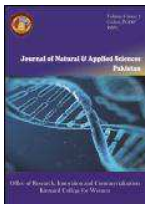
Contents lists available http://www.kinnaird.edu.pk/

Journal of Natural & Applied Sciences Pakistan

Journal homepage: http://jnasp.kinnaird.edu.pk/



SECURITY ISSUES IN CLOUD COMPUTING AND THEIR SOLUTIONS

Iqra Mazhar[1], Humna Shabir [1], Maham Zafar[1], Fatima Zunash Ahmad[1], Dr. Muhammad Rizwan[1*], Aysha Shabbir[1], Maryam Shabbir[1], Dr. Fahad Ahmad[1]
[1]Department of Computer Sciences,
Kinnaird College for Women, Lahore, Pakistan.

Article Info

*Corresponding Author
Tel: +92 333-4881501
Email Id:
muhammad.rizwan@kinnaird.edu.pk

Keywords
Cloud computing, technology, network, saas, paas, iaas, encryption, decryption, cryptography, des, 3des, aes, data security, steganography, security, browser security, cipher.

Abstract
Cloud Computing is the growing technology of providing more and more services and resources online on a shared platform. Problems occur in the implementation and adoption of cloud computing due to security concerns of data being leaked, stolen or lost. Confidentiality, Integrity and Availability (CIA) are the major concerns when dealing with security at cloud environment. There are implemented solutions and precautions to protect the data against CIA assurance like cryptography. In this paper, the various security concerns are discussed along with their solutions, but no one is solely sufficient to secure the data completely. Lastly, we proposed a hybrid approach against the assurance of data integrity at cloud.

1. Introduction

Cloud computing provides a network on which more than one computer or mobile devices are connected. It allows users to use shared resources, and is the future of computing. There are multiple types of cloud like public cloud, private cloud, community cloud and hybrid cloud which have different levels of privacy but all of them are susceptible to intrusion. Cloud computing is a cost-effective method that saves resources and costs by having shared platforms. Cloud computing is beneficial in obtaining platforms on a cloud; instead of buying software, developers can develop programs using compilers on cloud. Cloud has three models: PaaS (Platform as a Service), SaaS (Software as a Service), IaaS (Infrastructure as a Service). SaaS allows for data to be stored on the cloud and accessed when needed.

PaaS allows users to program using cloud resources and develop applications, and finally, IaaS serves to provide the physical media on which data is stored, i.e. through the utilization of hard drive(s). Cloud computing has many benefits and is no doubt one of the fast-growing technologies but it still faces security threats on all these different models and must be implemented in a way that it is secure and reliable so that many users can benefit from it.

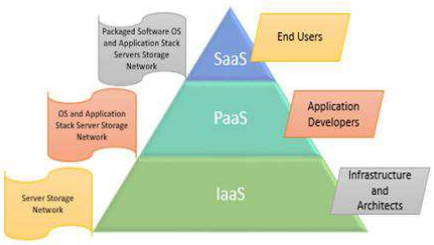


Figure 1. Models of Cloud

2. Problem Statement

Cloud Computing has become very common and it is an emerging technology, but it is plagued with various security issues which pose a threat to the data integrity, consistency, and privacy. The data is transferred and stored onto a remote server— the cloud. Apart from security concerns regarding storage of data such as data loss, abuse, and account hijacking, the main issue is the breach of data. The data is at risk of being accessed by intruders whether they may access the network or the cloud. There is an impending risk of sensitive data being accessed by unauthorized personnel. This makes the data vulnerable to change, being abused, corrupted, or (being) stolen. This is the main concern of data security on cloud. Data breaches make the data susceptible to other critical security issues. This research is intended to provide an overview of the security issues, commonly user security techniques, and by comprehending the lack of security against any single approach, we proposed a hybrid approach to ensure data integrity at cloud.

3. Distinct Security Issues

Cloud Computing Services are established between service providers and consumers through negotiation, known as SLA (Service Level Agreement) and data is accessed through Virtual Machines. Despite being a cost-effective technology that has many benefits for modern technology and its implementations, it faces severe security issues and its data is at risk of being tampered, stolen or lost. Methods should be devised to ensure the implementation of cloud computing in a secure environment.

