KEY POLICY – ATTRIBUTE BASED ENCRYPTION BASED INFORMATION ALLOCATION SYSTEM REVISITED IN CLOUD COMPUTING

[1]Dr.A.Rengarajan,[2]E.Manju,[3]B.Monisha N.Reshma[4]
[1]Assisstant Professor,[2,3,4]UG Scholar,
[1,2,3,4]Department of Computer Science and Engineering,
[1,2,3,4]Vel Tech MultiTechDr.RangarajanDr.Sakunthala Engineering College,
(Approved by AICTE, New Delhi & Affiliated to ANNA UNIVERSITY, CHENNAI) Avadi, Chennai-62, India.
rengarajan@veltechmultitech.org[1],
manjuelaiyaperumal2014@gmail.com[2],bmonisha9@gmail.com[3],nsreshma1995@gmail.com[4]

ABSTRACT

Cloud brokers recently introduced an additional computation layer for cloud Selection and service management tasks for cloud consumers. It is possible for dishonest broker to easily take advantage of limited capabilities of clients and Provides incorrect incomplete response. We propose a cloud based secure data System, which allows a semi trusted authority to store secret data with range of Data receiver. It reduces the key management complexity for authorizes, owners and data receivers. Different from previous system, data owners encrypt their Secret data for data receivers using CP-ABE encryption. Data receiver will send request to authority. The owner has access control. If owner want to share file with data receiver. After accepts request the data receiver download secret key and download original data.

KEYWORDS - Attribute based encryption, key policy-attribute based encryption, Semi trusted cloud, Access control

I.INTRODUCTION

Key policy attribute encryption is used which makes the cipher text depends upon the key. We generate if data receiver wants any data, then he will send the request to data owner, the data receiver does not have any download option. And when on data owner side, if he upload a file, it gets encrypted and three key along with their duplicates are generated and gets stored in the cloud server. The data owner verify whether he is a designated receiver by checking the attribute, the first key that is private key will be given to data receiver. Then the particular private key will be compared with all other files in the cloud server. Once the match is found, then the protected key and secret key by using these keys data receiver download original plain text.

1. Storing files

The data owner to securely store their secret data on the semi-trusted cloud service providers, and selectively share their secret data with a wide range of data receiver.Data owner upload the several files and data.

2.Data protection

For the security purpose we introduce the Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key.Data can be encrypted with respect to subsets of attributes.Data can be encrypted with respect to subsets of attributes, only be able to decrypt the cipher-text if the person holds the "matching attributes"

3.Authentication

Data owner will verify the data receiver's full details whether the person is the right person or cloud broker.The data receivers want to send request for the file which he want to download.Cloud server check the details if the Data owner want to share the original file with the data receiver he will accept the request

4.Secure data retrieval

After request being accepted by the data owner, the data receiver downloads the keys and use this key to download the original data in decrypted format.The key issue is, that someone should only be able to decrypt a cipher text if the person holds a key for "matching attributes" where user keys are always issued by some trusted party

EXISTING SYSTEM

- Cipher text-policy attribute-based encryption (CP-ABE) is used solve challenging problems of secure data sharing in cloud computing
- The shared data files generally have the characteristics of multi level hierarchy ,particularly in the area of military and health care
- An efficient file hierarchy attribute-based encryption scheme is proposed in cloud computing
- The layered access structure are integrated into single access structure and hierarchical files are encrypted with the integrated access structure
- The cipher text components are related to attributes could be shared by files
- Both cipher text storage and time cost of encryption are saved

PROPOSED SYSTEM

- A cloud-based secure data system , which allows data owner to securely store their secret data on the semi-trusted cloud sever
- Data owner selectively share their secret data with a wide range of data receiver
- Reduces the key management complexity for authority owners and data receivers
- The cloud server cannot access any file, since it is in encrypted cipher-text
- Attribute Based Encryption algorithm is a hierarchical structure to improve scalability and flexibility
- The performance measurements indicate that the proposed scheme is efficient to securely manage the data stored in the data storage servers and significantly reduces the computation time

ALGORITHM

ABE (ATTRIBUTE BASED ENCRYPTION)

In Attribute-based encryption (ABE) scheme, attribute play a very important role. Attributes have been exploited to generate a public key for encrypting data and have been used as an access policy to control user's access. The access policy can be categorized as either key-policy or cipher-policy. The key-policy is the access structure on the user's private key, and the cipher-policy is the access structure on the cipher-text. And the access structure can also be categorized as either monotonic or non-monotonic one.

