Digital Innovations
& Contemporary Research in SCIENCE,
ENGINEERING & TECHNOLOGY
Vol. 10. No. 1, 2022

Article Citation Format
Sarumi, J.A. & Longe, O.B (2022):
Towards Data Storage Security In Cloud Computing Using
Hybridized Advanced Encryption Standard & Authentication Scheme
. Journal of Digital Innovations & Contemporary Research in Science, Engineering
& Technology. Vol. 10 No. 1. Pp 25-48
DOI: https://dx.doi.org/10.22624/AIMS-2001

Article Progress Time Stamps

Article Type: Research Article
Manuscript Received:11th Dec, 2021
Review Type: Blind
Final Acceptance:: 20th February, 2022

Towards Data Storage Security in Cloud Computing Using Hybridized Advanced Encryption Standard & Authentication Scheme

Sarumi, J.A. (PhD) & Longe, O.B. PhD
Department of Computer Technology, Lagos State Polytechnic, Ikorodu, Lagos State, Nigeria
Faculty of Computational Sciences & Informatics, Academic City University College, Accra, Ghana
E-mails: sarumi.j@mylaspotech.edu.ng; Olumide.longe@acity.edu.gh

ABSTRACT

Cloud computing is at the heart of modern day computing and thus the rise in malicious attacks are increasing every day towards it. In recent times hackers have been engaging in different string concept on login fields and phishing in order to intrude cloud accounts. This research is proposed to carry out effective security mechanisms on loopholes in cloud data storage. We intend to engage the use of the Advanced Encryption Standard (AES), security Algorithms like Secure Hash Algorithm 1 & 3 (SHA1, SHA 3) and Message-Digest Algorithm (MDS) and the Standard Authentication Scheme (AS) as sure guide against phishing which when implemented can provide various login stages and codes like OTP (One Time Password) to mitigate attacks. With the application of these methods towards securing cloud computing data there will be less intrusion in accounts and loss of files.

Keywords: Brute-force, Cracking, Hacking, Advanced Encryption Standard, Authentication Scheme, AES, ES, Security

1. INTRODUCTION

Cloud computing is a developing registering worldview that can conceivably offer various imperative points of interest. One of the principal preferences is payment based on service usage evaluation model, where clients pay just as per their utilization of the service. It served as a web based registering. As stated by NIST (United State National Institute of Standard and Technology), cloud computing gives organizational potential benefit which included improved of business outcomes. It is powerfully conveys everything as a service over the web in view of client interest, for example, system, working framework, stockpiling, equipment, programming and assets.

These services are organized into three kinds and also deployed in three models for example, public, hybrid and private clouds. Outsourcing information and associations reduce the weight of nearby information storage and upkeep. In the meantime, while one's information are outsourced, it is essential to identify whether the information is genuinely put away at the right servers and be in place as expressed in "SLA" or Service Level Agreement.

The abuse rank and data breaches in cloud computing storage are among the greatest security challenges facing this technology specifically focusing on security challenges related to shared resources and on-demand nature of cloud computing. Based on report from California data breach record by stated that data breaches resulted due to security weaknesses like proper ways of encoding data. Data availability and confidentiality are perceived generally as major security issue in cloud computing that can easily cause customers to resist themselves from using this technology. Customers access their data frequently or regularly therefore, the data should be available at all the time for usages by the customers.

1.2 Statement of the Problem

The challenges facing the existing system which is based on Data Storage Security in Cloud Computing without AES and Authentication Scheme are in the aspect of malicious intrusion in systems through poor user authentication scheme, and the varying level of encryption / Decryption mode of other algorithm which are way porous and can be manipulated with brute force because they are not salted. Below are some of the enlisted challenges:

i. Lack of adequate Authentication check points before accessing user's account can lead to easy manipulation of the system.
ii. Poor code encryption can be easily bypassed like MD5 and SHA1
iii. Over cloud there are higher degree of volatility in data structure which an encryption without enough strength can be easily hacked.

1.3 Research Objectives

i. Identification of different security threats related to stored data in cloud computing storage.
ii. To achieve the strategies used to safeguard stored data while in cloud storage.
iii. System development using Advanced Encryption Standard as algorithm for data encryption and Authentication Scheme valid user's verification.
iv. Prevention of unauthorized access to all functional units of the system and examination of the significant of using Advance Encryption Standard and Authentication Scheme for ensuring data security while in storage.
v. To develop a reliable system that can manage encrypted data in cloud while providing a decryption method when in need in a secured database.

1.4 Significance of the Study

Data storage in cloud has been a major part in computing world today which a reliable security measures to it is a very crucial need and that has led to me engaging in this research; below are the impacts this research will have on data storage in cloud computing while adopting the Advanced Encryption Standard (AES) and Authentication Scheme.

I The design of AES is efficient for both software and hardware across varieties of platforms.

II It proposed system uses AES encryption algorithm that has uniform and parallel composition of four steps in each round except in the last round.

III While adopting the AES encryption mode it has long key length which is difficult to guess by unauthorized users.

IV The system has block size of 128 bit with strong key scheduling

V The authentication scheme used in the proposed system design and implementation is categorized in to two. Each user has username and password, both are saved in same database, to avoid possibility of unauthorized access to the database, each user has secret key, this help to strengthen authentication scheme. The secret key is in separate and save space with username and password. Despite user login with valid username and password, that doesn't grant access to the system functionality, secret key must be valid.

1.5 Scope of the Study

Our research will cover a broad range of security and cloud computing while adopting the AES and Authentication scheme; below are the key areas this research covers:

i. Cloud computing for storage of data

ii. Security over cloud computing using AES and Authentication scheme

iii. OTP, One Time Password for Authenticating user's account.

iv. The use of secrete key for Authentication.

1.6 DEFINITION OF TERMS

i. **Algorithm**: In mathematics and computer science, an algorithm is an unambiguous specification of how to solve a class of problems. Algorithms can perform calculation, data processing, automated reasoning, and other tasks.

ii. **AES:** The **Advanced Encryption Standard** (**AES**), also known by its original name **Rijndael**, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST).
AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes.

iii. **Authentication Scheme:** It provide a way to collect credentials and determine the identity of a user.

iv. **Bit**: The bit is a basic unit of information in information theory, computing, and digital communications. The name is a portmanteau of binary digit.

v. **Computer:** A **computer** is a device that accepts information (in the form of digitalized data) and manipulates it for some result based on a program or sequence of instructions on how the data is to be processed. Today's **computers** have both kinds of programming.

vi. **Cloud computing:** Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the Internet.

vii. **Data:** Data is a set of values of subjects with respect to qualitative or quantitative variables. Data and information or knowledge are often used interchangeably; however, data becomes information when it is viewed in context or in post-analysis.

viii. **Program:** A computer program is a collection of instructions that performs a specific task when executed by a computer. A computer requires programs to function. A computer program is usually written by a computer programmer in a programming language

ix. **MD5**: The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities.

x. **SHA1 and 3**: The Secure Hash Algorithms are a family of cryptographic hash functions published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard, including: SHA-0: A retronym applied to the original version of the 160-bit hash function published in 1993 under the name "SHA"

xi. **Brute force:** In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

xii. **Phishing**: Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

xiii. **Cracking**: Gaining unauthorized access to computer systems to commit a crime, such as digging into the code to make a copy-protected program run and flooding internet sites, thus denying service to legitimate users.

xiv. **Hacking:** This refers to unauthorized intrusion into a computer or a network.

2. RELATED LITERATURE

The Advanced Encryption Standard (AES) encryption algorithm had some several of itself definition and explanation but all the definition and explanation is established by National Institute of Standards and Technology (NIST) (Patrick D, Gallagher, 2014). In this overview, three types of AES's definitions and explanations from three different sources were discussed. Firstly, the AES is kind of formal encryption technique that had already accepted by worldwide. AES is one kind of the block cipher encryption algorithm; it uses the encryption key to encrypt a few rounds. So a block cipher is an encryption algorithm in a single data block.

Standard AES encryption algorithm block are 128 bits or 16 bytes in length, 192bits or 24bytes and 256 or 32bytes (Vincent Rijm en, et al., 2014). Others way to define the advanced encryption standard (AES) is a specification for the electronic data in encryption (Vincent Rijmen et al., 2014). Again AES encryption is an algorithm used to encrypt as well as decrypt data electronic transmission of data protection purposes. Moreover, AES algorithm allows the use of cipher key that are 128, 192, or 256 bits long and also that are to protect the 16-byte blocks in the data encryption key.

2.1 Data Encryption Standard (DES)

Data Encryption Standard (DES), this is the first time encryption standard by the NIST (United States National Institute of standards and technology) recommended in early 1970s. This DES algorithm is proposed by IBM while other names call LUCIFER (Abdel-Karim Al Tamimi, 2013). DES that is Data Encryption Standard is used 56-bits key and 16 cycle through each key is ranked 48 submarines formed by 56-bit key. When it is decryption, Sub-key in reverse order and it will use the same algorithm. 64- bit block size is L and R block of 32 bits (Milind Mathur et al., 2013). Certainly, there are advantages and disadvantages of DES algorithm. Advantages of DES are it is more fast process in hardware and comparatively fast in software, DES is more easily to learn the details as well as implement it and every five years the Government (United States) will required to renew the certify because this is their official Government standard. While disadvantages of DES are outdated because technology nowadays is more improving every minute by minutes so it is a chance to break the encrypted code. Then, it is slow when implement in software because it not designed for software and it cannot be decrypt the data (Cipher text) if we lost that secret key (Priya Kapoor et al., 2012).

2.2 Concept of Authentication Scheme

For the past two decades, computer networks have grown at an explosive rate. In a wide range of environments, such networks have become a mission critical tool. Organisations are building networks with larger scales than ever before, and the connectivity with the global Internet has become indispensable. Along with this trend has come an explosion in the use of computer networks as a means of illicit access to computer systems (Goyal et al., 2015; Liao et al., 2015). Internet is known as a very powerful platform that changes the way we communicate and perform business transactions in current technology (Syed Idrus et al., 2016; Syed Idrus, 2018). It has now touches every aspect of our lives along with emerging of newer security threats, ready to embark towards the journey of destructions. According to the Internet World Stats, as of June 30, 2012, over 2.4 billion users are using the Internet, and hence the numbers no doubt will keep on increasing.

Thus, the advent of information securities has revolutionised our life particularly with the information that are available, whereby data can easily be accessed and manipulated (Syed Idrus et al., 2014, 2015a). Transmitted information level is becoming more important especially as interactions that used to only be carried out offline, such as bank and commercial exchanges are now being carried out online in the form of Internet banking and electronic commercial exchanges, and damages due to such attacks will be greater. As increasing amounts of personal information are surfacing on the Web, it is essential to remain wary of the risks surrounding the ease in which our private details can be accessed. Social networking and online profiles contribute to this: giving potential intruders a plethora of sensitive information. Insafe reports that more than a quarter of children in Europe have online networking profiles which can be exposed, and with over 900 million people on Facebook alone the danger is widespread (ParrisLong, 2014).

2.3 Definitions of Authentication

Before presenting the different existing methods, we give some definitions and concepts. The concepts listed below are partially based on the result of (Menezes et al., 2016) and (Chabaud and Grumelard, 2016). The authentication process implies different entities:

- The claimant is the entity that authenticates to the system, in order to use the services. It could be a person or an Information System (IS);
- The monitor is the entity that provides an authentication service. It asserts the identity of a claimant (or reject it in case of a wrong authentication) and checks if it can grant him/her the use of the required service;
- The Information System (IS) provides services, such as an access to a computer account, an application, a door unlocking or a network printer, and will let the claimant use its services if the monitor correctly authenticated it (with a given required level of trust).