Some services are given to third party so there may be danger of illegal data access. In cloud computing, users are provided the access to the infrastructure such as the hard drives, which also subjects their data to risks of data loss and data integrity. Hardware malfunction, human error, communication error and disk failure are the threats to the integrity of data stored on cloud [1].

Some solutions for security issues have been proposed and implemented such as the most common solution that comes to mind: encryption and decryption of data. However, the techniques are a bit different than the traditional ones. Image Steganography is the method of hiding information in images to encrypt the data. Another encryption technique is Pixel Key Pattern. Pixel intensity is increased to mark sharp points on an image that reveal a pattern of information.

Data Breaches are also a security threat as clouds have data from multiple vendors and therefore unauthorized personnel can access data from all three models: IaaS, SaaS and PaaS. Encryption and key methods are used but they are not as effective as technology keeps advancing. To prevent the loss of data. Some DLP (Data Loss Prevention) tools have been developed [2].

- Adaptive Redaction – the removal of outbound or inbound sensitive data before it is leaked
- Kernel Level OS Agent Integration – Effective protection at servers (end points) as well as cloud servers
- Structured Data Fingerprinting – used to identify sensitive data quickly
- Email and Cloud Storage Discovery – used to Identify sensitive information in emails and storage servers
- Decryption and re-encryption of Web traffic – to save data from intruders during transmission

Many techniques have been proposed and implemented to ensure security in cloud computing, but there have been problems in these methods [3]. Encryption and decryption schemes have been used but they impose high-costs implications due to bandwidth required for decryption at a local site. Another approach to outsource data, which may cause the owner of the data to be isolated and denied access to his own data. Outsourcing is done by handing over the data to a remote service provider and the owner of the data does not know of his ownership of the data. In case of any hardware failure, it is dependent on the service provider how he deals with remote hard-drive failures. With the increase of storage of data on cloud, traditional techniques are not sufficient to secure the data on cloud.

Some Security Issues based on networks are [4]:

- Port Scanning: HTTP is always open as most connections are established on it, so intruders can access through this port. Solution: Encryption.
- Incomplete Deletion: Multiple copies of data exist as backups on the cloud

and it is possible that the deleted data may exist somewhere as a backup. Solution: Use virtualized private network

- SSL: 'Secure Socket Layer' exists between two communicating layers and may not be configured properly and a third party may access the data. Solution: Proper Configuration.
- Network Sniffing: Unencrypted data may be stolen. Solution: Ingrained encryption.

Some Security Issues based on access are:

- XML Signature Attack: Insertion of a new message in the body of the original.
- Browser Security: Browser cannot generate token of authentication and lead to hacking. Solution: Encryption in transport layer.
- Malware Injection Attack: Malicious data is inserted into the original data. Solution: Use hashing.
- Flooding: Unnecessary messages that stop services from being availed by other users. Solution: Use scheduling.

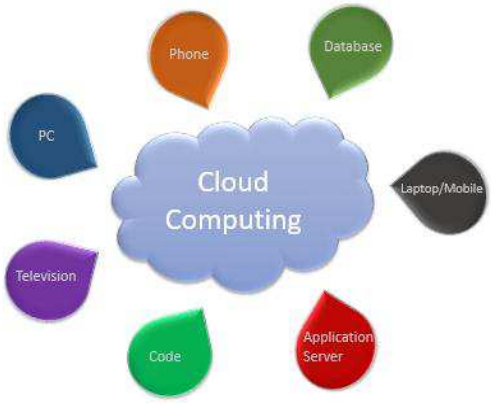


Figure 2. Cloud Computing Components

4. Solutions

Cloud Computing allows users to store data on remote servers that they do not own. These cloud services are provided by the CP (Cloud Provider) [5]. Only the CP has access to data security details, and the users cannot have any information about data integrity being lost. The system must maintain the data in a cryptographic manner so that only the users have the right to access the original data. This is done with the help of some encryption and decryption algorithms. Advanced Encryption Standard (AES) is used to ensure data integrity. It creates a digital signature that is verified by the Digital Signal Algorithm (DSA). In this way only the user has the rights to make any changes in the data and the changes are encrypted again.

