“MONA: SECURE MULTI OWNER DATA SHARING FOR THE DYNAMIC GROUPS IN THE CLOUD”

PROJECT REFERENCE NO. : 37S1225

COLLEGE  : SHRI TARALABALU JAGADGURU INSTITUTE OF TECHNOLOGY, RANEBENNUR
BRANCH   : COMPUTER SCIENCE AND ENGINEERING
GUIDE    : MANJULA P
STUDENTS : SHILPA A HADIMANI
          : SHRIDEVI S PATIL
          : SHEETHAL D S
          : SHRUTI V A

Keywords: Cloud computing, data sharing, privacy-preserving, access control, dynamic groups.

Introduction:

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

In several security schemes such as Plutus, Sirius, etc proposed for data sharing on untrusted servers, the 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 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. By setting a group with a single attribute, Lu et al. proposed a secure provenance scheme based on the ciphertext-policy attribute-based encryption technique, which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme. The single owner manner hinders the adoption of key policy attribute-based encryption and other schemes.

To overcome the above described challenges we propose the scheme- MONA

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 users.
- 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:**

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. Here, we propose a secure multiowner 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. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. Our project has the following features:

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

**Methodology:**

The software methodology in our project is the agile methodology. It combines incremental method and iterative method.

Here, first the initial system is developed and released to the market. If there are any development to be made to existing system or extra features has to be added then it is carried in the next development phase, which is again released to market, feedback is taken and the process iterates.

**System Model:**

The below diagram gives the overall system architecture of our project. It shows the working of our project where the users are registered for the usage of the cloud by group manager. The data can be uploaded in multi owner manner. The group member’s account is revoked by group manager once the member leaves the group.
Data flow diagram:

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.
Use case Diagram:

Here actors are the Group Managers and the Group Members. The system is the cloud. The following use case diagram shows the interaction between actors and the system.

Some of the interactions are Registration, Group login and signature verification, Maintenance of Group Accounts and Group Modification.

Class Diagram:

Class diagram express the class model. Classes define the attribute values carried by each object and the operations that each object performs or undergoes.
The classes here are Group Member, Group Manager and Cloud. These classes along with their attributes and operations are illustrated below.

**Implementation:**

**Modules:**

1. **Cloud Module:**

In this module, we create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud. We develop 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 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.

2. Group Manager Module:

Group manager takes charge of followings,

1. System parameters generation,
2. User registration,
3. User revocation, and
4. 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.

3. Group Member Module:

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.

Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Whoever in the group can view the files which are uploaded in their group and also modify it.

4. File Security Module:

- Encrypting the data file.
- File stored in the cloud can be deleted by either the group manager or the data owner(i.e., the member who uploaded the file into the server).

5. Group Signature Module:

A group signature scheme allows any member of the group to sign messages 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, which is denoted as traceability.
6. User Revocation Module:

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

Conclusion:

In our project, we design a secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud by combining group signature with the dynamic broadcast encryption techniques. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona 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 users can directly decrypt 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.

Future Enhancement:

Our project has been developed in a very short period of time and all the efforts have been taken so that this project is very efficient in its execution. Although, there still exists scope for the improvement of our project in the future.

Our project has been developed mainly by taking the example of the environment of the company. We can extend our project to the fields such as education, entertainment, various social networks and other wider areas. For example, we can employ our project in the universities to maintain the data base of the students which can be used by the groups of lecturers. Here lecturer becomes the group member and the head of the department becomes the group manager.

Further enhancement in the security of the data uploaded by the members can be done. We can also concentrate on creating sub groups in the groups.

We can concentrate on preserving identity privacy for its enhancement. Interaction between the group manager and the group member should be improved.