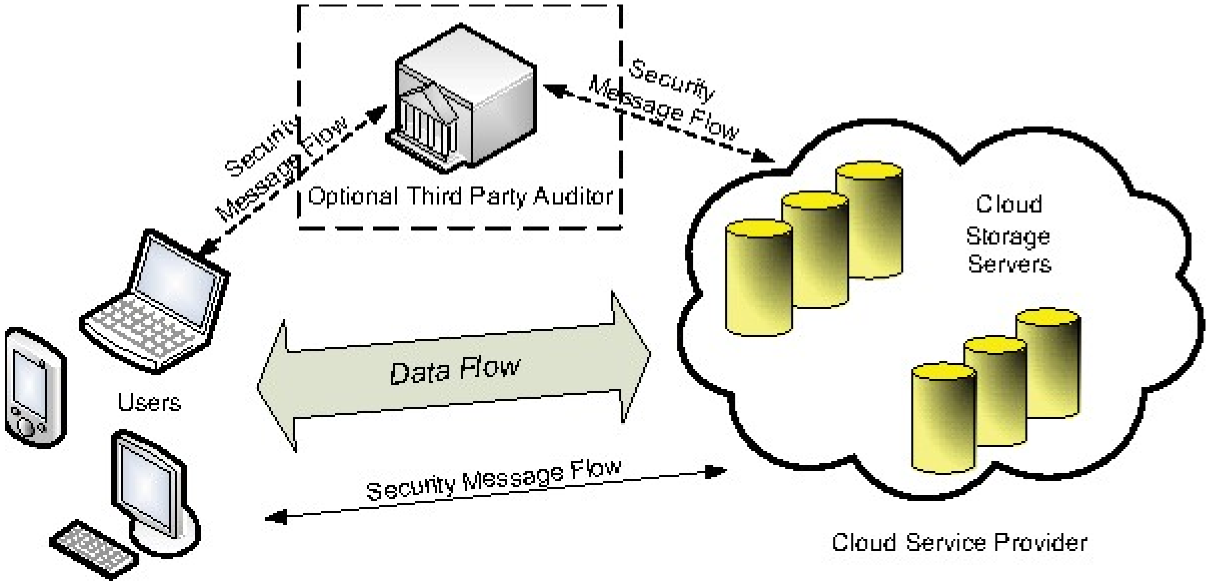

Fig 1: Ensuring data storage security in Cloud Computing
Source: Semanticscholar.org

3. THE AUTHENTICATION CONCEPT

‘Identification’, ‘authentication’ and ‘authorisation’ are three interrelated concepts, which form the core of a security system. Identification is the communication of an identity to an IS. Before authentication, the claimant typically provides the IS an identity anyway (for example, a login or an email address), and the monitor asserts the identity by authentication (for example, using a password). An authentication is a proof given by a claimant to assert a monitor that he/she really corresponds to the identity he/she provided. The monitor then asserts the IS of the identity of the user. Finally, the authorisation is the granted privileges given to the user.

Authentication systems provide the answers to both questions:
(i) who is the user? and
(ii) is the user really who he/she represents himself/herself to be?

Hence, authentication represents one of the most promising way concerning trust and security enhancement for commercial applications. It also denotes a property of ensuring the identity of the previously mentioned entities (Kotzanikolaou and Douligeris, 2017). Besides, authorisation is a process of giving individuals an access to the system objects based on their identity.

Authorisation systems provide the answers to the three questions:
(i) is user U authorised to access resource R?;
(ii) is user U authorised to perform operation O?; and
(iii) is user U authorised to perform operation O on resource R?

There is often a confusion between 'identification', 'authentication' and 'authorisation'. These words/terms do not have the same meaning at all. Each of these concepts requires an enrolment step. Enrolment is the 'registration' of a new user, including the emission of tokens and credentials. Enrolment is a major concern and should also be carefully handled. In the rest of this paper, we will consider the IS has already registered the claimant. Example: Let us consider the same example as the previous one. When the user authenticates himself with his token, he provides his identity by putting his card, which contains an identification number linked to his account. The system does not need to know the full description of the worker, so a simple identification number is enough.

Then, the card authenticates to the reader (for example, by a symmetric cryptographic protocol), to prove the authenticity of the provided identity. Finally, the authorisation will be given to the user to go through the door, if he has the right to do it. Having said that, we then need to have a link between both the claimant and the monitor. This link is denoted channel. A channel is a support of communication between the claimant and the monitor. It can either be considered as confidential, authentic, secure or as insecure. A confidential channel is resistant to interception; an authentic channel is resistant to tampering; a secure channel is resistant to both; and an insecure channel is none. The authentication goal is to assert an identity, but the scope of authentication methods is very large and it can vary in many ways. Below is a list of some of the common authentication methods:

- An ID (IDentification)/password: to open a session on a computer or to authenticate on Internet;
- A PIN (Personal Identification Number) code: to unlock a smartcard;
- An RFID card: for accessing a building;
- A fingerprint: to unlock a door;
- A facial recognition system with a webcam: to open a session on Internet;
- A USB token;
- A one-time password token;

3.1 Triple DES

Triple DES another name is 3DES was proposed is one algorithm that is enhancement of DES (Abdel-Karim Al Tamimi, 2013). And an IBM team is developed it around 1974 while in 1977 it is adopted become standard in national. The triple DES algorithm for just three times in a row with three different keys should be used for expanding the size of DES keys. Combinations to 168-bit key size (3 x 56) have no access to power (Abdel-Karim Al Tamimi, 2013). St the advantages of Triple DES are easily to implement inside both of the hardware and software application, more universal in libraries and most systems and also to fix the weaknesses of DES.

