A SURVEY ON THE DIFFERENT CRYPTOGRAPHIC TECHNIQUES USED FOR DATA ACCESS CONTROL IN CLOUD COMPUTING

S.Rajeswari[1], Rabubieyya Aiiysha Zahra[2], Dr. R.Kalaiselvi[3]
[1]Assistant Professor, [2]UG Student, [3]Associate Professor,
Information Science & Engg. Dept., Information Science & Engg. Dept.,
Computer Science & Engg. Dept.,
New Horizon College of Engg., New Horizon College of Engg., Noorul Islam University,
Bangalore. Bangalore. Kumarakoil, Thuckalay.

Abstract

Owing to the need for storage, of the rapidly increasing information that is generated each day, storage mechanisms have migrated from the traditional storage techniques to cloud storage. Cloud storage is a service model whose function is to maintain, manage and back up the data and make it available to all the users over a network. However, this growing new technology also poses various challenges such as data ownership, data security and trans-code data storage. Thus, this paper discusses the various cryptographic encryption algorithms that aim at solving these security challenges.

Keywords: Cryptography, public key, private key, Brute force, ciphertext, cipher.

I.INTRODUCTION

Cloud computing refers to the process of storing, managing, maintaining and processing data over a network of remote servers which are hosted over the internet. Instead of storing information on the traditional storage devices such as hard drives for your needs, today we use various services that are provided and available on the internet. Considering an example from our daily lives, today photographs and other documents can be stored online, by backing it up into a cloud server. The most common example of a publicly available free cloud server is, Google Cloud Platform. Using such services is called as employing "Cloud Computing" service. Using this, owners can easily access, store and manipulate their data on the cloud.

This growing technology also poses various security challenges and issues. In cloud computing, security refers to the protection of sensitive and critical information from harmful forces and the unwanted actions of unauthorized users. The main focus behind security is to ensure privacy while protecting personal data [5]. Thus, one of the main drawback of cloud computing is security. The numbers of users that are using the cloud computing services are increasing each day, owing to the need for storage of rapidly increasing data. Thus, because of this, the number of attackers and malicious users are also increasing. These attackers misuse the sensitive information for unethical and destructive purposes.

Some of the attacks include- Denial of Service (DoS) attack, Side Channel Attack, Cloud Malware Injection Attack, Brute Force, Man-In-The-Middle Cryptographic Attack, etc. Therefore to overcome these type of security challenges various cryptographic algorithms have been proposed.

II.SECURITY ALGORITHMS

The main purpose of these security algorithms is to use cryptography to secure any data or information that is being transmitted over the network. Cloud data security moreover classified into three different categories as,

Privacy Preservation that defines that Privacy of personal and important information in cloud is crucial as the cloud servers are not trusted. Confidentiality and authorization are main requirements of privacy preservation in cloud, Storage Security that defines that Cloud storage Security is the task of providing integrity to the shared data stored at dishonest cloud servers and the Data Security that defines that the data or information security is the process of protecting the data from unauthorized users, preventing alterations and restricting the access of sensitive information [5]. The term cryptography refers to the process of converting plain text into cyphertext where plain text is the ordinary language which is easily readable by humans and cyphertext is the information which has been encrypted and is not readable by human or even a computer, unless it is decrypted using a correct cypher. Cryptography can be used for user authentication and also protecting the data from unauthorized access and alteration.

These cloud storage security algorithms can be broadly classified into- symmetric and asymmetric algorithms as shown in the Fig.1 below.

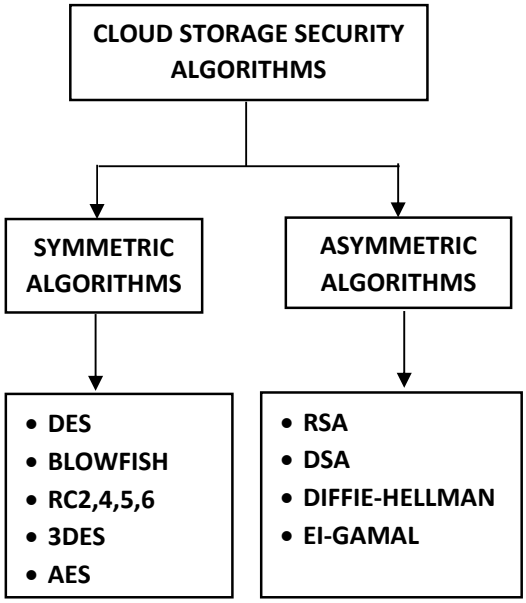

Fig1. Classification of Cloud Storage Security Algorithms

III.SYMMETRIC ALGORITHMS

Symmetric algorithms are also known as Secret key encryption or symmetric key encryption [2]. In this, the encryption and decryption of information is performed using the same key and it is hence kept as a secret. The computing power required by these algorithms is comparatively lesser. Symmetric algorithms can further be sub divided into Block cipher and Stream cipher [1]. In Block cipher, blocks of text is encrypted and in Stream cipher, one bit is encrypted at a time.

A. DES

DES stands for Data Encryption Standard. It is a block cipher which was first developed in the year 1997 and was the preliminary encryption standard that was recommended by NIST- National Institute of Standards and Technology. The key size and block size of the DES algorithm is 64 bits, hence it is a symmetric algorithm. When 64 bits of plain text is fed to the DES, it gives 64 bits of cipher text as the output. The algorithm and key that are used for encryption and decryption are almost the same with a few differences. Multiple Diffusion (Substitution) and Confusion (Permutation) rounds are used to increase the level of difficulty of performing a cryptanalysis on the cipher text. The entire process consists of three different phases. The first phase is the Initial permutation. In the second phase, 16 Feistel rounds are performed and the last phase consists of final computations.

B. Blowfish

This algorithm is used most commonly and which was developed by Bruce Schneier in the year 1993. Blowfish use a key of variable length of 32-448 bits to encrypt data clocks of 64 bits [3]. No attack has yetbeen successful against this algorithm. The supremacy of blowfish algorithm over other algorithms has been proved through many experiments and researches. This algorithm has better throughput and power consumption as compared to the others. The block size for Blowfish is 64 bits. Blowfish is not suitable for applications where the key changes often, like packet switching. It is suitable where the key does not change frequently, like Communications link encryption.

C. RC2,4,5,6

This is a block encryption algorithm with variable block and key sizes and developed by Ronald Rivest (RSA Labs). The attackers

without knowing the original size of the plain text find difficult to decrypt captured data. These algorithms, commonly uses SSL protocol to encrypt the web sites.

D. 3DES

Triple DES is a block encryption algorithm that simply spans the key size of DES. By applying the encryption algorithm three times recursively with three different keys. The combined key size is thus 168 bits (3 times 56).

E. AES

AES stands for Advanced Encryption Standard. It is the new standard for encryption which waspropose by NIST to be used instead of DES. The only attack that can break through this encryption is the Brute force attack. In this attack, the hackers try to unlock the encryption by testing all combinations of characters. Like the DES, the AES is also a block cipher. The key length varies from 128,192 or 256 bits. Data blocks of 128 bits are encrypted in 10, 12 and 14 rounds based in the size of the key. The advantage of this algorithm is that it is fast, flexible and can be applied on numerous platforms, even on small devices.

IV.ASYMMETRIC ALGORITHMS

Asymmetric algorithms are also called as public key cryptography [2]. In this technique of encryption, two distinct keys are used- the public key and the private key. While the public is used for encryption of data and is known to everyone the private key is used for decryption and is known only to the owner. The main advantage of public key cryptography is that it does not face the key distribution problem [1]. But the drawback of this is, that they is comparatively slower than the symmetric algorithms because of the large amount of power required for their process.

A. RSA

The RSA algorithm was developed by Ron Rivest, Adi Shamir, and Leonard Adleman in the year 1977. In this algorithm, the public key is shared to everyone who can use this to encrypt the message to be sent and private key is kept as a secret by the owner and not shared with anyone [1]. In this algorithm, plaintext and cipher text are integers between zero and n-1 for some n. The plaintext is encrypted in blocks by using the following formula: $C = M^e \bmod n$ where C is the cipher text and M the plaintext. Similarly, the plaintext is obtained by applying the formula: $M = Cd \bmod n$, where d is the private key.

B. DSA

The Digital Signature Algorithm (DSA) was recommended by the NIST to be used in their Digital Signature Standard(DSS) in the year 1991 and was also adopted as FIPS 186(Federal Information Processing Standard) in 1993. The final revised edition was released in 2013 as FIPS 186-4. In this, there are two phases for key generation. The first phase is the selection of parameters which can be shared among different system users. The second and final phase is the private and public key computation. The entropy, secrecy, and uniqueness of the random signature value k is crucial. It is so crucial that violating any one of these three requirements can disclose the entire private key to an assaulter.

C. Diffie-Hellman Key Exchange (D-H)

This algorithm was invented by Whitfield Diffie and Martin Hellman. This technique is used in a public network for exchanging cryptographic keys securely. In this, two users use a trusted network to exchange a single secret key. It requires two large numbers, one prime (P) and other is (G), a primitive root of P.

D. El-Gamal

ElGamal Encryption is an asymmetric key encryption algorithm that relies on the Diffie-Hellman key algorithm. It was presented in the year 1985 by Taher Elgamal. ElGamal encryption has three components: the key generator, the encryption algorithm, and the decryption algorithm. This algorithm gives an extra layer of security by asymmetrically encrypting keys which were formally used for symmetric text encryption.

