, JSSATEN, Noida. India (2202bhardwajpooja@gmail.com)

Tanvi Sharma, (M.Tech),CSE, JSSATEN, Noida. India (tanvisharmats54@gmail.com)

DOI: 10.35940/ijitee.F1231.0486S419

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

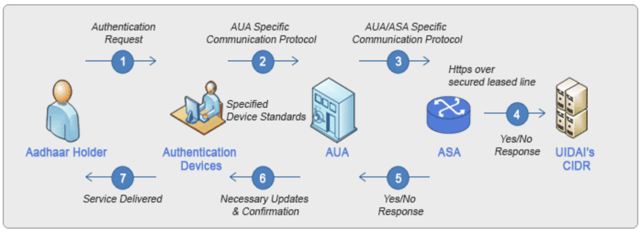

Authentication Request
AUA Specific Communication Protocol
AUA/ASA Specific Communication Protocol
1
2
3
Https over secured leased line
Specified Device Standards
4
Yes/No Response
Aadhaar Holder
Authentication Devices
AUA
ASA
UIDAI's CIDR
7
6
5
Service Delivered
Necessary Updates & Confirmation
Yes/No Response

Fig 1. Operational Model of Aadhaar Authentication

- Biometrics

The term “Biometrics” is the mixture of two Greek words ‘Bios’ meaning Life and ‘metrics’ meaning Measure.

It is mainly used to authenticate and determine a person’s identity analyzing and measuring the biological traits such as physiological and behavioral characteristic. Physiological characteristics are related to body parts like birth mark, fingers, hands, eyes whereas behavioral characteristics are related to behavior of a person such as hand writing, walk, voice etc.

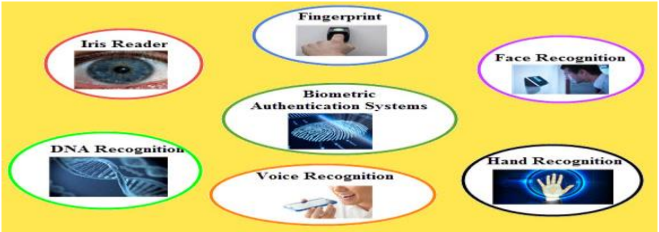


Fig 2. Types of Biometric Authentication

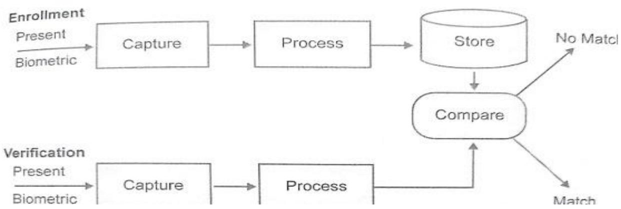


Fig 3. Biometric Authentication Process

Biometric systems are prone to false rejection and false acceptance rates.

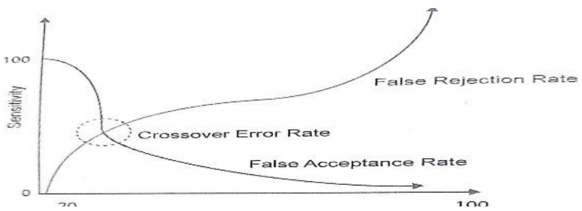


Fig 4. Error and Sensitivity Graph

There are different types of biometric authentication such as Fingerprint scanner, Retina scanner, Iris scanner, Voice recognition, Vein recognition, Signature recognition. Benefits of biometrics are availability, acceptability, performance, accuracy etc.

Dr. G. Jaspher Willsie Kathrine proposed a Smart card user authentication scheme to improve security so that it can be used in future mobile schemes. Biometric data device is provided by users in system which is assumed. Moreover, registration phase is the mandatory phase that exist in proposed key user is supposed to enter the biometric data service provider database in the registration phase. In his proposed scheme an identifier is used for every user which is based on integration of data and user name. thus, this scheme proved to be scalable for large users. The combination and computation cost are less which makes it to be used for mobile cloud users [2].

C. Security

Issues and solutions in cloud computing environment are

- Visibility

The security team faces challenge in tracking who is accessing what across the organization and where they are.

