Data Security in Cloud Computing Using Cryptography Algorithms

Vishal Agrahari

Department of Computer Science and Engineering
Galgotias University, Greater Noida
Uttarpradesh, India-201310

***Abstract*: Today cloud computing is one of the fastest growing technology that provides services to the customers over internet. Cloud is the collection of data centers and servers that are located at separate places. The main purpose for using the cloud is that the customer can save and retrieve data in the cloud from anywhere anytime. And the main advantage is that cloud services are cost efficient. This technology is totally different from traditional computing technology. But still there is concerns regarding the safety of the cloud environment. There are many advantages of cloud computing yet the process of adapting the technology is very slow because of the customer concern related to the data security. That's why a strong and protected user authentication is required for cloud computing that avoids unauthorized user access in the cloud. This paper is focused on the various cryptography algorithms that are mainly used to secure the data transferred between the user in cloud computing.**

***Keywords*: cloud computing, data security, cryptography algorithms, unauthorized user access**.

I. INTRODUCTION

Cloud computing is the way of providing cloud resources over the internet. It is the fastest growing technology that offers various services such as resource, infrastructure, platform etc. It gives permission to the organizations and individual users to utilize the resources that are managed and maintained by the service providers. Cloud computing allows the users to use the applications over the internet without installing in their own systems. There are many advantages of cloud computing but one of the major concerns is data security. [10] Organizations and individual users are always in worry about data security. Many users avoid cloud services because of the data security. They seem that their data is more secure in their own infrastructure and in place of expanding their business they stuck in maintaining the infrastructures.

This research paper focuses on data security in cloud using cryptography and the algorithms that are mainly used for securing data. One can use these algorithms to secure data in cloud.

II. ADVANTAGES OF CLOUD COMPUTING

There are many advantages of cloud computing, some major advantages are provided below.

1. *Cost Saving:*

Cost has been the main factor for starting a new IT company. Cost saving is the biggest benefit of cloud computing. Cloud service charge is paid depending on the usage of resources and services. Users have to pay as much as they use. Users can easily change their demand for resources and services depending on the work load of their organization.

2. *Scalability and Flexibility:*

Cloud computing provides facility to the organizations, companies and individual users to scale up or scale down their resources according to their need. If in a peak season they are doing well or want to expand their business then they can scale up their resources and services. In the same way they can scale down their resources and services in the weak season.

3. *Backup and Recovery [9]:*

In the cloud data is kept at data centers located at different places. Since all the data is stored in the cloud, data can be recovered very easily without losing data. And in case of any disaster cloud has multiple techniques to recover the data. Cloud providers can recover the data easily and faster than any individually set up organization avoiding their geographical locations.

4. Reliability:

Cloud computing service is better than self IT infrastructure and it is reliable and more consistent in comparison of own IT infrastructure because they have well managed platform. Many service provider offers 24x7x365 service level agreement and 99.9% availability. Cloud service providers use quick failover mechanism. In case if a server fails or stop working than hosted application and services are quickly transmitted to any other available servers.

5. *Manageability:*

Cloud computing provides advanced and simplified IT management and maintenance capabilities through central administration of resources. It is the responsibility of service provider to maintain and update all your resources, user does not require to concern about maintenance of resources and services. They have to use user interface based on web for accessing applications, software and other resources and services without the need for installation.

6. *Mobility:*

Cloud services are provided over the internet. Users or employee of a company can access all the services and resources from anywhere and anytime in the world. All the services can be used with many different devices like mobiles, laptops, pc, tablets etc. from different platforms. This facility has increased the work from home culture.

III. CHALLENGES IN CLOUD COMPUTING

Cloud computing has many advantages as mentioned above in the same way it has many challenges also. Users have to aware

about the advantages and disadvantages while moving towards cloud computing. While analyzing these challenges, one main and common challenge is data security. According to the survey by Gartner [8] , approximate 70% of Chief Technical Officers don't want to move or use cloud computing services because of the data security. Some of the major security challenges are as follows.

