International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

CIPHER TEXT POLICY ATTRIBUTE BASED ENCRYPTION BY DEDUPLICATION FOR TIME LIMIT CLOUD DATA SHARING

ANU BABY[1], CHINCHU JACOB[2]

[1]M.Tech student Computer science and engineering,
[2]Assit professor, Department of computer science and engineering, Indira Gandhi Institute of Engineering and Technology, Nellikuzhi, Kerala, India

---

Abstract - *Security in cloud computing is a major concern. Cipher text policy attribute-based encryption (CP-ABE) is a cryptographic technique for proper access control of outsourced data in the cloud. The main aim of this paper is to develop an efficient collaborative key management protocol for secure cloud data storage by implementing file encryption, key generation, methods. And also prevent de duplication during file uploading by checking whether particular file is existed or not. Also decrease the cloud storage. The collaborative mechanism effectively solves not only the key escrow problem but also the key exposure problem. Meanwhile helps markedly reduce client decryption overhead. In proposed system mainly there are three keys are provided to secure cloud data sharing. That is public key private key and secret key. Cipher text policy attribute-based encryption is a promising cryptographic technique for secure cloud storage. Data de duplication has been widely used for cloud storage to reduce storage space and by eliminating same data and storing only one copy. The proposed scheme performs better in cloud data sharing system serving massive performance with respect to either security or efficiency.*

***Key Words*: Security, Efficiency, CP-ABE, Cloud data sharing, Key Generation**.

1. INTRODUCTION

In order to achieve secure data de duplication the convergent encryption scheme and many of its variants are proposed. In proposed system mainly there are 3 keys are provided to secure cloud data sharing. That is public key, private key and secret key. The simultaneous participation of a large number of users requires proper access control for data sharing.

Attribute-based encryption (ABE) is a promising cryptographic primitive that offers an interesting solution to secure and flexible data sharing. Traditional de duplication schemes cannot work on an encrypted data. And also prevent de duplication during file uploading by checking whether particular file is existed or not. Main purpose is to decrease the storage of cloud. For large numbers of previous ABE schemes the key authority must be completely trustworthy, as it can decrypt all the cipher text using a generated private key without permission of its owner. This is commonly called the key escrow problem and is an inherent disadvantage that threatens user privacy.

1.1. OBJECTIVE

Data de duplication has been widely used in cloud storage to reduce storage space and communication problem by reducing same data and storing only one copy for them. Confidential and sensitive data stored in the cloud is extremely crucial. So that the main aim is to protect data sharing using keys.

1.2. SCOPE

The main scope of this is to provide security and efficiency of cloud data sharing .Also reduces the redundant data in order to decrease the storage of cloud. The proposed collaborative mechanism perfectly addresses not only key escrow problem but also key exposure

2. RELATED WORK

Fuzzy identity-based encryption (FIBE) based on classic identity-based encryption. The identity of a receiver is represented by a set of attributes, which is embedded into his/her private key. If and only if the distance between the attribute set of receiver and the one of sender is shorter than a threshold, a receiver can extract the plaintext correctly. Since FIBE indicated some many key features of ABE, it laid a by introducing access tree, they built a fine-grained access policy for ABE. There must be another type of ABE called cipher text policy ABE (CP-ABE). For CP-ABE, each cipher text is associated with an access policy and each private key is associated with a set of attributes. A concrete construction of CP-ABE, in which a data sender can flexibly define the access policy before data is encrypted. Consequently, their CP-ABE guarantees not only data confidentiality but also realization of autonomic access control.

The research demonstrated that CP-ABE is more suitable for construction of data outsourced system than KP-ABE. Novel access tree contain only AND gates with positive and negative attributes to enhance expressiveness of ABE access policy. At mean time, they introduced one-time signature to prove their CP-ABE is secure under chosen cipher text attacks (CPA-secure) with the reduction to Decisional

Bilinear Diffie-Hellman Assumption (DBDH). Their efficient scheme supports more flexible attribute revocation and user revocation, which enhanced forward and backward secrecy. Chandar concentrate their work on efficiency of revocation and proposed a hierarchical ABE (HABE).In their construction, lazy re-encryption was introduced .So that only message to be updated will be re-encrypted. The analysis demonstrated HABE markedly reduces the global computation overhead for attribute revocation and user revocation. In addition, the proposed scheme is proven to be selectively for secure with the reduction to Decisional Parallel Bilinear Diffie-Hellman Exponent Assumption (DPBDHE). Green indicated that cipher text size and decryption cost are major drawbacks of practical ABE applications. To overcome such problems, they proposed a novel ABE with outsourced decryption (OD-ABE) for both CP-ABE and KP-ABE used. That sets a proxy server for executing most of decrypting computation. When implementing decryption, a data receiver transfers a transform key and the cipher text to a proxy server and receives an ElGamal style cipher text. Subsequently, the plaintext can be extracted via very simple computation by the data receiver.

3. PROPOSED SYSTEM

Develop an efficient collaborative key management protocol for secure cloud data storage by implementing file encryption, key generation, methods. There are four important phases that are shown in Fig -1.