By use of Auto Discovery technology through API, we can overcome this issue.[4]

- Cloud Expertise

Security in cloud is major challenge to accomplish because the cloud service provider is not able to provide good quality of security to the customer.

By hiring people with complete knowledge about the cloud security and finding cloud security expertise to solve this.

- Configuration

Vulnerability do not protect deploying applications and data in cloud infrastructures. Cloud Workloads have their own vulnerabilities which are risky assets because traditional security solutions do not integrate Cloud Workload Protection technology.

An automated vulnerability management solution to monitor your environment continuously for your workloads security to the use of deploy and configure a standardized architecture that meets the Center for Internet Security (CIS) AWS Foundations Benchmark and CIS Microsoft Azure Foundation Benchmark.

- Training

Best practices give the better result in cyber world to secure the companies environment from misconfigurations.

Annual training is not enough because technologies are evolving. You must set up a long-term plan with customized training regarding each environment needs and data access.

D. Cyber Laws

Cyber laws are the laws used to deal with the legal issues associated with the use of cyberspace, internet and communication technology. Fraud, theft, forgery, defamation and other similar criminal activities are involved in cybercrimes which are subject to the Indian Penal Code (IPC). A cybercriminal uses a computer as tool or target object or both to commit cybercrime. Cyber Laws deal with cybercrimes where computer used as a target or weapon. Development of several new e-commerce systems, such as online shopping portals, online banking, online wallets, e-learning, and online marketing, has opened many doors to welcome cybercriminals. It happens because of cash transactions. So, it was mandatory to introduced some legal system that prevent and avoid fraudulent activities.

The most important Cyber Laws is Information Technology (IT) Act, 2000 which contains 13 chapters and 94 sections and 4 schedules. In 2008, the IT Act was Amended and now contains 14 chapters covering 124 sections. This Amendment replaced schedules I and II and deleted schedules III and IV of IT Act, 2000.

The IT Act 2000 handles concerns, such as legal recognition of digital signatures, legal recognition of electronic records, secured digital signature, secure electronic record, and license issued digital signature certificates.

II. RELATED WORK

A. Deepfake

Deepfake is combination of two words Deep learning and Fake. It is a technique based on Artificial Intelligence used for human image synthesis. By the use of Machine Learning technics called Generative Adversarial Network (GAN), the videos and images can be superimposed and combined into source image and video. It can manipulate existing and source videos or images that illustrate people performing actions and say things that never happen in reality. It is generally used for harassing or revenge purpose such as pornography, fake news, malicious scam [5].

One of the techniques of deepfake is Morphing. It is a technique which converts images or videos into other seamlessly without any noticeable change using a computer. It is done by coupling image wrapping with color interpolation. It is used in animation, games, motion picture, interactive UI designing etc [3].

Photo morphing is the technique used in cybercrime. No one can stay out of the reach of morphing if images are publically available on public platforms, anyone can misuse them and morph according to wrong intension and the victim becomes Xenophobic.

According to the literature review, information security is a major issue in computing world. There are various technologies used for data security such as Data Masking, Backups, Data Erasure. The most commonly used for method for securing information are encryption and authentication and alternatives to this is information hiding. Steganography and Digital Watermark are the two technologies used for information hiding in this the secret messages hidded and protected by covere message which embedded secretly called Stegodata in Steganography. To ensure the security, stegodata should be kept closed to cover message else existence secret message will be detected easily [3].

B. Digital Forensic

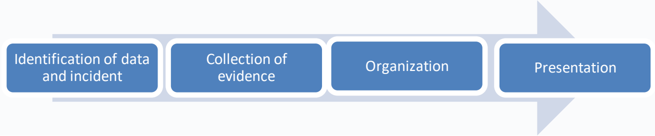
It is application of science that deals with the four procedures in cloud i.e. collection, organization, identification and presentation of evidence [4].

It maintains the data and preserves the integrity of the information during analysis. It has five essential characteristics i.e. broad network access, resource pooling, on demand service and rapid elasticity. It is found that cloud forensics is subset of network forensics. In public and private network, the network forensic deals with forensic investigations and cloud computing is based on multi access network. Thus, the main phase of network forensic process are as followed by cloud forensics in each phase of cloud computing environment [4].