1. *Confidentiality of data:*

Confidentiality is related to the data privacy. It refers to protecting data from being accessed by unauthorized person. Confidentiality ensures that data is visible to only authorized person. It is very hard to maintain data confidentiality when many users are using the resources and services simultaneously in a distributed network. And it is the responsibility of service provider to maintain confidentiality. The solution for maintaining data confidentiality is encryption there are many algorithms which are used for this.

2. *Data Integrity [3]:*

Data integrity refers to the preserving the data from any loss or modification by an unauthorized person. It can be defined as the data should be as original at the time of retrieval as it was at the time of storing or sending. Many users working on the same project may transfer data that can be modified by an unauthorized user sharing the application or platform in the cloud. This can be reason for data integrity failure.

3. *Data Remanence:*

Data remanence [7] is the residual of digital data that remains even after removing or erasing the data. Data must not only be protected against unauthorized user but also it should be securely deleted at the end of its life-cycle. If data is left on disks then it can be recovered by malicious users. There are many techniques that avoid data remanence. These techniques are divided as cleaning, destruction or purging.

4. *Data Transmissions:*

Most of the time data is transferred between user and cloud. During the transmission encryption is imposed aver the data. But most of the time data takes a lot of time in encryption or decryption and data is transferred without encryption. At this time intruders can hack the data, interrupt the data transfer or miss use the data.

5. *Malicious Insiders:*

Malicious Insiders are the authorized employee appointed by the cloud service providers for managing and maintaining the cloud. Sometimes these authorized users access the sensitive data and steal or corrupt the data. Sometime they forward these sensitive data to other organizations or users who are sharing the same cloud.

IV. CYBER-ATTACK ON CLOUD

There are many confidential data or sensitive information in the cloud, in order to access these information or services many attack happen by the hackers. Some cyber-attacks [6] are below.

1. *Denial of service attack (Dos):*

Denial of service attack overloads the server by sending a large number of requests to the targeted server. This attack shuts down a machine or network by making it unavailable to its intended users. The Dos attack deprives authorized users of the service or resource they expected. This attack can be reduced by using firewall based approach, filter based approach, and signature based approach.

2. *Authentication attack:*

This attack generally happens when an unauthorized user gets user id and password of an authorized user. Thus they can access confidential data and miss use it. It can be ignored by using advanced authentication technique such as one time password.

3. *Man-in-middle attack:*

This attack takes place when an intruder inserts him/ herself into a conversation between two users and gain access to information that the users are trying to send to each other. This attack allows a malicious user to intercept, send and receive data to the actual user without their knowledge. To avoid this attack there are various encryption and decryption algorithms that can be used to protect data.

4. *Malware Injection attack:*

Malware injection attack injects the malicious software or code which creates a door for the hacker in the cloud environment. The purpose for injecting malware is to control user data or resources in the cloud. To protect from malware injection cloud service provider needs to install hypervisor.

V. CRYPTOGRAPHY

Cryptography is the process of converting the data such as text, audio, video and other media into non readable, not understandable format during transmission and storage of data, this is also known as encryption. And the reverse process of accessing the real data is known as decryption. Some common terms of cryptosystem are follows:

- Plaintext: It is the original form of data that is protected from unauthorized access during transmission of data.
- Cipher text: It is the encrypted form of plaintext after applying encryption algorithm.
- Encryption Algorithm: Algorithm which is used to transform plaintext into cipher text.
- Decryption Algorithm: It is the reverse form of encryption algorithm which is used to transform cipher text into plaintext.
- Encryption Key: It is the key used by sender with encryption algorithm to transform plaintext into cipher text.
- Decryption Key: It is the key used by receiver with decryption algorithm to transform cipher text into plaintext.
- Sender and Receiver: These are the nodes that are communicating or sharing the information.