Cryptography is helpful in securing data and it can provide data security in backups, network traffic, and file system. It is implemented using symmetric and asymmetric algorithms. Some crucial symmetric algorithms are DES, AES and 3DES. [6]

4.1 DES (Data Encryption Standard)

DES is a key-block cipher introduced by NIST (National Institute of Standards and Technology). [6] DES takes 64 bits of plain and 64 bits of cipher text and a 56-bit cipher key for both encryption and decryption. [8] The right-most bit is the least significant bit in each byte. It is the parity bit and can be ignored. Only seven significant bits of each byte are used and cause the cipher to be of a 56-bit. The block of bytes goes through 16 iterations in which plain text blocks are interlaced with the key. This process is same for encryption and decryption. It takes a 64-bit input and generates 64-bit output. The process of DES is shown in Figure 3 here below [7].

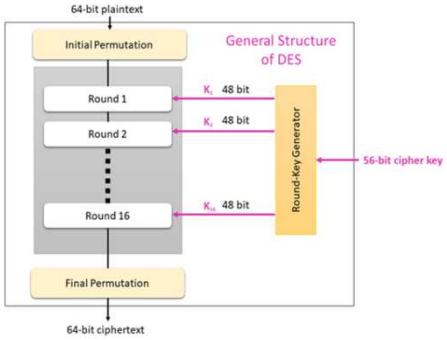


Figure 3. Data Encryption Standard

4.2 AES (Advanced Encryption Standard)

AES was initially known as Rijindael back in 2001 as shown in figure.4. AES is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption [7]. It is much faster than DES and Triple DES.

AES features are:

- 128- bit data
- Robust and faster

- 256\192\128-bit keys

Figure 4. AES Structure

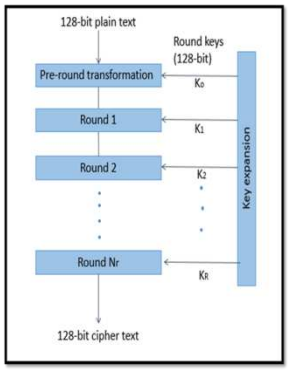
- Software can be coded in java and C language
- Comes with immense design and specification details
- More secure.

AES works (in) iteratively by shuffling and substituting bits. Computations are done on bytes rather than bits. 128-bits of plain text box are treated as 16-bytes which are arranged into 4x4 matrix. Key length determines the number of rounds
required. Implemented separately, encryption and decryption both are done in process of changing Plain text to Cipher text.

Table 1. Relationship between key size and number of rounds (R)

R	Key Size
10	128
12	192
14	256

In AES, encryption is done at each round. Four sub-processes (Sub-bytes, Shift rows, Mix Columns and Add round key) are involved in encryption process. These processes are explained and represented in Figure 5 below.
Decryption also carried out in every round. It comprises of same four 4 sub processes (Sub-bytes, Shift rows, Mix Columns and Add round key) which are same as encryption but carried out in reverse order. As shown by the Figure 6 below.



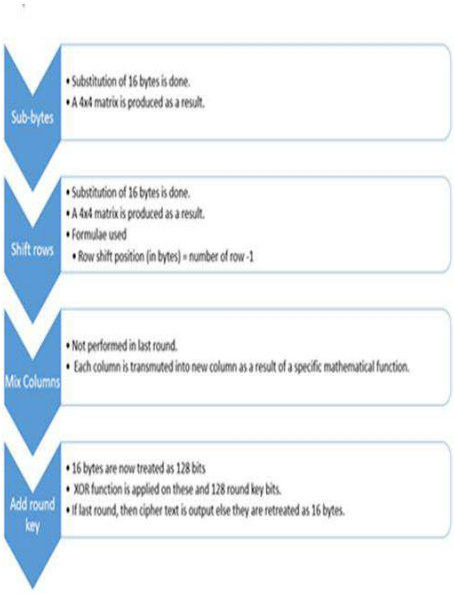


Figure 5. AES Encryption process flowchart

Figure 6. AES Decryption Process Flow

AES is the same as DES except that it uses more bits as function of increasing technology, and as the size of data is increasing, and DES does not have enough bits to encrypt the data. it was not secure to mitigate the 'Exhaustive Key Search Attack', (so) in other words AES was introduced with a greater number of bits than DES. [6] AES encrypts data with 128 bits [7].

