Security on Cloud using Hybrid Encryption Algorithm

Salini Dev P V [1], Ann Preetha Jose [2], Jesline Joseph [3]

[1] *Assistant Professor, Department of Information Technology,Viswajyothi College Of Engg. & Technology, Kerala, India*

[2] *Assistant Professor, Department of Information Technology,Viswajyothi College Of Engg. & Technology, Kerala, India*

[3] *Assistant Professor, Department of Information Technology,Viswajyothi College Of Engg. & Technology, Kerala, India*

ABSTRACT

Cloud computing is used for storing and accessing data over the Internet. Data stored in the cloud storage is one by Cloud Service Provider and it has a practical way to protect data from unauthorized users. So, to improve the data transmission over the cloud network is very essential aspect. Cryptography provides some methods for securing the data. For that Encryption Algorithms are used to protect the confidentiality of data. Hybrid encryption is a combination of two or more algorithms (symmetric or asymmetric) together and provides more security than a single encryption can do. The cloud has many security issues like networking, memory management etc. Cryptography in cloud computing provides a secure service regarding security and privacy in cloud. This provides safe data transmission over the cloud network. Hybrid encryption in cloud computing is an effective method to resolve the problem of safe transmission in Internet.

Keyword - *Cryptography, Hybrid encryption, cloud computing, safe transmission*

1. INTRODUCTION

Cloud computing is used for storing and accessing personal, confidential and sensitive data [1]. Therefore, improving such data over the cloud network is very essential. Data stored in the cloud storage is managed by Cloud Service Provider. Cryptography provides some algorithms for securing the data over the network [8]. Encryption Algorithms are used to protect the data. Hybrid encryption provides dual protection for the data over the cloud network [8]. Hybrid encryption is a process by which combines two or more algorithms together and provides more security than a single algorithm can do. Cloud computing is used for complex systems with large scale systems with multiple users [10]. So, it is very important to ensure the security of data and authenticity of users in the cloud network. Crypto Cloud computing provides safe transmission mechanism for data over the network. This mechanism includes confidentiality, integrity, authentication of identity, and non-repudiation [8], [9].

Internet is an open system to public; it must face many problems in various fields. The problems may include network attack, hacker intruding, interception and tampering of network information etc. Cryptography is used for safe data transmission over the network. Cryptography is the process by which the original message is converted

into some other form [8]. This conversion of original message to cipher text is called encryption and the encrypted message is called cipher text. This process is shown in Figure 1 [8]. And the reverse process is called Decryption; that is, creating the original message from the cipher text. There are different cryptographic algorithms. Cryptographic algorithms are mainly classified into

• Symmetric Encryption(Secret Key Cryptography)
• Asymmetric Encryption(Public Key Cryptography):Uses one key for encryption and another one for decryption.
• Hash Functions: Mathematical transformation is used for encryption.

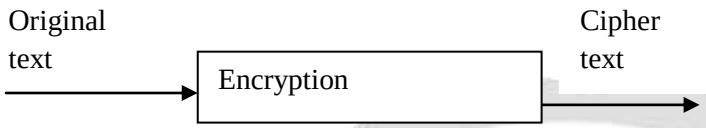

Figure1. Encryption

2. Symmetric Encryption(Secret Key Cryptography)

Single key is used for both encryption and decryption[8]. Different algorithms are used for encryption by single key. Some of them are:

2.1 DES (Data Encryption Standard) Algorithm

It is a traditional encryption algorithm adopted by American government in 1976 [8]. DES algorithm uses many cryptographic technologies. Plaintext is divided into many blocks. Each block has 64 bits and the key length is 64 bits. Only 56 bits are valid bits and the rest of 8 bits are used for parity checking. [3].

Disadvantages of DES:

- Length of DES key is too short.
- Distribution of key is difficult, if key lose system become worthless.
- Calculation of DES is linear.

2.2 Triple-DES (3DES)

3DES is three times secure than DES. The process of 3DES is same as DES, but the operations are performed three times. It provides 112 bits for keys [3][8].
Disadvantages of 3DES:
Computation (Encryption and Decryption) is performed 3 times than DES.

2.3 AES

Advanced Encryption Standard (AES) was adopted by US government. AES has 3 blocks 128,192,256 respectively [4][7]. AES has 10 rounds for 128 bit keys, 12 rounds for 192 bit keys and 14 rounds for 256 keys.

3. PUBLIC KEY ALGORITHM (ASYMMETRIC CRYPTOGRAPHY) -RSA ALGORITHM

Public key algorithm is also known as Asymmetric key algorithm. In Public key algorithm, for encryption it uses one key and for decryption it uses another key. And also, Public key is open and Private key is secret. There are two uses for public key cryptography, Public key encryption and Digital signature [2].

• RSA Algorithm: In RSA, public key is opened to outside and private key is kept secret [4].

• Diffie-Hellman: D-H is used for secret-key key exchange only, and not for authentication or digital signatures.

• Digital Signature Algorithm (DSA): The algorithm provides digital signature capability for the authentication of messages.

• ElGamal: Designed by Taher Elgamal, a PKC system similar to Diffie-Hellman and used for key exchange.

• Elliptic Curve Cryptography (ECC): ECC can offer different levels of security with small keys comparable to RSA and other PKC methods.

The public key algorithms are relatively costly compared with most symmetric key algorithms [2].

4. CLOUD SERVICE MODELS

There are mainly three types cloud services:

4.1 Software as a service (SaaS)

Cloud Service Providers manages and stores the data in the cloud storage. It is also known as "On-demand software" because usually cost is estimated on a pay-per-use basis [10].