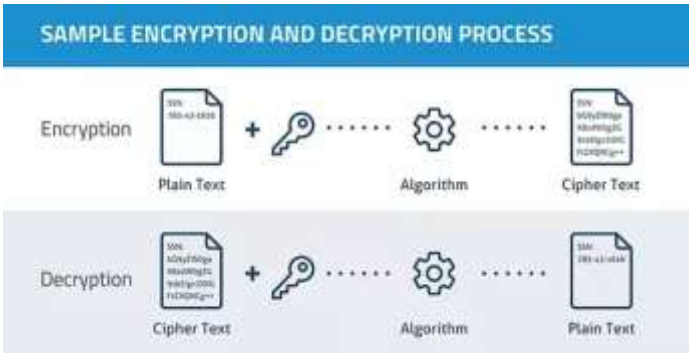

Figure 1: Encryption and Decryption process

Based on key, cryptography has been broadly divided into two parts:

1. *Symmetric key cryptography:*

This is also called private/single key cryptography. Single key is used at both the side (sender or recipient), the key which is used for encryption at sender side, is also used at receiver side to decrypt the data. Before transmission of data both the parties must agree with the private key. There are many symmetric key algorithms. Most useful algorithms are discussed below.

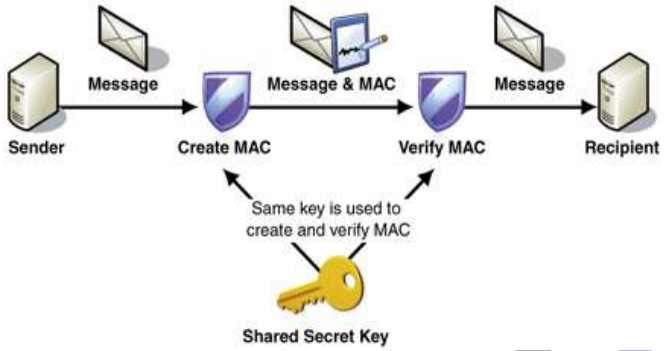

Figure 2: Symmetric key schema

a) Data encryption standard (DES):

DES is one of the famous [12] secret key cryptography designed by IBM and adopted by NIST in 1977. It is basically based on feistel cipher. It is a symmetric key-block cipher where same key is used for encryption and decryption. DES is a block cipher that transforms blocks of bits into non readable form. It uses a key of 56 bits length to transform plaintext of 64 bits length into cipher text. There is a round key generator which generates keys of 48 bits length from initial key of length 56 bits. Initially the whole text is converted into blocks of 64 bits length. At the time of encryption DES [13] takes a 64 bit plaintext to generate a 64 bits cipher text and at the time of decryption the process reverse. There are two permutations and 16 feistel rounds are used in encryption process. In every round a different round key of 48 bit length is used which is created from the initial cipher key.

b) Advanced Encryption Standard (AES):

It is also a symmetric key block cipher that uses the same key for encryption and decryption process. It is the advanced version of DES which is stronger and faster than DES. In DES key length is 56 bits which is less for current computational power and processing purpose while in AES the minimum length of key is 128 bits which is used over 128 bits of plaintext to transform into 128 bits of cipher text. The key used in this algorithm depends on the no of rounds. The key length for 10 rounds is 128 bits and key length for 12 rounds is 192 bits and key length for 14 rounds is 256 bits. This algorithm performs all the computations over bytes in place of bits. The plaintext of 128 bits is divided into 16 blocks of byte that are arranged in 4x4 matrix for processing. The algorithm is combination of permutation and substitution and it is iterative algorithm. In all the iteration there are some steps like sub bytes, shift rows, mix columns and add round key and after all the iteration we get cipher text.