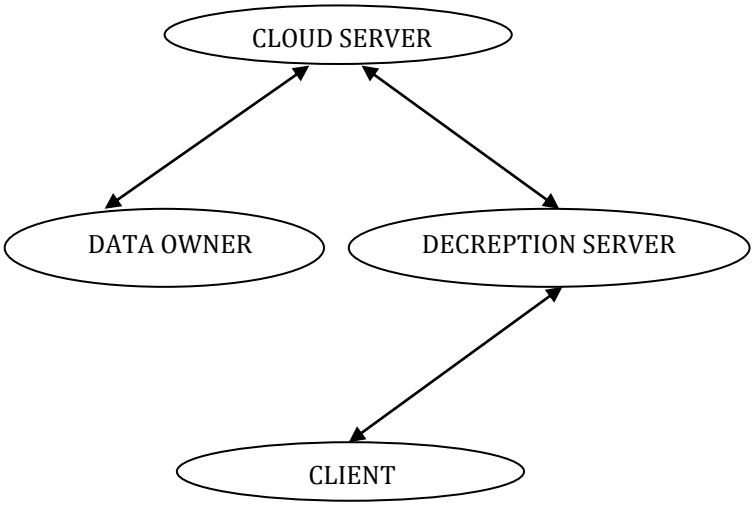

Fig -1: Basic Model of CKM-CP-ABE

Four different phases of Cipher text policy attribute-based encryption (CP-ABE).That is data owner, cloud server, decryption server and client.Fig-1 shows the four different phases of Cipher text policy attribute-based encryption (CP-ABE).That is data owner, cloud server, decryption server and client. A data owner (DO) is an authorized user in the system who can possesses data to be uploaded. A client (CL) is a user who intends to access data in cloud storage via front-end devices. Decryption server has powerful computing capabilities that are undertake and isolate the most but not all task of decryption. A cloud server (CS) is responsible for cloud storage management. All the data to be shared is in the control of the CS.

3.1 WORKING MODEL OF CKM-CP-ABE

Working model of CKM-CP-ABE contains data owner, cloud server, client and key authority. The main purpose of client is to access the data securely. So that three keys are mainly used for this. That is public key, private key and secret key. These three keys are generated from key authority (KA).Main purpose of this KA is generating keys securely as shown in Fig-2. KA is very important thing in this work. A cloud server (CS) is responsible for cloud storage management. All the data to be shared is in the control of the CS. A data owner (DO) is an authorized user in the system who can possesses data to be uploaded. If any client wants to download the data they can request the particular file for the data owner. So that data owner can accept that client request such that they can accept or reject it. If data owner wishes to accept client request then three keys along with client login id will generated on the client mail and to the registered mobile number .Then by using such keys and id client can enter these into the keys option and id option. From this way client can download the particular uploaded file.

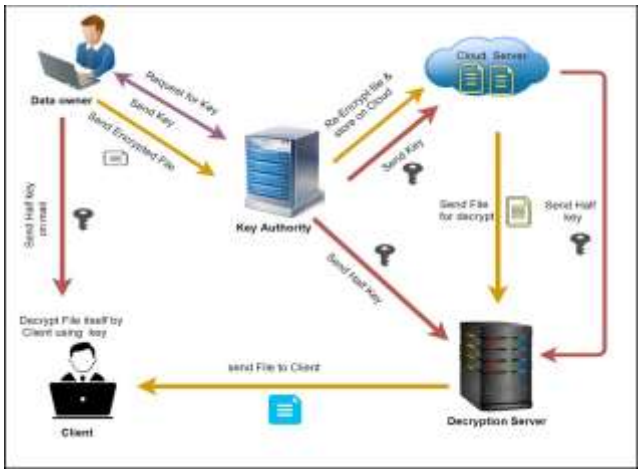

Fig -2: Working Model of CKM-CP-ABE

4. CONCLUSION

Cipher text policy attribute-based encryption is a promising cryptographic technique to realize proper access control in secure cloud storage. Collaborative key management protocol helps to enhance both security and efficiency of key management in cipher text policy attribute-based encryption for cloud data sharing system. The proposed collaborative mechanism perfectly addresses not only key escrow problem but also key exposure. Data

deduplication has been widely used in cloud storage to reduce storage space and communication overhead by eliminating redundant data and storing only one copy for them. In order to achieve secure data de duplication, the convergent encryption scheme and many of its variants are proposed.

REFERENCES

[1] S. Rafaeli, and D. Hutchison, "*A survey of key management for secure group communication," ACM Computing Survey, vol. 35, no. 3,* pp.309-329, (2003).

[2] A. Sahai and B. Waters, "*Fuzzy identity-based encryption," in Proc. Euro Crypt,* pp. 457-473, (2005).

[3] J. Bethencourt, A. Sahai, and B.Waters, "*Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secure. Privacy,* pp. 321-334, (2007).

[4] S. S. M. Chow, "*Removing escrow from identity-based encryption," in Proc. Int. Conf. Practice and Theory in Public Key Cryptography,* pp. 256-276, (2009).

[5]N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," in *Proc. Int. Conf. Pairing-Based Cryptography*, 2009, pp. 248-265, (2009).

[6] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "*Security and privacy challenges in cloud computing environments," IEEE Security & Privacy, vol. 8, no. 6*, pp. 24-31, (2010).

[7] B. Waters, "*Cipher text-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in Proc. Public Key Cryptography,* pp. 53-70, (2011).

[8] G. Zhang, L. Liu, and Y. Liu, "*An attribute-based encryption scheme Secure against malicious KGC," in Proc. TRUSTCOM, pp.*1376-1380, (2012).

[9] J. Hurl, *"Improving security and efficiency in attribute-based data sharing," IEEE Trans. Knowl. Data. Eng., vol. 25, no. 10,* pp. 2271-2282, (2013).

[10] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "*Privacy-preserving public auditing for secure cloud storage," IEEE Trans. Compute., vol. 62, no. 2*, pp. 362-375, (2013).