Data Sharing in Multi-Owner Access Control for Dynamic Groups in the Cloud

Divya N
PG Student, Dept of CSE
Channabasaveshwara Institute Of Technology GUBBI, India

Jyothi K S
Asso Prof, Dept Of CSE
Channabasaveshwara Institute Of Technology GUBBI, India

***Abstract* -- Many organizations large and small use cloud computing. They provide many benefits in terms of improve accessibility, unlimited storage, easy access to information, low cost and efficiently sharing data among cloud user in the groups. Due to the frequent changes of membership make data sharing in multi-owner access control for dynamic groups extremely difficult. Identity privacy and preserving data are the main issues related to data sharing. This paper brings an efficient secure data sharing in multi-owner access control scheme for dynamic groups in the cloud. In a group any cloud user can securely share data with others by providing group signature and dynamic broadcast encryption techniques. As a result the encryption computation cost and storage overhead of our scheme are independent with the number of revoked users.**

Keywords—Cloud Computing, dynamic groups, data sharing, access control.

I. INTRODUCTION

Cloud computing is a term that involves delivering services over the Internet. Now a days the use of cloud computing has increased in many organizations [1] that small and medium companies use cloud computing services for various reasons, including because these services provide fast access to their applications. More organizations outsource - their data storage in large scale to the cloud to save a large amount of money. The members of an organization can share data with other members easily by uploading their data to the cloud with the cloud storage service. With the help of powerful datacenters the cloud service providers, such as Amazon and Google drive will deliver various services to cloud users. To save significant investments on their local infrastructures and by using the local data management systems into cloud servers.

Data storage is one of the services offered by cloud. We shall think about a real time situation. The
department of a college allows its staff members belong to same group to share and store files in cloud. By consuming cloud, staff members can easily upload there data and share the data with others and get free from local data management. However confidentiality and access control is a common risk. User will be unable to trust the cloud service provider or third party because of their identity of users. Designing a secure and efficient data sharing in access control for groups in cloud scheme is a difficult task due to subsequent reasons. Initially identity privacy is one of the biggest problems for cloud users. To join the cloud group users are unwilling without guarantee of identity privacy. Attacker may easily get the real identity and other information like stored data of user. Second, it is highly recommended that the users must fully make use of the services provided by cloud service provider and also support multi-owner data sharing system. When compared with a single-owner system [2] only data owner has full right of entry to the cloud resources like upload a file edit or save, while in multi-owner model, all user gets equivalent preference in the group.

Many privacy techniques for data sharing on untrusted server have been recommended [3],[4],[5]. Here in this system the data owners who upload the data store the encrypted data on untrusted storage. These data owners will the respective decryption keys only to the authorized users unauthorized user have no access to this data. As others will not have the decryption keys they cannot access the data so this prevent the service providers and attacker to access the encrypted data. The new user who has registered has to take authorization from the data owners to right of entry the data in the group previous to generating a decryption key. These schemes are linearly increasing by the complexities of user participation and revocation of user.

In this paper it is focused on data sharing in multi-owner access control for dynamic groups in cloud with limited key management. Main beneficial in this paper is:

- As we recommend that any members of a group can securely store and share data with others in the same group in a multi owner manner.
- In our proposed system it supports dynamic groups, such that without updating the secret key, any user can directly decrypt files uploaded without contacting the data owners and user revocation list is updated each day by Group manager. Once the user has joined the group they

get full access to the stored data or if a user in a group is revoked they cannot use cloud resources at any time. This does not support any key management issues in the group.

- The real identities of group member can be revealed by the group manager that is admin only. Utilizing the cloud resource for any member in a group by providing secure and privacy-preserving access control to users.

II. RELATED WORK

In [3], Wang Q. proposed a scalable secure File Sharing storage system of cryptographic that enables on untrusted servers called by Plutus. Each box file is encrypted with a different key which is divided into no of blocks of small files .Every file group that is divided has a lockbox that stores all file keys belonging to that file group and each file block is encrypted with different keys. Readers and writers get lockbox keys by the owner. However, it brings heavy file sharing key distribution overhead. There will be low cryptographic overhead in file server.