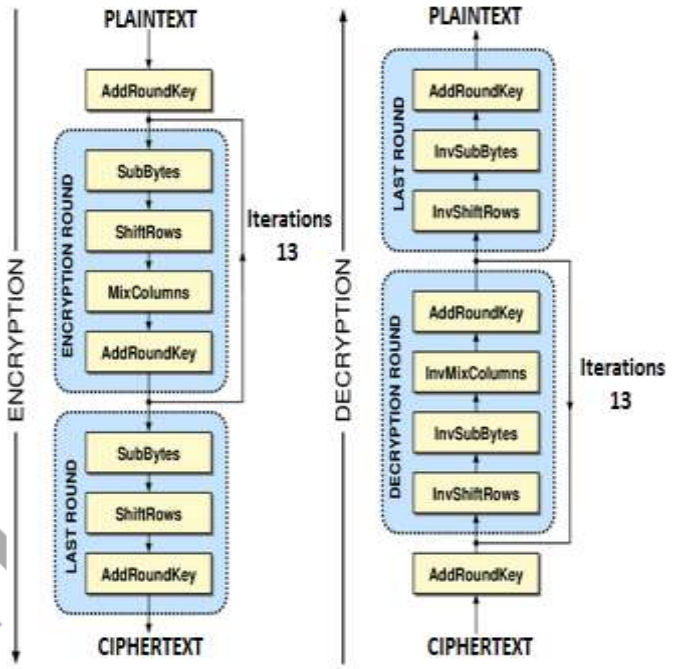

Figure 3: AES flowchart [1]

2. *Asymmetric key cryptography:*

It is also called public key cryptography where two keys are used public key and private key. Public key is used for encryption which is known to everyone and private key for decryption which is only known by the recipient. In this method there is an effective verification system such that if any alteration is done then it will cause failure. The interesting thing about this method is that only authorized person can access the data or services. There are many asymmetric algorithms like RSA, Diffie Hellman, Eliptic Curve Cryptosystem and many others but RSA and D-H are most famous algorithms.

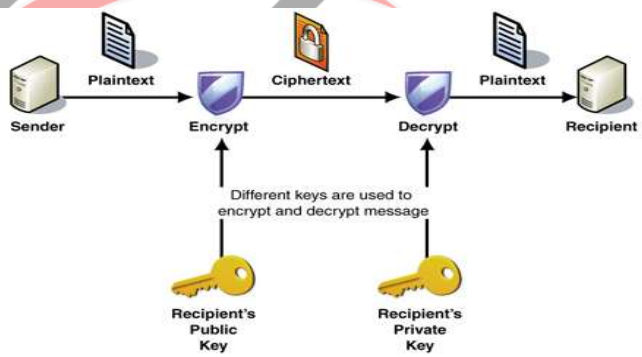

Figure 4: Asymmetric key schema

a) Rivest-Shamir-Adleman (RSA):

It is an asymmetric key cryptography algorithm which is one of the earliest developed asymmetric algorithms that is being used everywhere. This algorithm works over different length of data blocks and different length of keys. It involves a public key which is familiar to everyone and a private key only familiar by the receiver. This algorithm takes two prime numbers to generate the keys for the purpose of encryption and decryption. This algorithm works into three phases: by using two prime numbers generating keys, encryption and decryption. Today RSA algorithm is being used in multiple software, key exchange, digital signature etc. But this is mainly used for authentication purpose.

Procedure of RSA algorithm

- Select two large prime numbers P and Q such that P is not equal to Q.
- Compute N which is product of P and Q.
- Choose E (public key) such that E is not a factor of (P-1) and (Q-1).
- Choose D (private key) such that it follows: (D*E) mod (P-1) (Q-1) =1.
- Compute the cipher text C.T. = $(P.T.)^{E}$ mod N.
- Compute the plaintext P.T. = $(CT)^{D}$ mod N.

