ATTRIBUTE BASED ENCRYPTION USING MODIFIED HOMOMORPHIC ALGORITHM

Jasleen Saini[1], Roshan Srivastava[2]

[1]*Assistant Professor, Lovely Professional University*
[2]*Assistant Professor, Lovely Professional University*

Abstract

Cloud Computing provides the best platform for such a sharing service because of its scalability and availability. Cipher text policy attribute-based is becoming an appreciative to guarantee data security in cloud computing. In this paper, key escrow problem is solved by using the scheme of homomorphic encryption in which mathematical operations are done on encrypted data without compromising the encryption and proxy re-encryption is also used which is master secret secure. Also Diffie Hellman algorithm is used to make the data more secure. In this paper, previous related work is reviewed with a concentration on the security challenges associated with sharing of data in which third party is involved.

Keywords— *Homomorphic Encryption, Diffie Hellman Algorithm, Proxy Re-Encryption, Key Escrow*

----------***----------

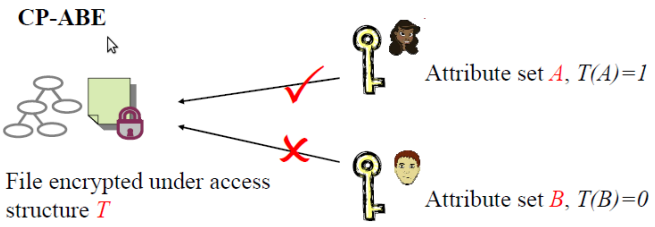
1. INTRODUCTION

Cloud computing includes the sharing of data in network. Cloud computing has been used widely for both computations and data storage. The cloud secures confidentiality, integrity and availability of data. The most important security concern is data confidentiality as the data stored in the cloud may be known to the unauthorized users in the cloud service provider. In order to protect the data present in cloud, data owners will encrypt their data before sending on the network. The cipher text attribute based is an advanced concept that enables data owner to define access policy over the attributes that a user needs to own in order to decrypt the cipher text ie., each user with a different attributes is allowed to decrypt the data. The attribute based encryption is reliable for data access control. The major contributions of attribute based encryption include:

• Examine the existing CP-ABE completely to monitor performance.
• Parallelize key generation and encryption and decryption process.

CP-ABE has reveled effecient potentials for cloud storage with major performance issues. There is one problem of key escrow which is solved by multiple attribute authority in which all the authorities communicate with each other to generate the key and user will get each part of key from each authority as authorizers has some part of key so that they cannot access the data. But in this method, computation overhead is more.

The representations of encryption and decryption based on the attributes are complex as the attributes for the accessing the control are different every time. As the computation overhead is high for key escrow problem in multiple attribute authority method, a homomorphic encryption is used in which computation is allowed to be carried out on ciphertext, thus generating an encrypted result which when decrypted matches the results performed on the plain text ie., mathematical calculations are done with normal encryption which makes the encryption complex and cannot be access by the third party or attribute authorities. An efficient attribute revocation method for cipher text policy attribute based encryption that sustain less computation cost as the key server only updates cipher text associated with revoked attributes and attribute key components. Since this attribute revocation does not necessarily update the keys of attributes.



2. LITERATURE SURVEY

Junbeom Hur (2013): In this paper, the author discuss the key escrow problem, in which the attribute authority can recognize the attribute keys to decrypt the data. So, the author took an approach to have multiple attribute authorities. All the attribute authorities will communicate with each other to generate the whole key as the different authorities have only a part of that key to generate and the user will communicate with every attribute authority to get the parts of the keys. The Key generation center and the data-storing center are involved in the user key issuing protocol. In the protocol, a user is required to contact the two parties before getting a set of keys.

The proposed algorithm increases the data privacy and confidentiality in the data sharing system against any system managers. The only problem is the extra burden as the attribute authorities have to communicate with each other. It increases the computation overhead as the cost increases for the communication.

HUANG Qinlong, MA Zhaofeng, YANG Yixian(2015): In this paper, work is related to the privacy and security of data sharing. The data sharing which is in encrypted form requires a key management in which the keys for decryption should be given to the authorized user which is considered to be less scalable and flexible. The attribute based encryption scheme will be considered as a good method for having better scalability and flexibility. The researcher proposed a homomorphic encryption with addition to attribute based encryption, to solve the key escrpw problem. Homomorphic operation is done on the cipher text to make it more complex so that any random third party cannot access the data to be transferred on the network. The homomorphic operation is donated by $\oplus$ which is used as a symbol during encryption.

For encryption, a plain text is taken and a public key after a generation of a public key which is denoted by C = Enc(PK,M) where C is the cipher text and in a similar way decryption is done ie., M = Dec(SK,C)where SK is the secret key. After that homomorphic encryption is done on the cipher text by taking two cipher texts ie., C1 and C2. By applying homomorphic algorithm the cipher text will be as C= C1 $\oplus$ C2.