4.3 3DES (Triple Data Encryption Standard)

3DES is exactly as the name suggests, it applies DES thrice to each data block to perform encryption without the need to make another algorithm [6]. The increase in the computational power has made the original DES algorithm subjected to attacks and hence the 56-bit cipher key size became insufficient. TDES resolves this problem by simply increasing the key size and applying TDES as shown in the Figure 7. TDES uses a "key bundle" with three 56- bit keys namely K1, K2, K3 for encryption as well as decryption.

1. Encryption Algorithm:

$$Ciphertext = E_{K3}(D_{K2}(E_{K1}(Plaintext)))$$

2. Decryption Algorithm:

$$Plaintext = D_{K1}(E_{K2}(D_{K3}(Ciphertext)))$$

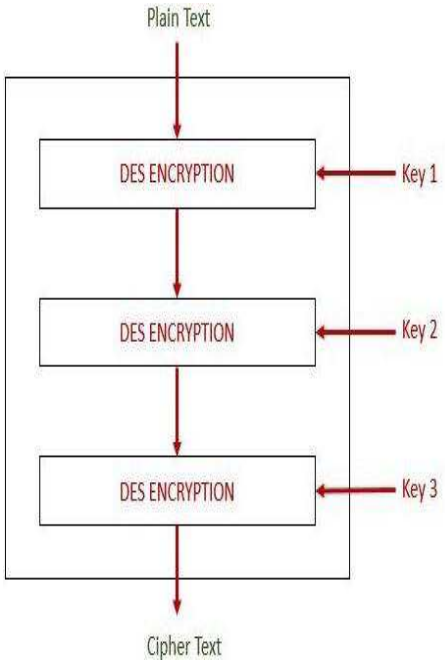


Figure 7. Triple Data Encryption Standard

5. Related Work

A company named "Ingrian Networks Inc." had introduced encryption devices that claim to provide high-level encryption of data. They used AES algorithm and performed encryption and decryption of network traffic. Keys are made to access the data. The OS is designed to only understand those commands and not perform other tasks, and they include two-factors authentication. The keys are only provided to the owner of the data. The keys are stored on a separate secured site.

6. Proposed System

File integrity is most important and this is maintained by validating it in periodic manner. Data stored on cloud is not at all compromised [9].

6.1 Overview

AES and DES algorithms are used collectively in order to design this model. Figure 6 shows how a file is encrypted at the time of its storage to cloud. Whenever a file is created then saved, the file undergoes 128-bit AES encryption. File firstly goes through Add Round key then it undergoes 10 rounds of sub bytes followed by Shift Rows then Mix Columns then Add Round key after all this a final round of Sub bytes followed by Shift Rows and Add Round Key.

Figure 8. File Encryption And Signature Creation While Providing Cloud Storage

When file has gone through all these processes, a message digest function "SH1" is given to the file and a digest is created as a result. Digest is transformed into DES signature using 1024-bit private key. Before the encryption process begins, a public key is generated using private key.

When the receiver/client opens the file for verification signature and 1024-bit signature is used. Message digest function "SHA1" is used to create digest. Signature and file are decrypted by combining together with public key created at the time of encryption whereas the digest expected is formed here. To check weather file's integrity is **a**ffected or not, the digest and digest expected are matched. In case both are the same meaning that, the file's integrity is not affected. If they do not match then the file has been modified and do not hold its integrity. This process is shown in Figure 9. Message digest "SHA1" is a cryptographic hash function, consisting of a string of digits formed from one-way hash. SHA-1 produces a

message digest of 160-bit (20-byte) [10]. A SHA-1 hash length of 40 digits.

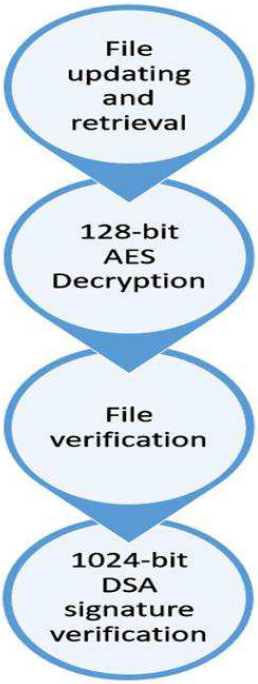


Figure 9. File AES decryption during file content retrieval and verification using DSA

6.2 Construction

As proposed earlier, initially the file is created then it is modified by inserting, deleting, or modifying the file contents. After that, the file is saved to cloud. AES algorithm is used for encrypting the file content, and 128 –bit keys are used for this (which is) based on 10 rounds of operation. Then DSA algorithm is used to generate the 1024-bit public and private key along with signature. Afterwards whenever the user will access the file, the AES algorithm is used for decryption and then the file contents will be shown to the user. This is shown in Figure 10.