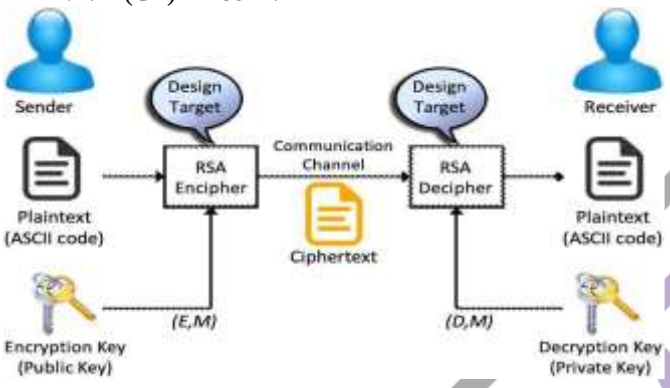

Figure 5: RSA architecture [2]

b) Diffie Hellman Key Exchange [11] :

It is also one of the earliest introduced asymmetric key cryptography algorithm. It is known for key exchange. This algorithm generates a secret key which is shared through a safe communication channel and with the help of this secret key cryptographic keys are exchanged. This algorithm helps both the end to jointly develop a secret key. This algorithm works like a puzzle where A generates a huge amount of encrypted keys and sends them to B. B selects a random key and now lets A know which he has choose. If an attacker is able to observe all the keys still he can't able to know which key B has choose because he has encrypted the response with the selected key. This algorithm is unable to work on exchanging a huge amount of data.

VI. CONCLUSION

Cloud computing provides various services over the network and many organizations and companies are moving towards cloud it means they are adapting the storage service provided by the cloud service providers. As people are storing their personal and sensitive data in the cloud, it is very important to provide security or protect it from unauthorized users or hackers. Data security becomes the major issue. To ensure data security over the cloud we have used cryptographic terms. There are many security algorithms to protect the data. In this paper we have discussed about important algorithms like AES, RSA, and D-H etc. that can be used to overcome the security issues. These are the algorithms that can prevent any kind of attacks and these algorithms can be used with all the internet protocols that follow IPv4 and IPv6.

VII. FUTURE SCOPE

There is a huge scope of enhancement in this area of data security in cloud computing. Cryptography can be used in many places in order to secure data, information, services and resources. Cryptography can help for managing cloud like who can access data, who can control data, data transformation, data transmission, data authorization, data authentication and secure data storage. There is a lot of research [4] required in this field of data security.

REFERENCES

[1] Vishwanath, R. Peruri, and J. He, Security in fog computing through encryption. DigitalCommons@ Kennesaw State University, 2016.
[2] H. Bodur and R. Kara, "Secure SMS Encryption using RSA Encryption Algorithm on Android Message Application," ISITES2015, pp. 1-10, 2015.
[3] Vijay Kumar, "Brief Review on Cloud Computing", International Journal of Computer Science and Mobile Computing, vol. 5, September 2016,
[4] M. Vijayapriya," security algorithm in cloud computing: overview", International Journal of Computer Science & Engineering Technology (IJCSET), Vol.4, ISSN: 2229-3345.
[5] Bokefode Jayant.D, Ubale Swapnaja A, Pingale Subhash V., Karane Kailash J. , Apate Sulabha S. ,"Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role bases Access Control Model", International Journal of Computer Applications, Volume 118-No.12, May2015
[6] Subramaniam.T.K, Deepa.B. January (2016) "Security Attack Issues And Mitigation Techniques In Cloud Computing Environments". International Journal of UbiComp (IJU), Vol.7, No.1.
[7] Data Remanence, https://en.wikipedia.org/wiki/Data_remanence.
[8] Gartener: Seven cloud-computing security risks. InfoWorld.2008-07-02. http://www.infoworld.com/d/security-central/gartener-seven-cloud computing-security-risks-853.
[9] Anca apostu, Florina puican, Geanina ularu, George suciu, Gyorgy todoran, "Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud", Recent Advances in Applied Computer Science and Digital Services
[10] Satyakam Rahul, Sharda, "Cloud Computing: Advantages and Security Challenges" International Journal of Information and Computation Technology, vol. 03, 2013
[11] https://crypto.stackexchange.com/tags/diffie-hellman/info
[12] Sumitra, "Comparative Analysis of AES and DES security Algorithms", International Journal of Scientific and Research Publications, Volume 3, Issue 1, January 2013, ISSN 2250- 3153
[13] Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications (0975–8887) Volume 67–No.19, April 2013