4.2 Platform as a service(PaaS)

In this model, the user can develop and deploy applications in the network without any expenditure and complexity. The user will have complete freedom over the application [10].

4.3 Infrastructure as a service (IaaS)

In this model, the institution which wants to use the cloud services outsources all its servers, storage, network etc. to external provider [2].

5. CLOUD CRYPTOGRAPHY

Cloud has many security issues like networking, memory management, virtualization etc. Cloud cryptography is a secure service regarding security and privacy. Cloud Cryptography depends on the cloud architecture used. Most valuable assets in the cloud network are user data. Hybrid encryption provides confidentiality, integrity and non-repudiation in the network [9].

The existing solutions for the security of data and information over the cloud are obtained by encryption algorithm, without taking into consideration the confidentiality level of data. Here propose a secure cloud computing model based on data classification. The objective of this proposal is to establish the required level of security for data. Data classification techniques are applied and based on this classification, different hybrid encryption algorithms are used to provide security for data. It reduces processing time and provides reliability and confidentiality.

6. THE IDEAS AND PROCESSES OF HYBRID ENCRYPTION ALGORITHM

Hybrid encryption combines symmetric and asymmetric algorithms together for ensuring security. Different hybrid encryption methods proposed here for securing different levels of data are:

6.1 DES and RSA algorithm

DES is symmetrical and RSA is asymmetrical encryption algorithms [6]. DES algorithm is used for data transmission because of its higher efficiency in block encryption, and RSA algorithm is used for the encryption of the key of the DES because of its management advantages in key cipher [1].

The comparison is showed as below:

- Combination of DES and RSA algorithm have strong security [5],[8].
- The speed of DES is faster than RSA algorithm. RSA algorithm has many steps for calculation, so speed of RSA is slower than DES [1].
- RSA algorithm is better than DES algorithm because, public key is opened to outside and private key is kept secret. However, DES needs key pair [5].

6.2 Triple DES and RSA

Data safe transmission bases on triple DES and RSA algorithm. It makes use of the advantage of triple DES which has the high encryption speed for plaintext [9]. And also, it provides three times more security than DES. It also uses the merit of RSA which manages the key easily [4].

6.3 ABE and AES algorithm

Each authorized user has username and password. Each user has a pair of security keys. With this keys user can encrypt and send the messages .We can see the sender A creates the data file and encrypts the attributes of the data using ABE and symmetrical encryption algorithm AES[4]. In ABE, the concepts of public and private keys are replaced by sets of attributes, which abstract from actual user properties. Moreover, ABE has a central trusted party called attributes authority issues the cryptographic credentials, which is in possession of a global master key for key generation. Since users are associated with sets of attributes, they might try to trade some attributes and related private key components to gain more decryption powers.

An Overview of Hybrid Encryption using ABE and AES algorithm,

A random session key (S) of AES algorithm is generated.

- The message(M) is symmetrically encrypted using AES under S, producing ciphertext C1.
- S is CP-ABE encrypted under an attribute policy, producing ciphertext C2.
- C1 concatenated with C2 represents the ciphertext C.
- Create message digest of C using suitable Hash Function [5].
- C is transferred to a receiver R.

Hybrid Decryption

- After reception of C = C1||C2, receiver R tries to decrypt C2, using his private attribute set {A}R.
- R's Key is recovered, in order to reconstruct S.
- S is used to symmetrically decrypt C1 to M using AES .
- Generate the Message digest from the received message using Hash Function [5].
- Compare the Hash of message generated & the Hash of message received.

CP-ABE can be used in hybrid mode: a message it self is encrypted with a random symmetric secret key. Only this session key is then CP-AB encrypted under a policy.

CP-ABE can be used in hybrid mode: a message it self is encrypted with a random symmetric secret key. Only this session key is then CP-AB encrypted under a policy.

6. REFERENCES

[1]. Wuling Ren, Zhiqian Miao,(2010),'A Hybrid Encryption Algorithm Based on DES And RSA in Bluetooth Communication', Proceedings IEEE Conference on Modeling, Simulation and Visualization Methods,Vol.5,pp.221225.

[2]. IEEE 1363: Standard Specifications for Public-Key Cryptography .

[3]. H. G. Zhang, Y. Z. Liu, "Evolution password and DES evolution research," Chinese Journal of Computer, vol 12, no. 2, pp. 1678-1684, September 2003.

[4]. B. Yang, Modern Cryptography[M], Beijing: Tsinghua University Press, 2006

[5]. Kui-He Yang, Shi-Jin Niu,(2009), 'Data Safe Transmission Mechanism Based on Integrated Encryption Algorithm', International Conference on Computational Intelligence and Software Engineering,Vol.7, pp.1 – 4.

[6]. S. P. Wang, Y. M. Wang, "Digital signature scheme based on DES and RSA," Journal of Software, vol 14, no. 1, pp. 146-150, June 2003.

[7] . Douglas R. Stinson, Cryptography Theory and Practice[M], Beijing: Publishing House of Electronics Industry, 2002.

[8]. Weber, S.G.: A Hybrid Attribute-Based Encryption Technique Supporting ExpressivePolicies and Dynamic Attributes. Information Security Journal: A GlobalPerspective 21(6), 297{305 (2012).

[9]. Salini Dev P V , Ann Preetha Jose, Jesline Joseph "Hybrid Encryption Algorithm for Data Transmission over public network "Vol-2 Issue-4 2017 IJARIIE-ISSN(O)-2395-4396

[10]. Akansha Deshmukh, Harneet Kaur Janda, Sayalee Bhusari, " Security on Cloud Using Cryptography" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 3, March 2015 ISSN: 2277 128X.