Minimum Replication of User Data Integrating Anti-Collusion Scheme in Cloud Groups

S. Priyanga[1], Ms. N. Devi[2]
[1] *PG Scholar, Department of Information Technology, Sri Venkateswara College of Engineering.*
[2] Assistant Professor, *Department of Information Technology, Sri Venkateswara College of Engineering, Chennai, Tamil Nadu.*

Abstract:

Cloud computing with the characteristics of intrinsic data sharing and low maintenance, provides a better utilization of resources. In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data. However, security concerns become the main constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted data into the cloud. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud. In this proposed system, a secure way for key distribution without any secure communication channels is proposed, and the users can securely obtain their private keys from group manager. It achieves fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. It also protects the scheme from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the untrusted cloud.

Keywords — Privacy preserving, Key distribution, Access control.

I. INTRODUCTION

Cloud Computing is an innovative technology that is revolutionizing the way we do computing.

Data sharing is becoming increasingly important for many users and sometimes a crucial requirement, especially for businesses and organisations aiming to gain profit. However, in recent times, it has been welcomed by a huge number of people as it has become significantly social. Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Cloud computing is defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. This paper proposes a secure data sharing communication between users in the cloud. The basic idea of data security lies on encryption of data as well as delegation of decryption key [iii]. In existence private key distribution is based on the secure communication channel. In this case, which user has private key can share data unfortunately revoked user also can share data. Revoked user means that who have changed their membership. Because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Therefore, secure communication channel is a strong assumption but difficult to use. Cloud storage is not efficiently utilized. Thus, the replica of data is possible in the existing system [viii].

II. SYSTEM DESIGN

A secure architecture for handling file access in a dynamic cloud group is proposed. The user belonging to a particular group can share data in the cloud in a secured manner [v].

The below figure explains the system model for the key distribution from group manager to the group members using cloud storage.

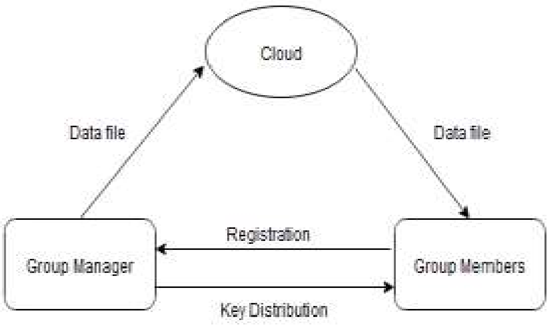

Figure.1 System Model

The user from a particular group requests for the group key to login as a group user. Then the group manager responds to the group user with the group key. With the help of group key the user can login to the group and can able to upload or download the files from the cloud. Once the user revoked from the group, the user cannot able to login to the group with the existing group key. This can avoid the occurrence of collusion in the cloud [iv].

In Proposed system the users can securely obtain their private keys from group manager. User can send request to group manager for access the wanted group, at that time this system provide individual secure key to user without activation. Then group manager see the requests and activate the keys after confirm them. After user's private key gets activation, then only user can access the group.

This scheme has fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. In proposed system the group manager performs the below tasks when a new user joins the group or a user has left the particular group.

1. Update the whole user name list.
2. Generate a secure key and encrypt the key without activation and send to the updated user list.
3. Update the rights in the cloud server.

Group manager takes charge of system parameters generation, user registration, and user revocation. In the practical applications, the group manager usually is the leader of the group. Therefore, we assume that the group manager is fully trusted by the other parties. Group members (users) are a set of registered users that will store their own data into the cloud and share them with others. In the scheme, the group membership is dynamically changed, due to the new user registration and user revocation.

The user leaving a group is termed as revoked users [iv]. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud. Thus this proposed system detects the revoked users and protects the data confidentiality and privacy. Secure data sharing is performed using private keys generated and transmitted using secure communication channels [vi]. In this scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels using attribute based encryption algorithm.

The group user can upload the files in real cloud server. To get a file, the user needs to send a request to the cloud server. The cloud server will also check the user’s identity before issuing the corresponding file to the user. During file access the user key has to match by the group manager and the requested file can be downloaded by the group users.