By using this attribute based algorithm having homomorphic encryption, the security aspect and the performance of the algorithm is analyzed. The data is confidential as the user who has enough attributes, used as a key, can decrypt the data. If the user has not suitable attributes cannot recover the data as the user is considered as an un-authorized person. If the user has stored the previous cipher text and use the set of attributes, he cannot decrypt the data.

SU Mang, LI Fenghua, SHI Guozhen, GENG Kui, XIONG Jinbo (2016): In this paper, the author has discussed attribute based encryption with cipher text policy which is suitable for data access control in cloud storage. The Proxy re-encryption technology is used to solve the large calculation which also provides support for implementation of attribute based encryption and Identity based encryption (IBE). The proxy re-encryption divides the plain text into different types and used different private keys. The Decisional Bilinear Diffie-Hellman algorithm is used. In this, a parameter is taken by using a generator say g and a key is generated. After that, the encryption is done. This process of generation of key and re-encryption is done in order to increase the security. The Proxy re-encryption algorithm reduces the computational overhead and key management.

Lifeng Li, Xiaowan Chen, Hai Jiang (2016): In this paper, the author has discussed the key management and encryption and decryption process. The analyzation of cipher text policy attribute encryption is done to identify its performance and multithreading technique is used for encryption and decryption. The parallelization of cipher text policy is done to speed up the major processes such as key generation and encryption and decryption for acceptable performance. Parallization CP-ABE adopts AES-CTR (Counter mode) to overcome the weaknesses in AES-CBC(Cipher Block Chaining). In AES-CTR, all data blocks are independent for full parallelization and direct data access is supported. Flexibility helps achieve performance gains. Finally, AES-CTR supports preprocessing to accelerate encryption and decryption further.

3. PROPOSED WORK

The proposed work for encryption includes Modified homomorphic algorithm which is the advancement of Homomorphic algorithm for Attribute based encryption which involves:

- Using the algorithm for Attribute based encryption, it makes the data complex as the data can be divided into two messages. It is further encrypted separately.
- Both the cipher texts will be first added and then multiplied to make it difficult to understand for any unauthorized person.
- The special operation is used for both the cipher texts to combine in one cipher text.

4. COMPARISON

In J.Hur (2013), the key escrow problem is solved by using different attribute authority to make the parts of key but it increase the communication overhead. But in HUANG Qinlong, MA Zhaofeng, YANG Yixian(2015) paper, they uses the homomorphic encryption due to which the algorithm is complex and the authority cannot decrypt the data. So only a single authority is concerned due to which communication overhead decreases.

In SU Mang, LI Fenghua, SHI Guozhen, GENG Kui, XIONG Jinbo (2016) paper, the diffie hellman algorithm is used for attribute based encryption but it creates problem while generating a generator. The generator is randomly taken which is not suitable always. Hence HUANG Qinlong, MA Zhaofeng, YANG Yixian(2015) paper is better in which homomorphic algorithm is used.

In Lifeng Li, Xiaowan Chen, Hai Jiang (2016) paper, the analyzation of cipher text policy attribute encryption is done to identify its performance and multithreading is used for encryption and decryption. The multiple processes are done to speed up the major processes.

5. CONCLUSION

From the literature survey it is concluded that the attribute based encryption is used for encryption in which a set of attributes are taken in order to get the data which can be decrypted using these set of attributes. From the above papers it is found that the Homomorphic encryption is better as it provides complexity during encryption in which

mathematical calculations are done. To make it more complex, the advanced version of homomorphic technique is used which is Fully Homomorphic encryption. It makes the algorithm more complex and efficient.

REFERENCES

[1]. Junbeom Hur, "Improving security and efficiency in attribute based data sharing", vol 25, No. 10, October 2013.
[2]. Junbeom Hur and Dong kun Noh, "Attribute based access control with efficient revocation in data outsourcing systems" , vol 22, No. 7, October 2011.
[3]. HUANG Qinlong, MA Zhaofeng, YANG Yixian, " Attribute based secure data sharing with efficient revocation in cloud computing", Information security center, Beijing, China, vol 24, No. 4, October 2015.
[4]. SU Mang, LI Fenghua, SHI Guozhen, GENG Kui, XIONG Jinbo, " A user-centric data Secure creation scheme in cloud computing", University of science and Tech., Nanjing, China, Vol 25, N0. 4, July 2016.
[5]. Lifeng Li, Xiaowan Chen, Hai Jiang, "Parallelizing cipher text policy attribute based encryption for clouds", College of Info. science and Tech., China, June 2016.