International Journal of Research in Engineering, Science and Management
Volume-2, Issue-9, September-2019
www.ijresm.com | ISSN (Online): 2581-5792

A Study on Cloud Computing Security

A. A. Jaiswal[1], Payal Bhanarkar[2], Surbhi Vyapari[3], Kanchan Kapgate[4], Priya Dhage[5]
[1]*Professor & HoD, Department of Computer Technology, K.D.K. College of Engineering, Nagpur, India*
[2,3,4,5]*Student, Department of Computer Technology, K.D.K. College of Engineering, Nagpur, India*

***Abstract*: Now where cloud computing is more popular in storing data online and offline. Whereas cloud computing is mostly used in industry, colleges and many more for storing data on cloud. The proposed model is liable to meet the required security needs of data centre of cloud. Encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms. The hybrid approach when deployed in cloud environment makes the remote server more secure and thus, helps the cloud providers to fetch more trust of their users. For data security and privacy protection issues, the fundamental challenge of separation of sensitive data and access control is fulfilled. Cryptography technique translates original data into unreadable form. Cryptography technique is divided into symmetric key cryptography and public key cryptography. This technique uses keys for translate data into unreadable form. So only authorized person can access data from cloud server. Cipher text data is visible for all people.**

***Keywords*: cloud computing, hybrid cryptography, security-privacy.**

1. Introduction

Cloud computing is combination of many preexisting technologies that have matured at different rates and in different context. Now a day cloud computing is more popular in storing data online and offline also where it is mostly use in industry, military, college and many more. For storing data on cloud. Many issues are face while storing data, the solution for these issues we are using storage security any cloud computing. Many organizations are moving into cloud because it allows user to store the data on cloud and can access at any time at anywhere. The goal of cloud computing is to allowed user to take benefit from all this technology.

2. Problem statement

The security issues in cloud computing includes:

- Data security
- Identity and access control

Among these main security issues in the cloud, data security and integrity are believed to be the most difficult problem which could limit the use of cloud computing. In fact, access control and key management are all issues involved in data security. Data security in the cloud refers to data confidentiality, integrity, availability and traceability (CIAT), and these requirements pose major problems for cloud computing. Confidentiality: Data confidentiality requires that information be available or disclosed only to authorized individuals, entities or IT processes. Integrity: Data integrity ensures that the data is maintained in its original state and has not been intentionally or accidentally altered or deleted. Availability: Data availability ensures continuous access to data even in the occurrence of a natural or man-made disaster or events such as fires or power outages. Traceability: Data traceability means that the data and communications are genuine in a transaction and that both parties involved are who they claim to be. Authentication: Authentication is a method by which a system verifies and validates the identity of a user of the system who wishes to access it.

3. Literature survey

In [1] It described the security issue that facing in storing the data on cloud therefore using hybrid cryptography technique it easy to maintain and secure the data in computing.

In [2], this paper is providing security using following technique i.e. public cloud, private cloud, hybrid cryptography for archiving the file security.

In [3] the Authors presented Cryptography and steganography techniques are more popular now a day's for data security. Use of a single algorithm is not effective for high level security to data in cloud computing. In this proposed system AES, blowfish, RC6 algorithms are used to provide block wise security to data File is spited into eight parts. Each and every part of file is encrypted using different algorithm.

In [4], it is proposed a simple data protection model where data is encrypted using Advanced Encryption Standard (AES) before it is launched in the cloud, thus ensuring data confidentiality and security.

4. Proposed methodology

Blow Fish: Blow Fish is a symmetric block cipher which uses a Fiesta network, 16 rounds of iterative encryption and decryption functional design. The block size used is of 64- bits and key size can vary from any length to 448. Blowfish cipher uses 18 sub arrays each of 32-bit commonly known as P-boxes and four Substitution boxes each of 32-bit, each having 256 entries. The algorithm design is shown in figure. It consists of two phases: one is Key Expansion phase another is Data Encryption phase. In Key expansion phase, key is converted into several sub-keys and in Data Encryption phase, encryption occurs via 16-round networks. Each round consists of a key dependent permutation and a key and data-dependent

substitution.

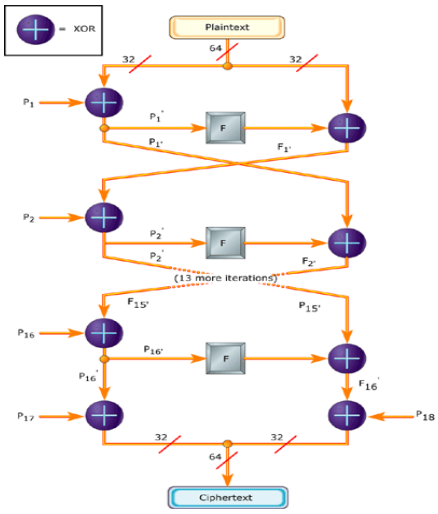

Fig. 1. Blowfish Algorithm

Encryption phase: At the encryption end, on the specification of user, the file being encrypted will be sliced into n slices. Each of the file slices is encrypted using Blowfish key provided by the user for each slice. The key will be encrypted using SRNN public key after encryption; we have encrypted files slices and the corresponding encrypted keys. The encryption phase is illustrated in the Fig. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text, encrypted data is referred to as cipher text the files are sliced at encryption phase and merged at decryption phase.

Decryption Phase: Decryption is a method which converts cipher text into plain text. That a user easy to access data.

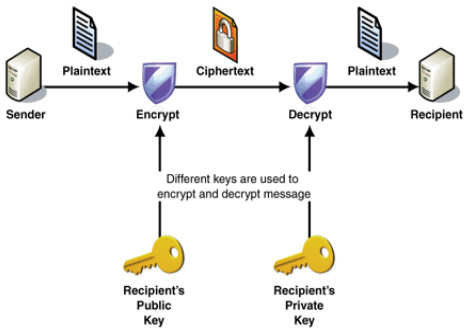

Fig. 2. Encryption and Decryption

5. Security issues in cloud

Cloud computing comes with numerous possibilities and challenges simultaneously. Security is considered to be a critical barrier for cloud computing in its path to success. The security challenges for cloud computing approach are somewhat dynamic and vast. In terms of customers personal or business data security, the strategic policies of the cloud providers are of highest significance. Security issues in cloud:

- Lack of trust
- Multi-tenancy
- Loss of Control

At highly sensitive data, if we use cloud high degree of security is required for our data. For hosted clouds, third party is responsible for storing and securing data. But is third parties trust worthy? Handing over sensitive data to other party is a serious concern. Data loss is also possible in cloud. A malicious hacker might delete a Target's data out of spite or data can be lost because of a careless cloud service provider. Trusting a third party requires taking the risk of assuming that the trusted third party will act as it is expected (which may not be true all the time). The scalable nature of cloud has posed another threat. Cloud service providers share infrastructure, platforms, and applications to provide services. There is no strong isolation. Two companies might be using same piece of hardware without knowledge. Another question comes who is responsible for security of data? Is it only cloud service provider's duty or stake holders, business entities are also responsible for maintaining safeguards. Legal decisions will ultimately determine who owns the responsibility for securing information shared within clouds [2].

6. Conclusion

As indicated by benefit conveyance models and organization models of cloud, information security and protection assurance are the essential issues that should be tackled. Information Security and protection issues exist in all levels in SPI benefit conveyance models. The previously mentioned demonstrate is productive in information as an administration, which can be stretched out in other administration models of cloud. Likewise, it is tried in cloud condition like Open Nebula, in future this can be conveyed in other cloud situations and the best among of all can be picked.

References

[1] A. Venkatesh, Marrynal S. Eastaff, "A Study of data storage security issue in cloud computing," International Journal Research in computer science, engineering and information technology, 2018.
[2] Tripathi Jyoti, and Gayatri Pandi, "Achieving Cloud Security Using Hybrid Cryptography Algorithm," IJARIIE, 2017.
[3] P. V. Maitri and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 1635-1638.
[4] Abha Sachdev, and Mohit Bhansali "Enhancing Cloud Computing Security using AES Algorithm," International Journal of Computer Applications, vol. 67, no. 9, April 2013.
[5] Md Sajid Khan, Chandra Shekhar Yadav, and Mayank Deep Khare" Implementing Cryptographic Method for Ensuring Data Security in Cloud Computing Based on Hybrid Cloud," IJSRST, 2018.
[6] Rishav Chatterjee, Sharmistha Roy, "Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud," IJESC, 2017.