Using ABE schemes can have the advantages:

(1) To reduce the communication overhead of the Internet,
(2) To provide a fine-grained access control.
(3) This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access and provides integrity. The scheme substantially reduced the computation time required for resource-limited devices to recover plaintexts.
(4) Data can be encrypted with respect to subsets of attributes. The key issue is, that someone should only be able to decrypt a cipher text if the person holds a key for "matching attributes" where user keys are always issued by some trusted party.
(5) Data confidentiality
(6) On-demand revocation
(7) Write access control
(8) Scalability and usability

KP-ABE (KEY POLICY – ATTRIBUTE BASED ENCRYPTION)

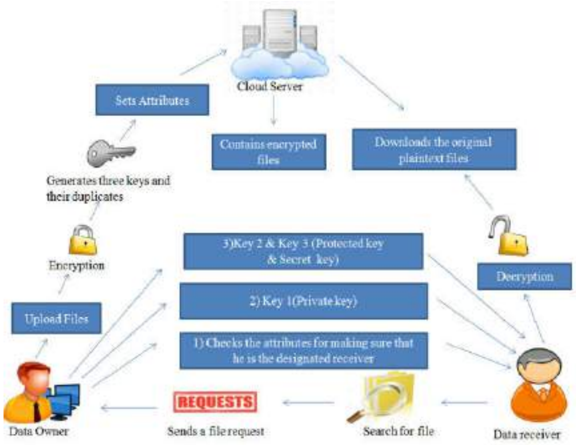
An important property which has to be achieved by both, CP- and KP-ABE is called collusion resistance.

This basically means that it should not be possible for distinct users to "pool" their secret keys such that they could together decrypt a cipher text that neither of them could decrypt on their own (which is achieved by independently randomizing users' secret keys)

The advantages of key policy – attribute based encryption are

- ✓ This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access and provides integrity. The scheme substantially reduced the computation time required for resource-limited devices to recover plaintexts.
- ✓ Data can be encrypted with respect to subsets of attributes. The key issue is, that someone should only be able to decrypt a cipher text if the person holds a key for "matching attributes" where user keys are always issued by some trusted party.

ARCHITECTURE


Cloud Server
Sets Attributes
Contains encrypted files
Downloads the original plaintext files
Generates three keys and their duplicates
Encryption
3)Key 2 & Key 3 (Protected key & Secret key)
Decryption
2) Key 1(Private key)
Upload Files
1) Checks the attributes for making sure that he is the designated receiver
REQUESTS
Data Owner
Sends a file request
Search for file
Data receiver

CONCLUSION

We tackle the open problem of proposing a leakage of data. We propose a cloud based secure data system, which allows trusted authority to securely store their secret data on the semi-trusted cloud service providers, and selectively share their secret data with a wide range of data receiver. Different from previous cloud-based data system, Data owners encrypt their secret data for the data receivers using CP-ABE Encryption scheme. In addition for classification of data files a new classification algorithm is proposed

REFERENCES

[1] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, “A secure cloudcomputing based framework for big data information management of smart grid,” *IEEE Trans. Cloud Comput.*, vol. 3, no. 2, pp. 233–244, Apr./Jun. 2015.

[2] A. Balu and K. Kuppusamy, “An expressive and provably secure ciphertext-policy attribute-based encryption,” *Inf. Sci.*, vol. 276, no. 4, pp. 354–362, Aug. 2014.

[3] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, and H. Shacham, “Randomizable proofs and delegatable anonymous credentials,” in *Proc. 29th Annu. Int. Cryptol. Conf.*, 2009, pp. 108–125.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in *Proc. IEEE Symp. Secur. Privacy*, May 2007, pp. 321–334.

[5] D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the Weil pairing,” *J. Cryptol.*, vol. 17, no. 4, pp. 297–319, 2004.

[6] M. Chase, “Multi-authority attribute based encryption,” in *Proc. 4th Conf. Theory Cryptogr.*, 2007, pp. 515–534.

[7] M. Chase and S. S. M. Chow, “Improving privacy and security in multiauthority attribute-based encryption,” in *Proc. 16th ACM Conf. Comput. Commun.Secur.*, 2009, pp. 121–130.

[8] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,” in*Proc. 14th ACM Conf. Comput. Commun.Secur.*, 2007, pp. 456–465.

[9] S. S. M. Chow, “Removing escrow from identity-based encryption,” in*Proc. 12th Int. Conf. Pract. Theory Public Key Cryptogr.*, 2009, pp. 256–276.

[10] C.-K. Chu, W.-T.Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, “Security concerns in popular cloud storage services,” *IEEE Pervasive Comput.*, vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.