COMPRESS AND SECURE DATA SHARING FOR MOBILE CLOUD COMPUTING

M.Thulasimani[1], M.Valarmathi[2], R.Limya[3]

[1,3]Research Scholar, Department of Computer Science, Vivekanandha College for Women, Tiruchengode, India.
[2]HOD of Computer Science , Vivekanandha College for Women, Tiruchengode,India.

Abstract - *In cloud computing mobile devices are used to store/retrieve personal data and organizational data from anywhere at any time. Therefore, the data security problem in mobile cloud becomes crueler and prevents further improvement of mobile cloud. Today data security problem is one of biggest problem in the cloud. The major challenge faced by one and all is to share the data all over the world securely without giving away the essential data to any exploiters. To triumph over the challenge to share the information securely over the cloud by using efficient data encryption algorithm for encrypting data before sending the data to the cloud. In this paper, Key policy Attribute Based Encryption (KP-ABE) and Cipher text Policy Attribute Based Encryption (CP-ABE), these are two Attributes used to storing and retrieving the data from the cloud. Among these two attributes which one is the best attribute for cloud saving and retrieving in secured manner through mobile devices.*

Key words: Mobile cloud computing, Key policy - ABE, Cipher text Policy – ABE, Data security, Data sharing.

1. INTRODUCTION

With the improvement of cloud computing the popularity of smart mobile devices, people are gradually getting into a new era of data sharing model in which the data is stored on the cloud and the movable devices are used to store/retrieve the data beginning the cloud. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider (CSP) to store and share the data. Nowadays, various cloud mobile applications have been widely used. In these applications, people (data owners) can upload their photos, videos, documents and other files to the cloud and share these data with other people (data users) they like to share. CSPs also give data administration functionality for data owners. Since personal data files are perceptive, data owners are allowed to select whether to make their data files public or can only be shared with definite data users. Clearly, data privacy of the personal sensitive data is a huge concern for many data owners. The state-of-the-art privilege management/access be in charge of mechanisms provided by the CSP are either not sufficient or not very convenient. They cannot meet all the necessities of data owners. First, when people upload their data files onto the cloud, they are leaving the data in a place where is out of their control, and the CSP may spy on user data for its commercial interests and/or other reasons. Second, people have to send password to each data user if they only want to share the encrypted data with certain users, which is very cumbersome. To simplify the privilege management, the data owner can divide data users into different groups and send password to the groups which they want to share the data.

2. EXISTING SYSTEM

With the unremitting growth in expansion of cloud computing people are getting clever and familiarized to a new period of data circulation model in which the data is stored on the cloud and the mobile devices are used to store and retrieve the information from the cloud. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider to store and share the data. The enlargement of cloud computing and the acknowledgment of smart mobile devices, citizens are steadily getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the movable devices are used to store/retrieve the data as of the cloud. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider to store and share the data.

3. PROPOSED SYSTEM

To address privacy issue in existing system we propose a crypto-system for secure sharing of data over the cloud, which uses among Key policy Attribute Based Encryption and Cipher text Attribute Based Encryption Algorithm for secure encryption of the data over cloud.

The main three works are as follows:

1. Identify the issues in cloud system for data storage on cloud. Since data is not secure on cloud user can upload the data in encrypted format.
2. Propose a crypto-system which can run on all limited resources devices. It can take data from the user and provide off-line-online service.
3. Apply Key policy Attribute Based Encryption and Cipher text Attribute Based Encryption for encryption of data to firmly transmit the data between the users.

3.1 Architecture And Modules Details

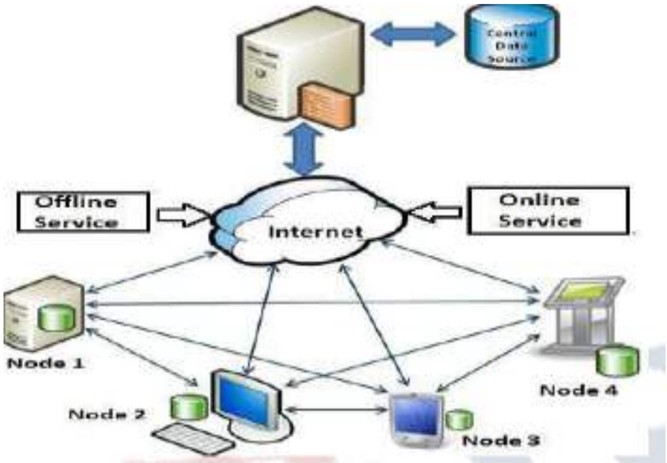

Figure 3.1.1: System Model

The construction of the proposed system is shown in the outline which shows the users and the operations caught up. The detailed depiction of the architecture is explained as follows:

- **Nodes**: The consumer is answerable for uploading and sharing its personal data on the cloud.
- **On-line and Off-line Services**: In On-line Service data will encrypted and honestly transfer to the particular user. In Off-line Service if there is rejection Internet link the data will get encrypted first and then it will get stored in central Server. Awaiting the system does not comes on-line the data will not be shared over the cloud
- **Cloud Service Provider**: Cloud service provider is dependable for providing all the required services to its users according to their difficulty.
- **Encryption and Decryption**: At this point we are using the mixture of KP-ABE and CP-ABE algorithm to encrypt and decrypt the files.
- **File Upload and Download**: The files which are uploaded on cloud are encrypted structure. User's containers download the files which are decrypted if he is sanctioned.