In addition, the disadvantages of 3DES are not support larger key size, not faster implement in both software and hardware and also outdated when the technology is more increasing and also improving fast (Quora, 2014).

3.2 Blowfish

In this algorithm that is provided by Bruce Schneier and it is a domain encryption that most common public. Blowfish is 64-bit algorithm block cipher with a variable length key. So the Blowfish is burn on 1993 that start introduced through publication. This algorithm can be executed on hardware application while mostly it is used in software application refer to Abdel-Karim Al Tamimi (2013). BLOWFISH, it is aim to replace the DES algorithm. From 32 bits to 448 bits, use a variable-length key. Blowfish patents and licenses are not available for free, and can be used free of charge for all. Blowfish is a fast block cipher is one of the most developed to date (Milind Mathur et al., 2013).

The advantages of Blowfish are it is support larger size of key length (32-448 bits), it is a fast block cipher but not included changing keys and there are freely to everyone to used it because it's not set any patents. Another perspective disadvantages are it is not suitable to encrypt the files size 4 GB and not secure if users choosing a weak keys become their secret keys (Bruce Scheier, 2009).

3.2 Advanced Encryption Standard (AES) / Rijindael Algorithm

The Advanced Encryption Standard (AES), this is a symmetric block cipher that uses a symmetric key that can be 128, 192, or 256 data blocks of 128 bits' encryption. AES encrypted the data block when process encryption in 10, 12 and 14 rounds that it depends on the key size.AES encryption is fast and flexible (Milind Mathur et al., 2013)

Otherwise, the advantages of AES are faster executed in both of the hardware and software, it is the latest that required by United States and International Standards and also more securely to use, lastly it support a larger key sizes than others algorithm. Then, disadvantages of AES are difficult to know the details of process because it is too patents encryption and it will difficult to decrypt the data (Cipher text) if lost the secret (private) keys (Quora, 2014).

It was recorded by the research and study done by this great researcher (Selvamani & Jayanthi, 2015) on "A review on cloud data security and its mitigation techniques" which stated that, Cloud customers are permitted to put information into cloud server via distributed storage and reducing weight of protection and recouping in close-by device. Data can be shared by a customer in a social occasion. It is essential to guarantee the uprightness of collective data and the exactness of the dispersed stockpiling. Open assessing instrument is used to survey the exactness of the regular data. Both data proprietor and the Third Party Auditor (TPA) can survey shared data respectability without transferring the data from cloud server.

The “Dynamic remote data auditing for securing big data storage in cloud computing” a research work carried out by (Sookhaka, et al., 2015) stated that, cloud computing has created as another preparing perspective that offers magnificent potential for securing data remotely. In a matter of moments, various affiliations have reduced the heaviness of adjacent data outsourcing in order to stockpile and upkeep data stockpiling to the cloud. In any case, reliability and security of the outsourced data continues involving noteworthy sensitivity toward data proprietors in view of the nonappearance of control and physical responsibility for data. To mitigate from the threat, they proposed remote data evaluating (RDA) techniques. In any case, most of existing RDA strategies is relevant for motionless chronicled data and is not material for inspection on or intensely updating the out-sourced data. Based on work done by (Prasanthi T., 2014) on “Efficient Auditing Protocol for secure Data Storage in Cloud computing” highlighted that cloud computing is increasing more cordiality from both academic and industrial group. It allows on-interest system access to an offer pool of configurable figuring assets.

Clients leave the upkeep of IT administration to cloud service provider who is extremely well regarding giving learning and keep up the IT assets. For the security difficulties, for example, information uprightness and protection, in other to address such issues, they chip away at using the procedures of mystery key based cryptography plan called "Symmetric key cryptography" which empowers Third Party Audit (TPA) to play out his obligation "inspecting" without requesting clients put away information nearby duplicate. Best on their convention, TPA couldn't take in any thought regarding the put away information content in the cloud server amid typical evaluating process.