7. Results

The solutions DES and AES have limitations in terms of size and security of data being encrypted. Thus, a more secure and practical solution of the issue i.e., Security in Cloud Computing has been proposed. The proposed model is the hybrid form of AES and DES, which together secures the data by strong encryption and increased size. The drawbacks of the two systems have been cancelled out when used together. The file integrity is not at all compromised in the new model. However, the previous models posed real threats to the file's content and integrity. The proposed solution comprises the assurance of data Integrity at cloud against the combined benefits of AES and DES.

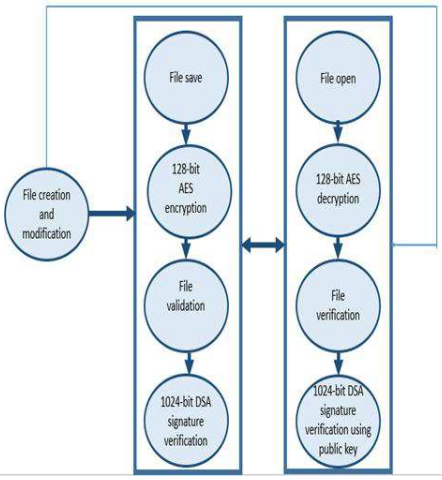


Figure 10. Proposed Model

8. Conclusion

Many schemes like Cryptography, and those used by the above-mentioned Ingrian Networks Inc. company are effective solutions to ensure data security and prevent breaching, but the reliability of the security of data, falls on the keys generated for the encrypted data. An effective solution would be to do layered encryption, similar to 3DES**,** where three blocks are encrypted. Encryption can be done on multiple layers like in transport and data link layer and the keys should be stored on a dedicated site. Another main key should be generated which allows access to that site. That key can be stored on cloud and hidden using image steganography, by adding multiple dimensions and layers to data encryption, the data can be considerably secured. This research provides an overview of security concerns at cloud, the commonly used security schemes and by comprehending the deficiencies of any single we provided a hybrid approach against the data integrity assurance a cloud.

References

J. K. Randeep Kaur M.Tech Scholar, "Cloud Computing Security Issues and its Solution: A Review," in 2015 2nd International Conference on Computing

for Sustainable Global Development (INDIACom), Patiala, India, 2015.

M. I. Napoleon C. Paxton, "Cloud Security: A Review of Current Issues and Proposed Solutions," in 2016 IEEE 2nd International Conference on Collaboration and Internet Computing, 2016.

P. S. a. A. Agarwal, "Cloud Computing Data Storage Security framework relating to Data Integrity, Privacy and Trust," in 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015), Dehradun, India, 2015.

A. H. A. S. K. K. Navdeep Singh, "Unfolding Various Security Brawls and Concerns of Cloud Computing," in International Conference on Innovative Applications of Computational Intelligence on Power, Energy and Controls with their Impact on Humanity(CIPECH14) 28 & 29 November2014, Jalandhar, INDIA, 2014.

G. B. Prasanth SP, "AES and DES Using Secure and Dynamic Data Storage in Cloud," IJCSMC, vol. III, no. 1, p. 401 – 407, 2014.

M. S. S. D. Miss. Shakeeba S. Khan, "Security in Cloud Computing Using Cryptographic Algorithms," International Journal of Computer Science and Mobile Computing, vol. III, no. 9, pp. 517-525, 2014.

D. G. J. Shaffy Bansal, "Analyzing Working of DES and AES Algorithms in Cloud Security," International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), vol. IV, no. 3, pp. 1-9, 2017.

S. Gurpreet Singh, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," International Journal of Computer Applications, vol. 67, p. 0975 – 8887, 2013.

Prasanth SP et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, January-2014, pg. 401-407

Symposium on Colossal Data Analysis and Networking (CDAN), 2016.