3.2 Key policy Attribute Based Encryption (KP-ABE)

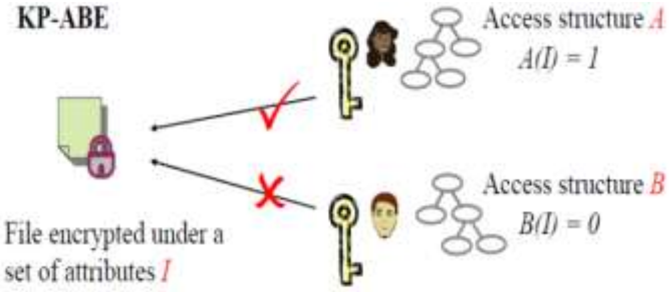

Figure 3.2.1: KP-ABE Access control

It is the customized form of established model of ABE. Users are assigned with an access structure (AS) above the data attributes. To echo the access structure the secret key of the user is defined. Cipher texts are labeled with sets of attribute and private keys are connected with monotonic access structure that control which cipher texts a user is able to decrypt. Key policy Attribute Based Encryption (KP-ABE) method is designed for one-to-many infrastructure. Algorithm takes input K as a protection bound and profits PK as public key and the system master top secret key MK. PK is used by message senders for encryption.MK is used to produce user secret keys and is known only to the authority. Designed for encryption algorithm takes a memo M, the public key (PK), and a set of attribute as input. It outputs the cipher text (CT). Key creation algorithm takes as input an access structure (AS) and the master secret key MK. It outputs as a secret key SK that enables the user to decrypt the point encrypted in a set of attributes if and only if matches T. Decryption is feasible only if the attribute set satisfies the user's access structure. The KP-ABE method can reach protected access control and more flexibility to be in charge of users than ABE scheme.

Drawbacks

The difficulty with KP-ABE method is encrypted cannot make a decision who can decrypt the encrypted data. It can only prefer descriptive attributes for the data, it is not fitting in some submission because a data owner has to trust the key issuer.

3.3 Cipher text Policy Attribute Based Encryption (CP-ABE)

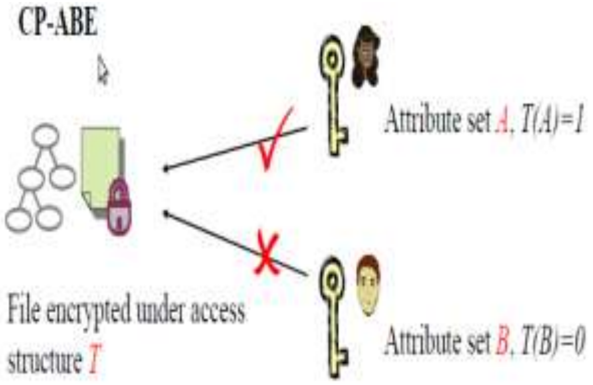

Figure 3.3.1: CP-ABE Access Control

CP-ABE is the customized form of KP-ABE introduced by Sahai. In a CP-ABE plan, every cipher text is linked with an access policy on attributes, and all user's private key is associated with a set of attributes. A user is talented to decrypt a cipher text just if the set of attributes associated with the user's private key satisfies the access policy associated with the cipher text. CP-ABE works in the reverse way of KP-ABE.

The algorithm takes as input a protection parameter K and returns the public key PK as well as a system master secret key MK. PK is used by message senders for encryption.MK is used to generate user secret keys and is known only to the power. On behalf of encryption of data algorithm takes as input the open parameter PK, a message M, and an access structure AS. It outputs the cipher text CT. Key-invention this algorithm takes as input a set of attribute associated with the user and the master key MK. It outputs a covert key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T. Decryption of the data only if satisfy the access arrangement associated with the cipher text CT. It improves the drawback of KP-ABE that the encrypted data cannot choose who can decrypt. It can carry the access control in the real situation. In count, the user's private key is in this scheme, a grouping of a set of attributes, so an user only use this set of attribute to satisfy in the encrypted data.

4. CONCLUSION

In this paper, we have used two algorithms for data sharing and security. The two algorithms are KP-ABE and CP-ABE. In KP-ABE algorithm cannot decide who can encrypt data therefore KP-ABE is in secured algorithm. In CP-ABE algorithm, authorized user can only use the secret key to decrypt the data. So this algorithm is more secured algorithm.

REFERENCES

[1] “A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing “Ruixuan Li, Member, IEEE, Chenglin Shen, Heng He, Zhiyong Xu, and Cheng-Zhong Xu, Member, IEEE

[2] “Towards Se-cure Data Sharing in Cloud Computing Using Attribute Based Proxy Re-Encryption with Keyword Search” Hanshu Hong; Zhixin Sun

[3] X. Liang, Z. Cao, H. Lin, and 1. Shao, "Attribute based proxy re-encryption with delegating capa-bilities," in Proc. 4th ACM Int. Symp.

[4] M. Chase, Multi-authority attribute based encryp-tion," in Proceedings of the Theory of Cryptography Conference, pp. 515{534, 2007}.

[5] M. Chase and S. S. M. Chow, Improving privacy and security in multi-authority attribute based encryption," in Proceedings of the 16th ACM conference on Computer and communications security, pp.121{130, 2009}.

[6] C. C. Chang, I. C. Lin, and C. T. Liao, An accesscontrol system with time-constraint using support vector machines," International Journal of Network Security, vol. 2, no. 2, pp. 150{159,2006}.

[7] L. Cheung and C. Newport, \Provably secure cipher-text policy ABE," in Proceedings of the ACM con-ference on Computer and communications security,pp. 456{465, 2007}.