This can accomplish by incorporating the encryption with hashing. According to research done by (Gadichha, 2013) on “Third Party Auditing (TPA) for Data Storage Security in cloud with RC5 algorithm” highlighted that, cloud computing services improve due to increase in security focuses on resources and centralization of data but the main concern is loss of control over assured of sensitive information and absence of security for stored kernels. Securing stored data in cloud storage is even more needed than in traditional system. To safeguard data correctness, Third Party Auditing is use in place of clients for verification. The fundamental requirements need to meet includes that the auditing process should transport in no any leakage toward users data and should be capable to audit data while in cloud storage in efficient way without requesting any local data copy or additional online burden to the customers.

It was also analyzed that today most of communication occurs electronically. There have been advancements utilizing digital multimedia signals as vehicles for steganographic communication. These signals, which are typically audio, video or still imagery, cover signals. Schemes where the original cover signal is needed to reveal the hidden information are known as cover escrow. Diversity of interchangeable image fragments allows coding of hidden data. For this purpose in every case of comparison with the rank block all domain candidates should be described: one should determine the set of candidates and compare with each element of the set corresponding numerical index. In this case it is sufficient to note, that the losses of secret information are due to the errors of non-correspondence of indices while building-in and restoration. On the other hand, the increase of staganographic efficiency can also be achieved by increase of the number of indices.

The fundamental principle of fractal coding consists of representing an image by a contractive transform of which the fixed point is close to that image block. Davern and Scott in (2012), proposed the use fractal image compression technique to identify the domain blocks and range block of image fractal image compression technique is used to find the self similar structure in the image and they choose a block from one of the two domain sets depending on whether the data bit they are embedding is a one or a zero.

4. CLOUD COMPUTING

Over the past decade, there has been a heightened interest in the adoption of cloud computing by enterprises. Cloud computing promises the potential to reshape the way enterprises acquire and manage their needs for computing resources efficiently and cost-effectively (Marc, 2013). In line with the notion of shared services, cloud computing is considered an innovative model for IT service sourcing that generates value for the adopting enterprises (Lima, 2014). Cloud computing enables enterprises to focus on their core business activities, and, thus, productivity is increased. The adoption of cloud computing is growing rapidly due to the scalability, flexibility, agility, and simplicity it offers to enterprises. A recent cross-sectional survey by (Jeffery,2015) on the adoption rates of cloud computing by enterprises reported that 77% of large enterprises are adopting the cloud, whereas 73% of small and medium-sized enterprises (SMEs) are adopting the cloud.

Cloud computing is “an old idea whose time has (finally) come” (Parker, 2013) The term cloud is old since it was drawn in network diagrams as a metaphor representing the Internet (Jerry, 2016). Cloud computing is generally referred to as providing “Internet-based computing service”; however, the technical meaning is richer, as cloud computing builds on already-existing computing technologies, such as grid computing and virtualization, which are forms of distributed computing technology. Virtualization involves masking the physical characteristics of computing resources to hide the complexity when systems, applications, or end users interact with them. Grid computing is “a model of distributed computing that uses geographically and administratively distant resources, and, thus, users can access computers and data transparently without concern about location, operating system, and account administration”.

With the advent of cloud computing, the merits of virtualization and grid computing have been combined and further improved. Cloud computing shares some characteristics with virtualization and grid computing; however, it still has its own distinguishing characteristics as well as associated risks. Cloud computing has been given numerous definitions since its advent. Basically, definitions started with the notion of an application service provision (ASP) that is an IT sourcing model for renting business applications over the Internet. This definition became wider as Internet-based IT service offerings comprised storage, hosting infrastructure, and network; thus, it is given the name net sourcing, to fit the variety of IT service offerings (Franklyn, 2016). HP defines cloud computing as “Everything as a Service”, while Microsoft perceives the value of cloud computing as “Cloud + Client,” emphasizing the importance of the end user . T-Systems define cloud computing as “the renting of infrastructure and software, as well as bandwidths, under defined service conditions.

These components should be able to be adjusted daily to the needs of the customer and offered with the utmost availability and security. Included in cloud computing are end-2-end service level agreements (SLAs) and use-dependent service invoices".

4. DESCRIPTION OF PRESENT SYSTEM

The present system is a cloud computing platform without AES and Authentication scheme on the storage security; lack of these two proposed security measures on cloud data storage systems has caused loss of files over time as intrusions has occurred time without number where hackers can easily maneuver accounts and sign in to do malicious things. These occurs because the systems lack that double authentication before login which a code is automatically sent to the users email or phone where login is done via running the code. Also, lack of the AES technology on the codes gives room for easy code hacking and cracking.