The user request for the group key to the group manager, then the group manager authenticates the authorized user and responds with the group key. Then the user can login to the group using the secured key provided by the group manager.

The group key can be used only the user in the particular group (Group A or Group B or Group C). A legal user can access its own data fields. The group user can download the file from the particular group in the cloud using the secret key.

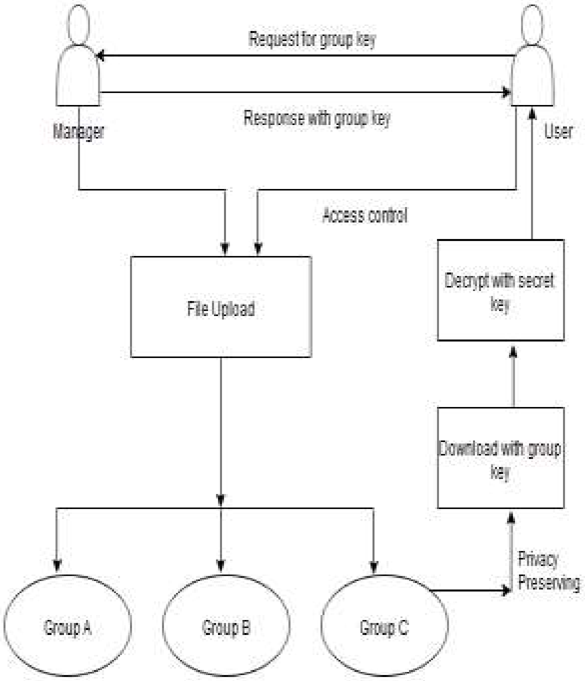

Figure.2 Anti-collusion

The group key can be used only the user in the particular group (Group A or Group B or Group C). A legal user can access its own data fields. The group user can download the file from the particular group in the cloud using the secret key.

The downloaded file will be in an encrypted format using attribute based encryption algorithm, thus the user can decrypt the file using the secret key. Thus in this system the revoked users cannot able to access the data using the key and thus provides anti-collusion in data sharing [v].

III. DESIGN AND IMPLEMENTATION

A. Authority User Verification and Privacy-Preserving

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized user's information on a local operating system or within an authentication server.

User Verification

At first Initial stage all users must create own username and password. After the Registration the user can login to their own space. This application verify the username and password which is either matched or not with the user registration form which is already created by the user while user registration process. If the valid user did not remember the username or password correctly the user can generate own password by using this application.

Privacy-Preserving

In the Privacy preservation environments, a reasonable security protocol would be developed to achieve the following requirements.

Authentication: A legal user can access its own data fields, only the authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user.

Data anonymity: Any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel.

User privacy: Any irrelevant entity cannot know or guess a user's access desire, which represents a user's interest in another user's authorized data fields. If and only if the both users have mutual interests in each other's authorized data fields, the cloud server will inform the two users to realize the access permission sharing.

Forward security: Any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages.

B. Key Distribution and Access Control

Key distribution is done by the group manager for the particular user in the group. This can avoid the collusion occurrence in the cloud between the users in the same group [iii].

Key Distribution

Group manager takes charge of system parameters generation, user registration, and user revocation. In the practical applications, the group manager usually is the leader of the group. Therefore, we assume that the group manager is fully trusted by the other parties [iii].

Group members (users) are a set of registered users that will store their own data into the cloud and share them with others. In the scheme, the group membership is dynamically changed, due to the new user registration and user revocation.

Revoked users cannot access data after they have been revoked [iv]. The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information. The protocol supports multiple read and writes on the data stored in the cloud. The costs are comparable to the existing centralized approaches and the expensive operations are mostly done by the cloud.

Attribute-Based Encryption

Attribute-based encryption (ABE) is a public-key based one to many encryptions that allows users to encrypt and decrypt data based on user attributes [ii]. In which the secret key of a user and the cipher text are dependent upon attributes. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. Decryption is only possible when the number of matching is at least a threshold value.

Collusion-resistance is crucial security feature of Attribute-Based Encryption [ii]. An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. The application of this scheme is restricted in the real environment because it uses the access of monotonic attributes to control user's access in the system.

1. The user sends IDi, pk, v1 as a request to the group manager, where IDi is the identity of the user, pk is the public key used in the asymmetric encryption algorithm.

2. On receiving the request, the group manager then chooses a random number r.

3. The group manager compares the received IDi message with the identity IDi computed by decrypting AENCsk (IDi, v1, ac).

4. The group manager then sends the encrypted message AENCpk (KEY, v2) to user and stores (xi,Ai,Vi, IDi) in the local storage space.

5. Finally, the user decrypts the message AENCpk (KEY, v2) by his private key in ECC and then he can obtain his private key (xi, Ai, Bi). After successful registration, the user becomes a group member.

Collusion Attack

The user leaving a group is termed as revoked users. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud [iv]. Thus this proposed system detects the revoked users and protects the data confidentiality and privacy.

C. Secure Data Sharing and Cloud Storage

Secure data sharing is performed using private keys generated and transmitted using secure communication channels [viii]. In this scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels using attribute based encryption algorithm [ii]. The following are the requirements of secure data sharing in the cloud.

Data Confidentiality:

Unauthorized users (including the Cloud), should not be able to access data at any given time. Data should remain confidential in transit, at restand on backup media. Only authorized users should be able to gain access to data.

User revocation:

When a user is revoked access rights to data, that user should not be able to gain access to the data at any given time [iv]. Ideally, user revocation should not affect other authorized users in the group for efficiency purposes.

Scalable and Efficient:

Since the number of Cloud users tends to be extremely large and at times unpredictable as users join and leave, it is imperative that the system maintain efficiency as well as be scalability.

Collusion between entities:

When considering data sharing methodologies in the Cloud, it is vital that even when certain entities collude, they should still not be able to access any of the data without the data owner's permission.

IV. CONCLUSION AND FUTURE ENHANCEMENT

The proposed scheme provides a possible way to fight against immoral interference with the right of privacy. A secure data sharing scheme is proposed for dynamic users. Key distribution done without any secure communication channels and the user can get the individual key from group manager.

Data Deduplication is one of the techniques that can be further implemented which is used to solve the repetition of data. The deduplication techniques are generally used in the cloud server for reducing the space of the server. To prevent the unauthorized use of data accessing and create duplicate data on cloud the encryption technique to encrypt the data before stored on cloud server.

REFERENCES

[i]. Wenhao Li, Yun Yang, and Dong Yuan (2015), "Ensuring Cloud Data Reliability with Minimum Replication by Proactive Replica Checking", IEEE Transactions on Computers, Volume: 65, Issue: 5.

[ii]. Shulan Wang, Joseph K. Liu, and Kaitai Liang (2016), "Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", IEEE Transactions on Information Forensics and Security, Volume: 11,Issue: 8.

[iii]. Baojiang Cui, Lingyu Wang, and Zheli Liu (2015), "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage", IEEE Transactions on Computers, Volume: 65, Issue: 8.

[iv]. Tao Jiang, Jianfeng Ma, and Xiaofeng Chen (2015), "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation", IEEE Transactions on Computers, Volume: 65, Issue: 8.

[v]. Mazhar Ali, Eraj Khan, and Revathi Dhamotharan (2015), "SeDaSC: Secure Data Sharing in Clouds", IEEE Systems Journal, Volume: PP, Issue: 99.

[vi]. Xuefeng Liu, Boyang Wang, and Yuqing Zhang (2013), "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Transactions on Parallel and Distributed Systems, Volume: 24, Issue: 6.

[vii]. Dongliang Lei, Hao Jin, and Ke Zhou (2014), "SFDS: A Security and Flexible Data Sharing Scheme

in Cloud Environment", 2014 International Conference on Cloud Computing and Big Data (CCBD).

[viii]. Deepa Maria Polson, M. S. Rajasree and S Sabitha (2016), "Fine grained key computation scheme for secure data sharing in cloud", International Conference on Advances in Computing, Communications and Informatics (ICACCI).

[ix]. Xu An Wang, ZhihengZheng, and FatosXhafa (2016), "Identity Based Proxy Re-Encryption Scheme (IBPRE+) for Secure Cloud Data Sharing", International Conference on Intelligent Networking and Collaborative Systems (INCoS).