In [4], the contents of files placed on remote server are metadata and file data. The file metadata contains the access control data that encompass collection of encrypted keys. These metadata files are encrypted with public key of authorized users. As the file metadata should be refurbished, the user abrogation in the scheme is an uncompromising issue particularly for large-scale sharing. Nonetheless, the private key should be regenerated for each user for every new user addition into the group. This limits the application to support dynamic groups. Another issue is the encryption load enhances with the sharing scale.

The proxy re-encryption model given by Ateniese et al. [5] strengthens the distributed storage. The data encryption done by the data owners is a two step procedure. First, encryption is done using exclusive and symmetric content keys. Second, the a master public key is used to encrypt the data. Proxy cryptography is used by the server re-encrypt the particular content keys from the public key. Conversely, the remote storage server can be attacked by any malicious user to find the decryption keys of all encrypted blocks.

In [2], S. Yu, C. brings a achieving scalable secure and fine grained data access using Key Policy-Attribute based Encryption method in cloud. The data owner generates many random key to encrypt the file, where the selected random key is again re-encrypted along with KP-ABE by a set of attributes. Decryption keys to the user are provided by group manager to access the data. To complete user revocation, data owner needs to update all attributes and keys. The attributes satisfy the access structure assigned if the cipher text can be decrypted by the user. In the single owner manner may hold back the implementation of applications, where any member in a group should be allowed to store and share data files with others.

In the proposed scheme there are many benefits when compared with the existing system. This features as follows :

a. Any members can store and share data files with others in the group by using cloud.
b. The complexity and size taken for encryption is independent with the number of revoked users in the system
c. New members can easily decrypt the files stored in the cloud and user revocation can be achieved without updating the private keys of the remaining users.

III. SYSTEM MODEL AND DESIGN GOALS

A. System model

Here we believe a cloud system design combining with an example that consist a company allows all its staff members to share and store files with others in a group. The structure model consists of three different entities as illustrated in below Figure, a group manager that is admin (i.e., the company manager), one or more large number of group members (i.e., the staffs) and a cloud. System model is given in Fig.1.

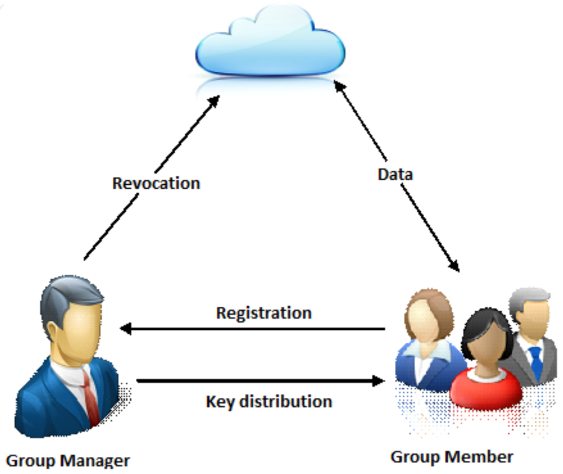

Fig 1: System Model

Cloud is operated by cloud service provider and provides priced abundant storage services. The users can upload their data in the cloud. By developing this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users trusted domain. Similar to [7] we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes [8], but will try to learn the content of the stored data and the identities of cloud users.

Group manager takes charge of followings that is generating system parameters, user revocation, user registration, and revealing the real identity of a dispute data owner. Therefore, we assume that the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager has the logs of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too.

Group members are one or more registered users who are all allowed to store and share their private data in the cloud. Usually the group members are the team members or staffs in the organization. Group membership is dynamically changed due to the staff resignation, newly joining in the organization.

B. Design goals

Designed goals of the proposed system are as follows:

Access control: If the group member has a valid key then they can access the cloud resource where as unregistered user and revoked user cannot access the cloud resources they are strictly prohibited.

Data confidentiality: Unauthorized users are unable to get the content of stored data in the cloud. One of the challenging issues is to maintain confidentiality for dynamic groups. Because new user must be able to decrypt the files while revoked users unable to decrypt stored files.

Efficiency: Efficiency of the proposed system can be explained as follows: Many users can store and share files with other users in the cloud. If a user as been revoked remaining users don't need to update their private keys. User revocation can be performed by group manager.

IV. PROPOSED SCHEME

A. *Techniques used*

To complete data sharing for dynamic groups in the cloud, we look forward to combine the group signature and dynamic broadcast encryption techniques. Specially, the group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users.

In a group signature [9] scheme allows any member of the group can sign messages, the receiver can verify that it is a valid group signature ,but cannot discover which group member made while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs.

Broadcast encryption [8] encrypted data to a set of users so that only a privileged subset of users can decrypt the data. It also allows the group manager to dynamically include new members, user decryption keys need not be recomputed, it support file sharing in dynamic.

Signature generation algorithm inputs user private key, system parameters (P, U, V, H, W) and data M to generate a valid group signature on M.

Signature verification algorithm inputs system parameters (P, U, V, H, M) and a signature generated key to verify and output true or false.

Revocation verification algorithm inputs system parameters (H0, H1, H2) ,a group signature key and a set of revoked keys to get valid or invalid output[6].

B. *Scheme Description*

My proposed system in Fig 2 consists following entities and techniques:

System Setup: System setup can be performed by group manager. Here more users can join with group manager to store and share files. This can be done by making a call to group manager. To provide an approval for data access in cloud user registration process need to be made to which will be evaluated by group manager. Once, user got registered with the cloud system, he is free to access any file until revocation is made on the basis of request. Initially, group manager collects attributes relevant to the data file units and are encrypted, then uploaded to cloud server. Once the user gets a group signature he can access files and download file directly

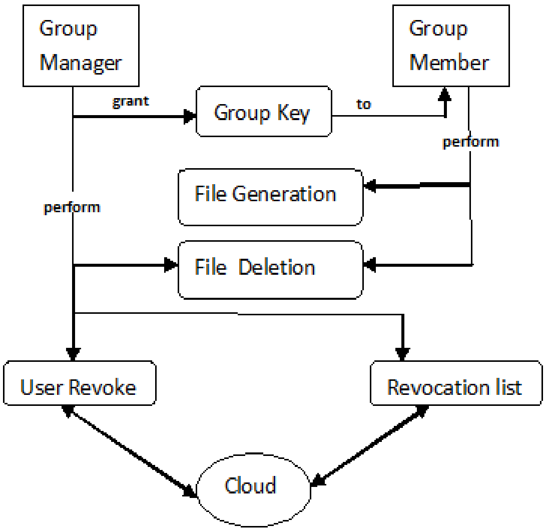

Fig 2: System Architecture.

User Registration: After successful creation of cloud setup, users need to get registered with the system through user registration process. While registering, users need to submit their personal details for completion of registration process. But, the system guarantees Identity privacy. During registration process, user obtains a private key, which will be used for group signature generation and file decryption. Group manager adds user into the group.

User Revocation: User revocation is the process of removal of user from system user list which is performed by Group manager via a public available revocation list (RL). Group manager updates the revocation list each day even no user has being revoked in the day. If user is revoked, so that they can't have access to cloud.

File Generation: To store and share a data file group member performs the following operations:
First getting the revocation list from the cloud. In this, the member sends the group identity IDgroup as a request to the cloud. Then, the cloud responds the revocation list RL to the member. Second verifying the validity of the received revocation list. If the revocation list is invalid, the data owner stops this scheme. Third Encrypting the data file M.
File Deletion: This operation can be performed by either the group manager or the data owner (i.e., the member who uploaded the file into the server).

File Access: To access the data that are stored in the cloud, group member will give request as group id, data id. Cloud server will verify their signature, if the group member in the same group then allow to access file. Group member have rights to access data, but not having rights to delete the data that are stored in the cloud. If any request from revoked user, cloud server won't allow accessing the data.

V. CONCLUSION

In this paper, we design a data sharing in multi-owner access control for dynamic groups in cloud. Without revealing user identity they can store and share the data efficiently in the same group. This model supports efficient user revocation and new user joining. The new users can directly decrypt files stored in the cloud before their participation. Moreover, user revocation can be easily achieved through a public revocation list without updating the private keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users.

REFERENCES

1. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
2. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.
3. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
4. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius:Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.
5. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.
6. Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", ieee transactions on parallel and distributed systems, vol. 24, no. 6, june 2013.
7. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.
8. C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007. D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.