An Efficient Data Sharing Technique in the Cloud: An EDST

Rachapalli Devendra Reddy
Asst. Professor, Department of CSE
Srikalahasteeswara Institute of Technology (SKIT)
Srikalahasti, Chittoor (DT), Andhra Pradesh, India
e-mail : csdreddy@gmail.com

P Ravi Kiran
Asst. Professor, Department of CSE
Srikalahasteeswara Institute of Technology (SKIT)
Srikalahasti, Chittoor (DT), Andhra Pradesh, India
e-mail : camravikiran@gmail.com

Abstract: Mainly large amount of data can be stored at cloud and it is offered by cloud providers. Cloud computing is use full platform for data sharing among clod members .Because with this scheme we can share large amount of data with less cost. And also it is efficient technique for sharing data among cloud members with less maintenance. For sharing dynamic data by different members from cloud it is necessary to register before they want to view shared data. It is problematic to maintain data security and user privacy in this traditional strategy. In our proposed system an efficient data sharing is provided by using two keys called Group Manager Key and Cloud Key for the cloud members.

*****

I. INTRODUCTION

Cloud computing is a competitive alternative to general distributed data sharing Scheme [1]. Cloud computing is less cost, efficient and less maintenance overhead. , In it the cloud service providers (CSPs), such as Amazon, providing data for customers by recognizing as powerful datacenters. Comparing with the local data management systems with clod computing, users can enjoy high-quality services. For example, An organization allows its employees in the same cluster or department to store and share files in the cloud. By utilizing the cloud, the employees can be freed from the troubles of local data storage and maintenance. But, it may has a considerable risk to the Privacy of those stored files. Specifically, the cloud servers managed by cloud providers are may not fully trusted by users while the data stored in the cloud may be confidential, such as companies business plans and personal to them. To maintain data privacy, it is to encrypt data files, and then upload data into the cloud [2]. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues:

1. The guarantee of identity privacy, For example, a misbehaved employee can misguide others in the organization by sharing wrong data without being traceable. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable.

2. It is necessary, that any member in a group could be able to enjoy the data storing and sharing services provided by the cloud providers, More concretely, each user in the group is able to read others data, and he can modify his/her part of data in the entire data shared by the organization. Compared with single owner system [3], multi owner secure system is more efficient.

3. Groups are normally dynamic in practice, e.g., new employee joining and current employee revocation in a organization. The changes of membership made secure data sharing very difficult.

Several security techniques for data sharing on not trusted servers have been proposed[4],[5],[6] .In these approaches, data owners store the encrypted data files in not trusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. The protection of computer based resources that include hardware, software, data, functions and people against misuse or natural affects such as System Security. System Security can be divided into four related issues: Security, Integrity, Privacy & Confidentiality.

II. SYSTEM DESIGN

In designing a solution for the problem, it is a process of identifying inputs, outputs and explains functions of the system in terms of sample test cases. System design is the high level strategy for solving the problem and building a solution. System design includes decision about the organization of system into subsystems, the allocation of subsystems to hardware and software components, and major conceptual that form the framework for detailed design.

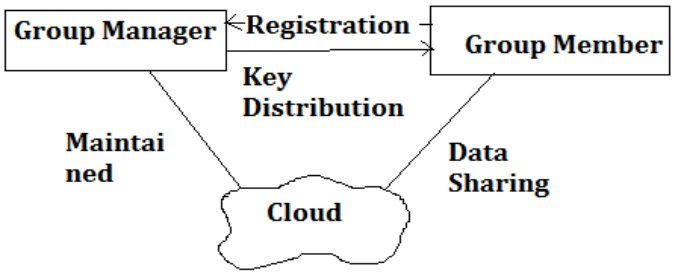

Figure 1: System Architecture

A. *Design Goals*

Design goals of the proposed system include user access control, shared data confidentiality, traceability, and efficiency as follows:

User access control: The requirement of access control is twofold. First, group members are able to use the cloud for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked.

Shared data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable of Traceability: Anonymity guarantees that group members can access the cloud without revealing the his/her real identity. For example, an inside attacker may store and share a mendacious information to derive substantial benefit. Thus, to tackle the inside attack, the group manager should have

the ability to reveal the real identities of data owners.

Efficiency: The efficiency is defined as follows: Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users. That is, the remaining users do not need to update their private keys or re-encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

III. PROPOSED SCHEMA: EDST

A. *Overview*

To solve the challenges presented above, we propose a dynamic data sharing technique for dynamic group members in the cloud. The main contributions of EDST include: We propose an efficient data sharing technique. It implies that any member in the group can securely share data with others by the not trustable cloud. Our proposed system is able to support dynamic groups efficiently. Specifically, new permitted members can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. We provide secure and privacy-preserving user access control to members, which guarantees any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.

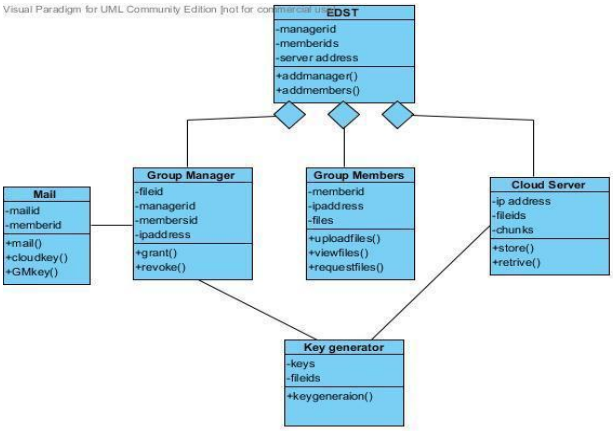

Figure 2: Class diagram

B. *Schema Description*

The EDST in cloud has been divided into four modules:

- *Group member:* Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. In our example, the staffs play the role of group members. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company.
- *Group manager:* Group manager takes charge of system parameters generation, user registration, and user revocation, and revealing the real identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company. Therefore, we assume that the group manager is fully trusted by the other parties.
- *Cloud server:* Cloud is operated by CSPs and provides priced abundant storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users trusted domain. 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, but will try to learn the content of the stored data and the identities of cloud users.
- *Key generator:* Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users. That is, the remaining users do not need to update their private keys or re-encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

IV. TEST RESULTS

Figure 3: Signing in as a registered member

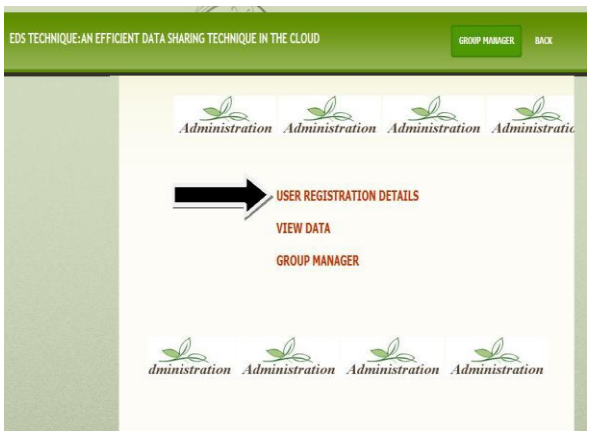

Figure 4: Fields for group manager

ISSN: 2321-8169
1718 – 1720

Figure 5: Data uploading file in a cloud server

Figure 6: User view data

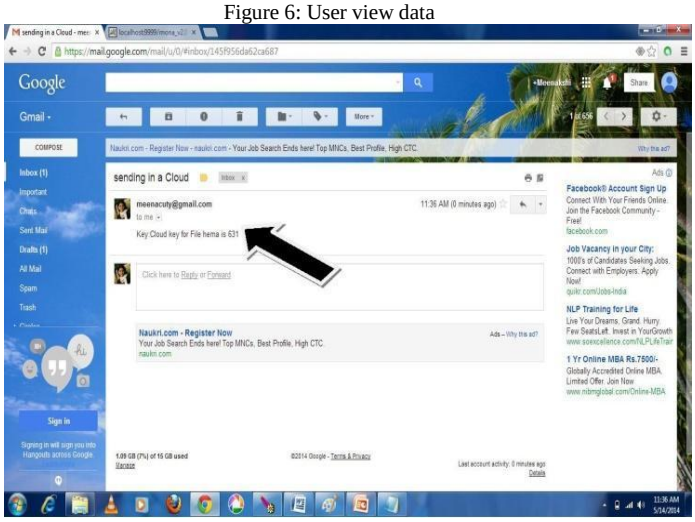

Figure 7: Cloud key sent to mail

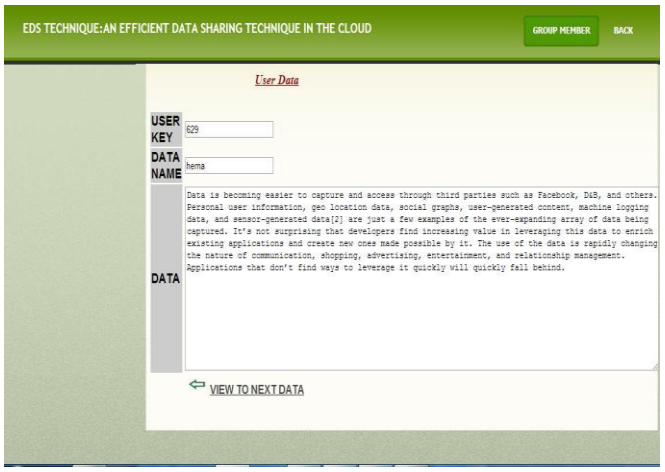

Figure 8: Viewing the desired file

V. CONCLUSION

In this paper, we proposed an efficient data sharing technique, for dynamic groups in an untrusted cloud. In an EDST, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, An EDST supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new members can directly decrypt data files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

VI. FUTURE ENHANCEMENTS

As future work, we would like to extend the type of data being uploaded in the cloud server. In our project we have tested only text document data, which can be further extended to audio and video.

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.

[2] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc.Int’l Conf. Financial Cryptography and Data Security (FC).

[3] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing,”Proc. IEEE INFOCOM.

[4] 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.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, “Sirius:Securing Remote Untrusted Storage,” Proc. Network and DistributedSystems Security Symp. (NDSS)

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “ImprovedProxy Re-Encryption Schemes with Applications to Secure distributed Storage,” Proc. Network and Distributed Systems Security Symp.(NDSS).