V. COMPARISION OF CLOUD STORAGE SECURITY ALGORITHMS

The Table 1 (a) shown below gives the comparison of various cloud storage security algorithms based on the functional and non functional requirements of the cloud data [4].

Whereas the Table 1 (b) shown below gives the merits and demerits of the various cloud storage security algorithms based on their usage.

Table 1 (a): The comparison of various cloud storage security algorithms

CHARACTERISTICS	AES	RSA	BLOWFISH	DES
Key Size(in bits)	128,19 2,256	1024	32-448	64
Key Used	Encryption and Decryption key used is same.	Encryption done is public key and decryption done using private key.	Encryption and Decryption key used is same.	Encryption and Decryption key used is same.
Scalability	Can be scalable.	Cannot be scalable.	Can be scalable.	Can be scalable.
Initial Vector Size(in bits)	128	1024	64	64
Security	Security applied for both provider and user.	Security applied for only the user.	Security applied for both provider and user.	Security applied for both provider and user.
Data Encryption Capacity	Large amount of data can be encrypted.	Small amount of data encrypted.	Less than AES.	Less than AES.
Authentication	Authenticity provided is the best.	Authenticity provided is robust.	At par with AES.	Less authentic than AES.
Memory Usage	RAM needed is low.	Algorithm uses highest memory.	Memory required for execution is less than 5KB.	More than AES.
Execution Time	Fastest.	Requires most amount of execution time.	Less time for execution.	At par with AES

Table 1 (b): The Merits and Demerits of the Various Cloud Storage Security Algorithms

TECHNIQUE	MERITS	DEMERITS
DES	Same algorithm is used for encoding and decoding, which is very easy for hardware as well as software requirements. Completeness: A single bit of ciphertext is dependent on multiple bits of plaintext.	Different inputs on permutation may sometimes result in the same output from S-Box. DES does not clear the linear crypt-analysis, because this attack was invented after DES was invented.
Blowfish	Blowfish is an incredibly quick	The key must be transferred to the user

	encryption tool. It has a comparatively simple structure and is very effective.	out of band, specifically not through the unsecured transmission channel. Key management becomes complex as the number of users increase, thus leading to increase in the number of unique key pairs for each user.
AES	The key used for encryption is of variable length ranging from 128,192 and 256 bits hence making it more immune against any attacks. It is a very safe protocol, since 2^{128} attempts are required to break into this algorithm (128 bits).	Every block is encoded in the same way. In the counter mode, the AES algorithm software implementation is very complicated considering both performance and security.
RSA	RSA is public-key cryptography it provides increased security Since they is no need to transmit private keys to anyone, there is no danger. RSA algorithms produce digital signatures that cannot be rejected.	One of the major disadvantages of RSA is speed. This algorithm is much slower than all the secret-key encryptions. Public-key encryptions like RSA are very prone to impersonations.

VI. CONCLUSION

Cloud computing is a very useful service for everyone, both people and organizations. Cloud computing has proven to be very successful because it provides services to store large amounts of data virtually, without occupying any local space. And this data can be accessed anytime, as and when needed by the owner. Since people are using these services to store their personal and crucial data, security of this data is one of the main challenges. Many different algorithms are available to overcome these security challenges. Some of these algorithms include symmetric algorithms like RSA, Diffie-Hellman and DSA and asymmetric algorithms like DES, AES and Blowfish.

VII. FUTURE SCOPE

The main advantageof cloud computing is that it provides virtual storage to the user. But this also leads to many security issues. The security of the stored data is of utmost importance. Even with the development of numerous security algorithms, attackers still find a way to break into these algorithms and result in unauthorized access and the manipulation of stored private and personal data. So it is important and necessary to continue to increase the security that is provided by the cloud computing services.

REFERENCES

[1] Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms," *International Journal of Engineering Research and Applications (IJERA)*, ISSN: 2248-9622, Vol. 3, Issue 4, Jul-Aug 2013.

[2] Eng. Hashem H. Ramadan, Moussa Adamou Djamilou, " Using Cryptography Algorithms to Secure Cloud Computing Data and Services," *American Journal of Engineering Research (AJER)*, Vol. 6, Issue 10, 2017.

[3] T.Ramaporkalai, "Security Algorithms in Cloud Computing," *International Journal of Computer Science Trends and Technology (IJCST)*, Vol. 5, Issue 2, Mar – Apr 2017

[4] NasarulIslam.K.V, Mohamed Riyas.K.V, "Analysis of Various Encryption Algorithms in Cloud Computing," *International Journal of Computer Science and Mobile Computing*, Vol.6 Issue.7, July- 2017.

[5] S. Rajeswari, R. Kalaiselvi, "Survey of Data and Storage Security in Cloud Computing," *In Proceedings of the IEEE International Conference on Circuits and Systems (ICCS)*, pp. 76-81, 2017.