Issues with cloud forensic:

In the cloud computing environment the forensic is not able to complete events where some are access logs, deletion of information, legal issues, volatile data, dependency on cloud service provider, not easily accessible to network routers, reinforcement and multitenancy.

Digital Forensics procedures are [4]



C. Encryption

Cloud computing is a utility which was available on internet, so due to various issues are arrived like user privacy, user theft, leakage, eavesdropping, unauthenticated access and various attacks are raised. To solve the security issues of authentication, privacy, data protection and data verification are main hindrance in cloud computing. We adopt the secure architecture and mechanism for it. There are three mechanism of security control: Authentication, encryption and data verification. Digital signature provide authentication, encryption algorithm which gives encrypted key. This key is used to encrypted/decrypted data which was saved in cloud to maintain the integrity of data [9].

To check data integrity there are simple methods that are efficiently implemented for the users. The main problem between customer and TPA is trust which was solved. This can be done by calculating the hash value of the data by customer itself and this computed hash value are locally stored in hash repository which was created by customer [10].

This method lets the user to conclude hash digest and then upload the file for stored in cloud. In this cloud, data is encrypted and stored all the saved value, this stored value can be easily retrieved from the cloud whenever the customer want to check integrity of data. Data decryption is done at the cloud side and return to the customer. Then the computer hash value was checked by matching the privately stored value. If they are saying integrity of data is maintained and hash value of message is not altered, and if not then the value was altered [10].

- Digital Signature (Digital Code)

It is created and certified by public key encryption which is used to verify the document and also sender identity. Digital Signature is mechanism to provide data authenticity and integrity through authentication and non-repudiation for ease of asymmetric cryptography. It authenticates message received is same as sender created identity. It is created by asymmetric encryption and hashing technique. The receiver signifies the signature validity by public key to decrypt the digital signature, which produced the message digest to original message [6].

Cloud computing supports distributed services multi domain infrastructure and multi user where resources are shared to all server and individual users. Digital signature messages are cryptographically based shared message software into resources and provide non repudiation which ease represented as bit string.

According to Vishal R. Pancholi, some legal requirement for digital signature are Signature authentication, Message authentication and Affirmative act [6].

- AES (Advanced Encryption Standard)

Cloud computing is used in lot of areas, due to this user was face many security issues. Security of information is a crucial issue because of hacking and unauthorized access. To solve this issue various techniques like hash code, victimization has code which enhance authorization process. Nowadays, for safety purposes we use Steganography technique. Steganography is a security mechanism that use the set of rules of symmetric key cryptography. In this AES contains set of rules which are used to offer safety of records. Length of set of rules is 128 bits. After that, new method was introduced for key information security which came to known as Steganography. This file was split in 8 parts and each part was encrypted using set of rules and then all encrypted parts are assists of multi- threading technique concurrently.

AES is a symmetric block cipher that was published by National Institute of Standard Technology (NIST). In encryption AES is heavily used by user. It operates communication on bytes so, it treats 128 bits as 16 bytes. These bytes were arranged properly in rows and column(four) as a matrix. AES cipher specifies the size of key so that number of transformation rounds used in encryption process. [8]

Possible keys for 128 bits keys.
10 rounds for 128 bits keys.
12 rounds for 192 bits keys.
14 rounds for 256 bits keys.

- Cloud VPN (Hosted Virtual Private Network)

It is different from traditional VPN which deploy the network to deliver the VPN services based on cloud. It is globally accessible VPN access to end user through cloud platform over public internet. The main purpose of cloud VPN is to furnish the same level of security. Globally accessible VPN services access without the need of any VPN infrastructure on the user's end. The end user connects to hosted VPN via website/ desktop/mobile app. It charges the customers based on "pay per usages" or "flat free subscription" on the amount of resources utilized [5].

VPN provide data confidentiality and data integrity by encryption. Whenever VPN connected by the use of tunneling mechanism to hide the encrypted data into secure tunnel, with public reader head that can cross a public network. Data integrity in VPN ensure that data has not be altered during transmission. It supports authentication mechanism i.e. Smart Card, Token etc [5].

ANALYSIS RESULTS & DISCUSSIONS

- IDS

It is a passive networks tool/device or application that monitors the network traffic for malicious activities and attempts of legal/unauthorized accesses. The main objective is to warn the user about any suspicious activities. It only logs the relevant information regarding attacks send in alert.

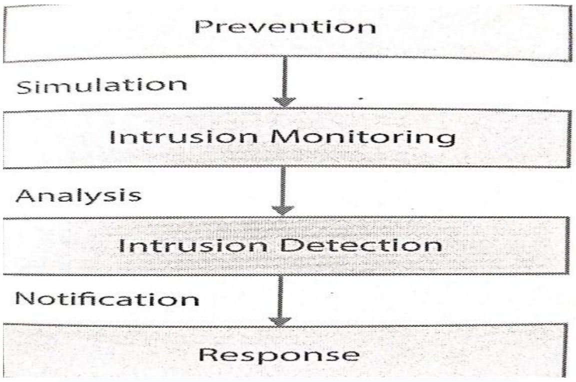


Fig 5. The sequence of the IDS Activities

In cloud, IDS is important for organization to reallocate the services and workload to public cloud infrastructure. For example Amazon Web Services.

- Blowfish

In present day security is the major goal. In cloud to overcome these attacks, there are various encryption techniques like blowfish encryption algorithm for cloud security. Blowfish was designed in 1993 by Bruce Schneier as an encryption algorithm. Blowfish is an encryption algorithm that can be used as replacement of the DES and IDEA algorithm. It is a symmetric private key which acts as block cipher that uses a variable length key. This key contains 32 bits to 448 bits. It is useful for both domestic and exportable purposes. It is faster then DES algorithm and free for use. It comprises with 16 rounds. Blowfish figuring, it is measure of a message is not diverse of 8 bits and then bits are padded [7].

III. CONCLUSION

In this literature survey, we present some authentication mechanism by which security can be enhanced and implemented in the cloud. Cloud computing is the emerging technology, but has some challenges that it must overcome. People often question or doubt about whether their data is secure or not. This paper highlights some laws and methods to make cloud more secure and usable for user.

ACKNOWLEDGMENT

First of all, with due respect we would like to give our special thanks to our Assistant Professor Ms. Chaitra K.M. for her guidance and to give us the opportunity to do this review paper. After collecting the data, we provided measures for implementing security and preventing cybercrime by authentication mechanisms in cloud.

REFERENCES

1. Mohd. Aman Kalyankar, CRS Kumar, "Aadhaar Enabled Secure Private Cloud with Digital Signature as a Service", Coimbatore, India, pp. 533-538, 2018
2. Dr. G. Jaspher Willsie Kathrine, "A secure framework for enhancing user authentication in cloud environment using Biometrics", Coimbatore, India, pp. 283-287, 2017
3. Hiroyuki Nakamura, Qiangfu Zhao, "Information Hiding Based on Image Morphing", Okinawa, Japan, pp. 1585-1590, 2008

4. Shams Zawoad, Ragib Hasan, “Trustworthy Digital Forensics in the Cloud”, pp. 78-81, 2016
5. M. Judith Bellar, “Cloud Computing Security with VPN”, Kodaikanal, India, Vol. 4, pp. 100-103, August 2015
6. Vishal R. Pancholi, Dr. Bhadresh P. Patel, “Improve Security of Cloud Storage using Digital Signature”, Udaipur, Rajasthan and Modasa, Gujarat, Vol. 3, pp. 46-48, October 2016
7. B.Thimma Reddy, K.Bala Chowdappa, S.Raghunath Reddy, “Cloud Security using Blowfish and Key Management Encryption Algorithm”, Vol. 2, pp. 59-62, June 2015
8. Nasarul Islam.K.V, Mohamed Riyas.K.V, “Analysis of Various Encryption Algorithms in Cloud Computing”, Vol. 6, pp. 90-97, July- 2017
9. Prashant Rewagad, Yogita Pawar, “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing”, Gwalior, India, June-2013
10. Shephali Singh , Puneet Sharma, Dr. Deepak Arora, “Data Integrity Check in Cloud Computing using Hash Function”, Lucknow, UP, India, Vol. 8, pp. 1974-1978, May – June 2017

Retrieval Number: F12310486S419/19©BEIESP
DOI: 10.35940/ijitee.F1231.0486S419

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication