Secure Multi-Owner Data Sharing for Dynamic Groups in Cloud

D. Arifa Khanam
Dept of CSE
Besant Theosophical College

P. Veeramuthu
Assistant Professor
Dept of CSE
Besant Theosophical College

Abstract:- **Cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose a secure multi owner data sharing scheme, named secured data sharing for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.**

INTRODUCTION

1.1INTRODUCTION TO SECURE DATA SHARING IN DYNAMIC GROUPS IN CLOUD:

Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. One of the most fundamental services offered by cloud providers is data storage. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. 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:

- Identity privacy
- Single Owner
- Dynamic nature of Groups

To overcome the above described challenges we propose the scheme
That includes the following:

- Secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud. ∑ Support dynamic groups efficiently. Specifically, new granted users 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 user
- Provide secure and privacy-preserving access control to users, 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.

OBJECTIVE

The main objective of the implemented application is given by:
This paper presents a Secure Multi owner data sharing scheme, Named Mona, For dynamic groups in the cloud. By leveraging group Signature and dynamic broadcast Encryption techniques, any cloud user can anonymously share data with others. It implies that any user in the group can securely share data with others by the un trusted cloud. This scheme is able to support dynamic groups .
New granted users 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.

1.3EXISTING SYSTEM

To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task.
In the existing System data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well.
l as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively.

DISADVANTAGES OF EXISTING SYSTEM:

- In the existing Systems, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily

disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable.

- Only the group manager can store and modify data in the cloud.
- The changes of membership make secure data sharing extremely difficult the issue of user revocation is not addressed.

PROPOSED SYSTEM

A secure multi-owner data sharing scheme is provided. It implies that any user in the group can securely share data with others by the un trusted cloud. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users 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. A secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource, is provided. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur. A rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

ADVANTAGES OF PROPOSED SYSTEM:

- Any user in the group can store and sharedata files with others by the cloud.
- The encryption complexity and size of cipher texts are independent with the number of revoked users in the system.
- User revocation can be achieved without updating the private keys of the remaining user.
- A new user can directly decrypt the files stored in the cloud before his participation.

PROJECT OVERVIEW

Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. Annotation strategies that use attribute-value pairs are generally more expressive, as they can contain more in-formation than un-typed approaches.

A recent line of work towards using more expressive queries that leverage such annotations, is the “pay- as-you-go” querying strategy in Data-spaces: In Data-spaces, users provide data integration hints at query time. The assumption in such systems is that the data sources already contain structured information and the problem is to match the query attributes with the source attributes. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application.

A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. 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.

CLOUD MODULE

In this module, we create a local Cloud is created which is payee for only used space in storage services. The users can upload their data files in cloud. I develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are beyond the users knowledge. Similarly it is assumed that the cloud server to be honest. The service providers will not delete or modify user data because of the protection data schemes, but will try to read and know the content of the stored data and the identities of cloud users.

GROUP MANAGER MODULE

Group manager is responsible for providing the user’s with,

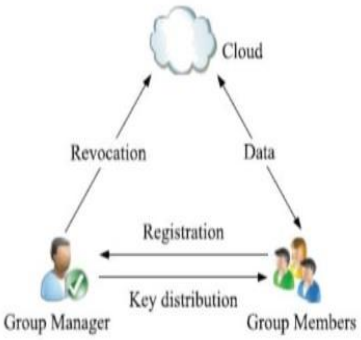
- System parameters generation,
- User registration,
- User revocation, and
- Revealing the real identity of a dispute data owner. Therefore, the group manager is assumed to be trust worthy by the user’s. The Group manager is also known as an admin.

  The group manager has the logs of each and every functions done by user’s in cloud. The group manager accepts user registration and also he will do user revocation.

GROUP MEMBER MODULE

Group members are registered users in cloud they will store their private data into the cloud server and share them with others in the group. Therefore, the group members can store their files as members are dynamically changed, due to the user resignation and new user registration in the company. The group member has the ownership of changing the files in the group. Anyone in the group can view the files which are uploaded in their group and also modify it.

SYSTEM DESIGNING



SOFTWARE DESIGN

The below data flow diagram shows that under the cloud module, there are two modules Group Manager Module .Group member module Both can login using their login details. After successful login, Group Manager activates newly added members of the cloud. He can also check the group details, file details of the cloud and he can also delete the files.After successful login, Group Member's signature is verified. After successful verification, the member can upload, download and can modify the files.The Group Member's account can be revoked after he leaves the cloud by the Group Manager.If the login fails, due to the wrong login details, both in Group Member and Group Manager Modules, an error is generated. Because of which neither Manager nor Member can login.During group signature verification in the Group Member module, if the verified result turns out to be false, it is treated as an error and the Member has no access over the group.

CONCLUSION

In this research paper, I designed a scheme for dynamic groups to share their data with others securely in an untrusted cloud. A registered user is able to share data with others in the group by preserving his identity privacy in the cloud. It is to be understood that this scheme invariably supports efficient user revocation and new user joining. To be more clear and specific, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users and new users can directly decrypt files stored in the cloud before their actual involvement. However, it is established that the storage overhead and the encryption computation costs are constant. Elaborate study and analysis show that proposed scheme is upto the setter security requirements and assures total efficiency in the fullest perspective.

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. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[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, pp. 534-542, 2010 . [4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and

[4] K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc.