IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURE DATA SHARING WITH IN GROUPS IN THE CLOUD

Gouthami Velakanti*, Niranjan Reddy .P, Sravanthi Venishetty
* Department of Computer Science and Engineering, Aurora's Research and Technological Institute,Warangal,India-506002

DOI: 10.5281/zenodo.59675

ABSTRACT

Cloud computing refers to the delivery of computing resources over the Internet. Cloud provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. It provides high level of scalability, reliability and efficiency. In this paper we propose a secure data sharing scheme within the groups and how encryption techniques help the groups in sharing the data dynamically. Sharing of data between dynamic groups the storage overhead and encryption computation cost changes based on revoked users. So to avoid, this we are providing three level of security mechanism for individual members in a group with the help of encryption techniques to share data. In this technique data can be uploaded in to the server after the encryption of the content by the secret group key. When a new member is added to the group, this user can be granted access to the file wherein he can directly download the decrypted data file, without contacting the data owners but when they are downloading the file a secret key is generated and sent to their own mobile number, using that key user can download the data. Due to this mechanism data in the cloud is secured.

KEYWORDS: Cloud,User revocation, Signature Generation, Signature Verification, Revocation Verification, encryption.

INTRODUCTION

Cloud computing represents a different way to architect and remotely manage computing resources, It is a style of computing in which dynamically scalable and often virtualization resources are provided as a service over the internet. In cloud computing the cloud service providers such as Amazon, are able to provide various services to cloud users with the help of powerful data centers. By migrating the local management systems into cloud servers, users can enjoy high quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage.

Let us consider a practical data application. In any Organization group of users or staff of same department or different department will store and share files in the cloud. However; it also poses a significant risk to the confidentiality of those stored 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 using encryption techniques, 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.

Providing the trusted environment in cloud computing to users or staff because 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 Therefore traceability, which enables the group manager to reveal the real identity of a user, is also highly desirable.

In this mechanism instead of single owner for data multi owner scheme is established Single owner does mean that a file is owned by only one person who is known as data owner. The data owner has rights to access data. In this we explored the multi owner environment in the presence of dynamic groups. We considered a company with employees working on various projects. The related employees are grouped together so as to manage easily. Each group has a group manager. All the group members of a group have rights to access a common file. In other words they have rights to shared data as far as they belong to that group. Members may be revoked by group manager from the corresponding group when employee leaves organization or moves to different project within the group. Individual group is provided with unique secret key by group manager, the encrypted file is uploaded into cloud by group manager with the help of secret key they can decrypt file from the cloud using decryption keys .

The changes of membership make secure data sharing extremely difficult. On one hand, the anonymous system challenges new granted users to learn the content of data files stored before their participation because it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management several security schemes for data sharing on untrusted servers have been proposed in these approaches 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.
To solve the challenges presented above, we propose SDDC, a secure multi-owner data sharing scheme for dynamic groups in the cloud.

The main contributions of this paper include:

1. We propose a secure data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud.

2. 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.

3. We 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.

4. We provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

5. We provide multi level Security i.e. three level of security mechanism in order to decrease the revocation rate in cloud and provide more security to data, so here individual group member is provided with login credentials and decryption key to download a file from cloud.

6. If a new member is added to the group, this user can be granted access to the file wherein he can directly download the decrypted data file, without contacting the data owners but when they are downloading the file a secret key is generated and sent to their own mobile number, using that key user can download the data.

7.The same process is followed for existing member if they are feeling insecurity of data in cloud they can also generate their own secret key which acts as a OTP,every time they can regenerate the new key for downloading the file from cloud due to this crooked user cannot access the file from cloud if knows the login credentials and group secret key of the member.

RELATED WORK

In [1], the authors specified a secure data sharing model, Mona, for dynamic groups in a remote storage. In Mona, a data owner can share data with others in the group without announcing their identity.Moreover, Mona supports effective user repudiation and new user registration. More specially, efficient user repudiation can be attained by a public revocation list without ideating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their presence Kallahallaetal. proposed [2] a cryptographic storage system that enables secure file sharing on untrusted servers, named Plutus. By dividing files into file groups and encrypting each file group with a unique file-block key, the data owner can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key issued to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing.

The user revocation in the scheme is an intractable issue especially for large-scale sharing, since the file metadata needs to be updated. In their extension version, the NNL construction is used for efficient key revocation. However, when a new user joins the group, the private key of each user in an NNL system needs to be recomputed, which may limit the application for dynamic groups. Another concern is that the computation overhead of encryption linearly increases with the sharing scale.

Atenie se etal [3] leveraged proxy re encryptions to secure distributed storage. Specifically, the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key. For access control, the server uses proxy cryptography to directly re encrypt the appropriate content key(s) from the master public key to a granted user's public key. Unfortunately, a collusion attack between the untrusted server and any revoked malicious user can be launched, which enables them to learn the decryption keys of all the encrypted blocks.

Yu et al.[4] presented a scalable and fine-grained data access control scheme in cloud computing based on the KPABE technique. The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Then, the group manager assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a cipher text if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegate's tasks of data file re encryption and user secret key update to cloud servers. However, the single owner manner may hinder the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others.

EXISTING 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 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

1. We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud.
2. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users

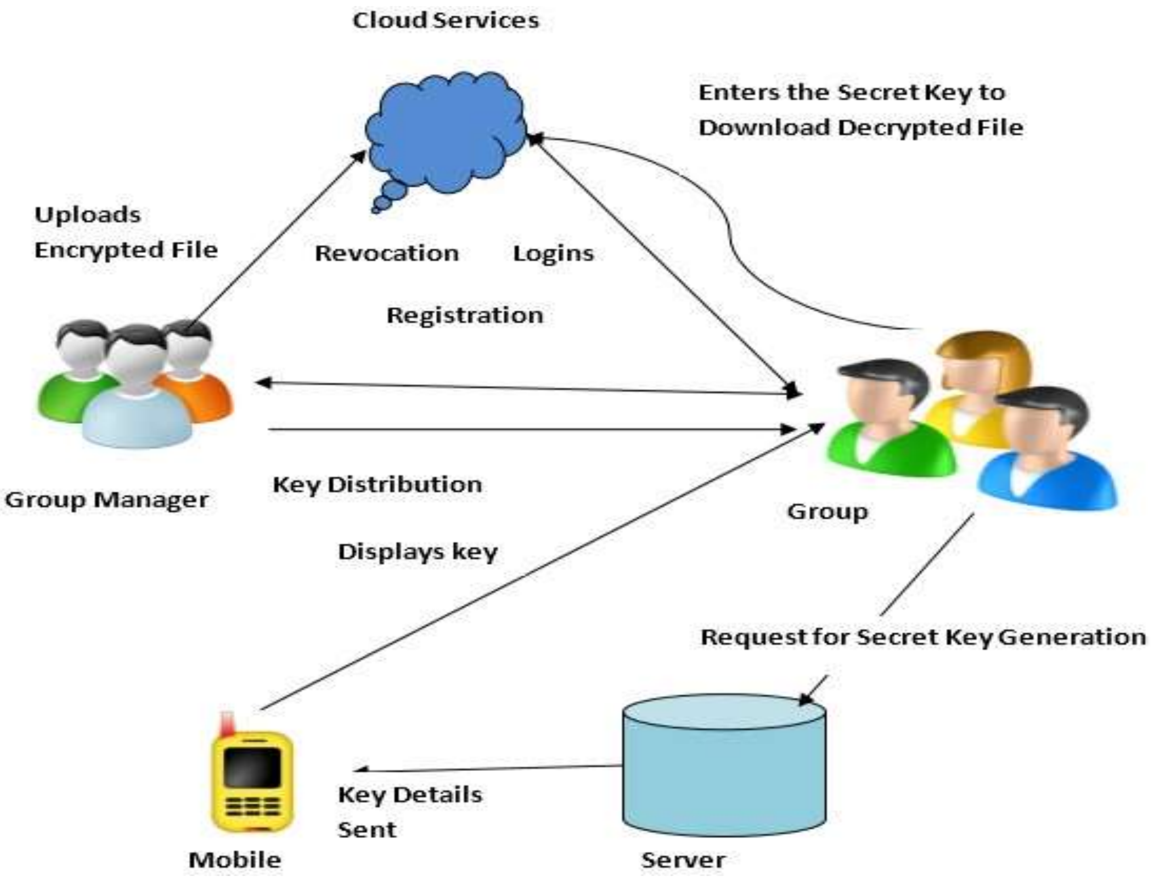
can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users.

3. We 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.
4. We provide 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

1. Any user in the group can store and share data files with others by the cloud.
2. The encryption complexity and size of cipher texts are independent with the number of revoked users in the system.
3. User revocation can be achieved without updating the private keys of the remaining users.
4. A new user can directly decrypt the files stored in the cloud before his participation.
5. Third level of security mechanism included for existing and new user as follows, when user logins with the help of their login credentials ,their next step is download a file from the cloud by using the group secret key.
6. Instead of using group secret key individual secret key is generated and sent to their mobile with the help of this key user can download the file from the cloud this process repeats every time when user login due to this ,security level is increased and also avoids unauthorized user to access the group file.

SYSTEMARCHITECTURE

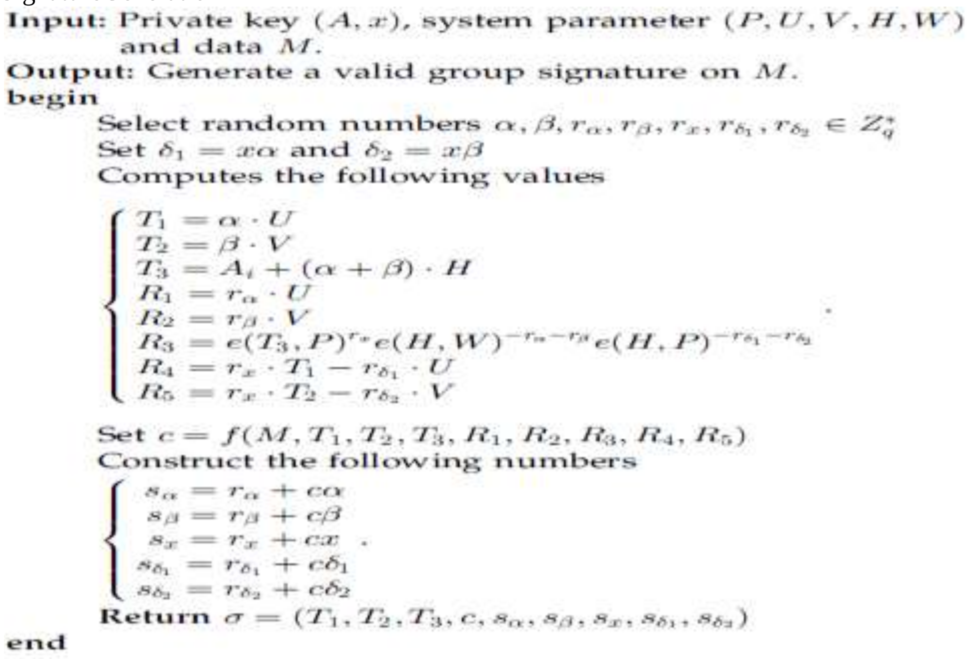


Algorithms Used

- ✓ Signature Generation
- ✓ Signature Verification
- ✓ Revocation Verification

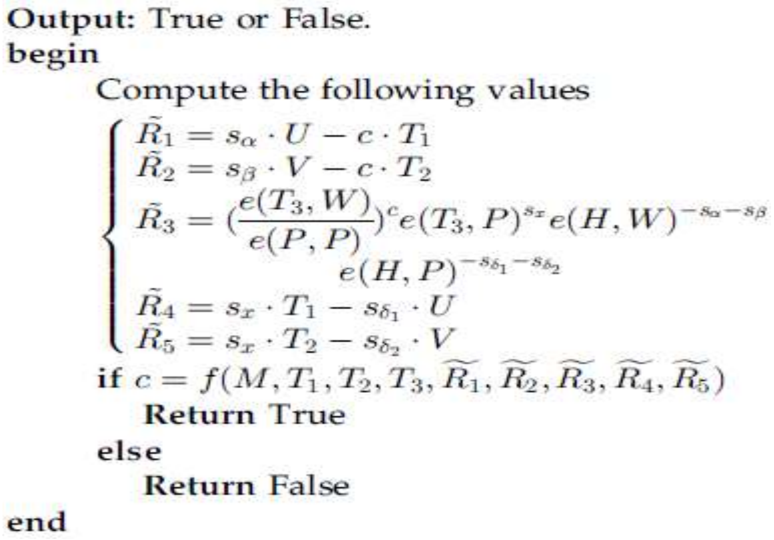
Algorithms Description

- ✓ SignatureGeneration



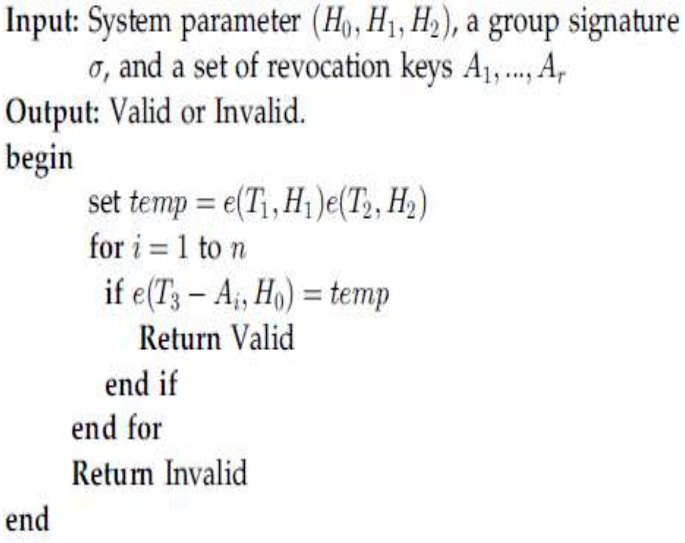
```
Input: Private key $(A, x)$, system parameter $(P, U, V, H, W)$
       and data $M$.
Output: Generate a valid group signature on $M$.
begin
    Select random numbers $\alpha, \beta, r_\alpha, r_\beta, r_x, r_{\delta_1}, r_{\delta_2} \in Z_q^*$
    Set $\delta_1 = x\alpha$ and $\delta_2 = x\beta$
    Computes the following values
        $T_1 = \alpha \cdot U$
        $T_2 = \beta \cdot V$
        $T_3 = A_i + (\alpha + \beta) \cdot H$
        $R_1 = r_\alpha \cdot U$
        $R_2 = r_\beta \cdot V$
        $R_3 = e(T_3, P)^{r_x} e(H, W)^{-r_\alpha - r_\beta} e(H, P)^{-r_{\delta_1} - r_{\delta_2}}$
        $R_4 = r_x \cdot T_1 - r_{\delta_1} \cdot U$
        $R_5 = r_x \cdot T_2 - r_{\delta_2} \cdot V$
    Set $c = f(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$
    Construct the following numbers
        $s_\alpha = r_\alpha + c\alpha$
        $s_\beta = r_\beta + c\beta$
        $s_x = r_x + cx$
        $s_{\delta_1} = r_{\delta_1} + c\delta_1$
        $s_{\delta_2} = r_{\delta_2} + c\delta_2$
    Return $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$
end
```

- ✓ **Signature Verification**



```
Output: True or False.
begin
    Compute the following values
        $\tilde{R}_1 = s_\alpha \cdot U - c \cdot T_1$
        $\tilde{R}_2 = s_\beta \cdot V - c \cdot T_2$
        $\tilde{R}_3 = (\frac{e(T_3, W)}{e(P, P)})^c e(T_3, P)^{s_x} e(H, W)^{-s_\alpha - s_\beta}$
                      $e(H, P)^{-s_{\delta_1} - s_{\delta_2}}$
        $\tilde{R}_4 = s_x \cdot T_1 - s_{\delta_1} \cdot U$
        $\tilde{R}_5 = s_x \cdot T_2 - s_{\delta_2} \cdot V$
    if $c = f(M, T_1, T_2, T_3, \widetilde{R_1}, \widetilde{R_2}, \widetilde{R_3}, \widetilde{R_4}, \widetilde{R_5})$
        Return True
    else
        Return False
end
```

- ✓ **Revocation Verification**



```
Input: System parameter $(H_0, H_1, H_2)$, a group signature
    $\sigma$, and a set of revocation keys $A_1, ..., A_r$
Output: Valid or Invalid.
begin
    set $temp = e(T_1, H_1)e(T_2, H_2)$
    for $i = 1$ to $n$
      if $e(T_3 - A_i, H_0) = temp$
        Return Valid
      end if
    end for
    Return Invalid
end
```

SYSTEM MODEL AND DESIGN GOALS

System Model

We are proposing the architecture with multiple owners and users. The owners of a single data/file may belong to an organization or institution. Here the data may have multiple owners, the owners register into system as a group but having individual access keys and passwords. Anyone in the group can store and share the data. The system model consists of three different entities: the cloud, a group manager (i.e., the company manager), and a large number of group members (i.e., the staffs) as illustrated in Fig. 1.Cloud is operated by Cloud Service Provider 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 curios. Group manager takes charge of system parameters generation, user registration, 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. 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. One more security mechanism included for existing and new user as follows, when user logins with the help of their login credentials, their next step is downloading a file from the cloud by using the group secret key. Instead of using group secret key individual secret key is generated and sent to their mobile with the help of this key user can download the file from the cloud this process repeats every time when user login due to this ,security level is increased and also avoids unauthorized user to access the group file.

Design Goals

Design goals of the proposed scheme including access control, data confidentiality, anonymity and traceability, Access Key Generation, and efficiency as follows:

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

Data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, new users should decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud after the revocation.

Anonymity and traceability: Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system. 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.

Access Key Generation: Two Types of keys are generated one is group key and other secret key by member, group key is a unique key shared among users in a group, inorder to download a file from cloud individual secret key is generated by user by requesting key details to server and server sends the key info to their personal mobile with the help of this user can download the file from cloud.

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 reencryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

THE PROPOSED SCHEME

To achieve secure data sharing for dynamic groups in the cloud, we expect 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. Unfortunately, each user has to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme, which results in that both the computation overhead of the encryption and the size of the cipher text increase with the number of revoked users. Thus, the heavy overhead and large cipher text size may hinder the adoption of the broadcast encryption scheme to capacity-limited users.

To tackle this challenging issue, we let the group manager compute the revocation parameters and make the result public available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the cipher text size. Specially, the computation overhead of users for encryption operations and the cipher text size is constant and independent of the revocation users.

MODULES INVOLVED IN THIS

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.

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.

Group Member Module

Group members are a set of registered users that will

1. store their private data into the cloud server and
2. 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. The group meme

File Security Module
1. Encrypting the data file.
2. 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).

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.

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 this paper, we design a secure data sharing scheme, for dynamic groups in an untrusted cloud. In SDDC, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, SDDC 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.

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 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. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Transactions on Information and System Security (TISSEC), vol. 9, no. 1, pp. 1-30, 2006.