4.1 Limitation Of Present System

Data control

Information is existing in outside of enterprises base and is realized that, they may loss protection over information. In spite of the fact that the worries are to a great extent speculative and mental as opposed to real, because of the youthfulness of this services, measures of conveyance for services and developing plan of action, clients may have bona fide worries about the service provider reasonability and operational procedures. The new model of data access services or information hosting brings about access control challenge.

Application suitability

A sort of more static information, inert information, for example, applications that incorporate online reinforcement and chronicling is the best fit for distributed storage. The chronicling sort of information functions admirably in the cloud in light of the fact that the information changes less every now and again. This information doesn't require fast value based access. Mass information can be effectively packed utilizing information lessening advances and also it can be effortlessly scrambled.

Data security threat

This is the fundamental reasons for most of the commercial enterprises which kept them down from cloud system services. Data security can be fluctuated like in normal stockpiling or even more. The cloud innovation is a language registering which is conveyed on top of all these corporate systems. Lack of data encryption in cloud storage help to encourage risks in users' data which could lead to the expose of various data information to illegible clients.

4.2 Solution Preferred By The Proposed System

Authentication scheme:

This is the way toward guaranteeing that only valid clients are accessing the information. In cloud, this scheme means to ensure clients are putting away the information by giving a legitimate client name and secret key which is a solitary variable verification strategy utilized. The client needs to demonstrate his or her personality to the cloud administration supplier in order to get access to information put away in cloud.

Data encryption

This is the way toward making plaintext into an indiscernible organization by a client or an outsider. The change made into figure content is unscrambled up to destination. The information is scrambled and put away into the cloud in order to protect the integrity of information while in cloud storage. Cloud service provider offers ways of protecting users' information by using of good encryption scheme.

5. CONCLUDING REMARKS AND FUTURE WORKS

The safety of stored data while in cloud storage is in danger because of several reasons. Despite that the bases under cloud are considerably more solid than individualized computing devices. Store data security issues has been a significant aspect that determined value of service provided by cloud service provider or weaknesses. Data should be put in safe place while maintain it integrity and completeness throughout retention period. There are both internal and external threats that affect the honesty of stored data in cloud storage. Lack of good security techniques for storing data into cloud server or inappropriate mechanism for execution of stored data in a large portion of cloud server can cause data integrity issue. Using a combination of encryption and protection schemes proposed in this work will assure additional security that makes the cloud safe for users. Our future work would geared towards the implementation of these hybridized schemes.

REFERENCES

[1] Kumar, A., Lee, B. G., Lee, H., & Kumari, A. (2012). Secure storage and access of data in cloud computing. 2012 International Conference on ICT Convergence (ICTC).

[2] Rewagad, P., & Pawar, Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.

[3] Ping, Z. L., Liang, S. Q., & Liang, L. X. (2011). RSA Encryption and Digital Signature. 2011 International Conference on Computational and Information Sciences.

[4] Sunita Sharma, Amit Chugh: 'Suvey Paper on Cloud Storage Security'.

[5] Rawal, B. S., & Vivek, S. S. (2017). Secure Cloud Storage and File Sharing. 2017 IEEE International Conference on Smart Cloud (SmartCloud).

[6] Austrialian, A.,(2015) Cloud Computing Security for Tenants , Australia: Australian Government Cyber security center.

[7] Batra, K., Sunitha, C. & Kumar, S., 2013. An Effective data storage security sheme for cloud computing. International Journal of Innovative Research in Communication Engineering, 1(4), pp. 808-810.

[8] Bernabe, J. B. et al., 2014. Semantic- Aware – multitenancy-authorization system for cloud architectures. Future Generation Computer Systems, Volume 32, pp. 154-167. Blumenthal, M. S., 2010. Hide and Seek in the Cloud. IEEE, pp. 57-58.

[9] Borgmann, M. et al., 2012. On the Security of Cloud Storage Services, Germany: Fraunhofer Institute for Secure Information Technology SIT Rheinstraße 75 64295 Darmstadt. Carlson, M., 2009. Cloud Storage Reference Model, s.l.: SNIA Technical Council and the Cloud Storage TWG.

[10] Chadwick, D. W. & Fatema, K., 2012. A privacy preserving authorization system for the Cloud. Journal of Computer and System Sciences, 78(5), pp. 1359-1373.

[11] Evans, M., Huynh, T., Le, K. & Singh, M., 2011. Cloud Storage, Uk: MIS 304 – Fall 2011 Professor: Fang Fang . Gadichha, N. M. Y. a. V. B., 2013. Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3(11), pp. 1032-1037.

[12] Gueron, S., 2012. Intel Advanced Encryption Standard (AES) New instruction set, Israel : Intel Architecture Group, Israel Development Center. Harris, K. D., 2016. California Data Breach Report, United State of America: California Department of Justice. Innovator, 2015.

[13] The Path to Clarity in the Cloud, s.l.: NTT DATA, Inc. 2015_03-FSH-m2cloud. Inukollu, V. N., Arsi, S. & Ravuri, S. R., 2014. Security issues associated with big data in cloud computing. International Journal of Network Security & Its Application (IJNSA), 6(3), p. 46.

[14] Joseph, A. O., Kathrine, J. W. & Vijayan, R., 2014. Cloud security mechanism for data protection. Survey. International Journal of Multimedia and Ubiquitous Engineering, 9(9), p. 84.

[15] Meyer, D. T., Shamma, M., Wires, J. & Zhang, Q., 2014. Fast and Cautious Evolution of Cloud Storage, Columbia: Department of Computer Science Univesity of British. Pachauri, G. & Gupta, S. C., 2014.

[16] Ensuring data integrity in cloud data storage. IJISET- International Journal of Innovative Science, Engineering and Technology, 1(3), p. 54. Parekh, M. D. H. & Sridaran, D. R., 2013.

[17] An Analysis of Security Challenges in cloud copmuting. (IJACSA) International Journal of Advanced Computer Science and Applications,, 4(1), pp. 38- 41. Prasanthi T., B. C. K. S. S. a. K. K., 2014.

[18] An Efficient Auditing Protocol for Secure Data Storage in Cloud Computing. London UK, Proceedings of the World Congress on Engineering Purushothaman, D. & Abburu, D., 2012.

[19] An Approach for Data Storage Security in Cloud Computing. IJCSI International Journal of Computer Science Issues, 9(2), pp. 100-101. Rao, K. N., Naidu, G. K. & Chakka, P., 2011.

[20] A case study of the Agile Software Development Methods, Applicability and implication in industry. International Journal of Software Engineering and Its Applications, 5(2), pp. 35-38.

[21] Sabale, R. G. & Dani, D. A., 2012. Comparative Study of Prototype Model For Software Engineering With System Development Life Cycle. OSR Journal of Engineering (IOSRJEN), 2(7), pp. 22-23. Sarkar, M. K. & Chatterjee, T., 2014. Enhancing Data Storage Security in Cloud Computing Through Steganography. ACEEE Int. J. on Network Security, 5(1), pp. 13-14.

[22] Selvamani, K. & Jayanthi, S. b., 2015. A REVIEW ON CLOUD DATA SECURITY AND ITS MITIGATION TECHNIQUES. Odisha India, Interscience Institute of Management and Technology, Bhubaneswar,. Sharma, S., Sarkar, D. & Gupta, D., 2012. Agile Processes and Methodologies: A Conceptual Study. International Journal on Computer Science and Engineering (IJCSE), 4(5), pp. 893-894.

[23] Singh, R., Kumar, S. & Agrahari, S. K., 2013. Ensuring Data Storage Security in Cloud Computing. International Journal Of Engineering And Computer Science ISSN: 2319-7242 , 2(3), pp. 825- 826. Sommerville, L., 2011.

[24] Software Engineering. Ninth Edition ed. United State of America: Pearson Education, Inc., Permissions Department, 501 Boylston Street, Suite 900, Boston, Massachusetts 02116.. Sookhaka, M., Gania, A., Khanb, M. K. & Buyyac, R., 2015. Dynamic remote data auditing for securing big data storage in cloud computing. Information Sciences, 25 September, pp. 1-16.

[25] Takahashi, K., 2016. Data Integrity and Compliance with CGMP Guidance for Industry, United State: U.S. Department of Health and Human Services Food and Drug Adminis. Center for Drug Evaluation and Research (CDER). Tidke, P. M. P. a. P. B., 2014. Improving Data Integrity for Data Storage Security in Cloud Computing. International Journal of Computer Science and Information Technologies (IJCSIT), 5(5), pp. 6680-6684.