

## An Approach to Secure Data Sharing for Dynamic Groups in the Cloud

<sup>1</sup>Gagan Jain G C, <sup>2</sup>Venkataravana Nayak K, <sup>3</sup>Krishna Gudi

<sup>1</sup>PG Student Dept. Of CS&E, <sup>2</sup>HOD Dept. Of CS&E, <sup>3</sup>Assistant Professor Dept. Of CS&E  
<sup>1,2,3</sup>GSS Institute of Technology, Bangalore-60

---

**Abstract:** As the low maintenance, cloud computing supply an capable solution for sharing group resource within cloud users. Sharing data with the two or more owners while preserving data and identity privacy from an un-trusted cloud is still an issue, due to the frequent change of the membership. In this paper, we propose a secure data sharing scheme for dynamic subgroups in the cloud. By using group signature and dynamic broadcast encryption techniques, only privileged cloud user can store and share data. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users.

**Keywords:** Cloud Computing, Data sharing, Access control, Privacy preserving, Dynamic subgroups.

---

### I. Introduction

Cloud computing is recognized as an alternative to traditional information technology [1] due to its intrinsic resource-sharing and low-maintenance characteristic. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of datacenters. By migrating the local data management systems into cloud servers, users can enjoy the 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 take an practical data application. A company allows its staff members in the same group or department to store and share files in the cloud. By utilizing the cloud, the staff members can be completely released from the troublesome local data storage and maintenance. It also setup a significant risk to the confidentiality of those stored files. Specifically, 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. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data files 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.

First issue is that, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guaranty of identity privacy, users may be disinclined to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, absolute identity privacy may incur the violate of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables group manager (e.g., a company manager) to reveal the real identity of a user, is also a highly desirable.

Second issue is that, it is highly recommended that any member in a subgroup should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multi-owner manner. Compared with the single-owner manner [3], where only the group manager can store and modify data in the cloud, the multi-owner manner is more flexible in practical applications. More concretely, each user in the subgroup is able to not only read data, but also can modify his/ her part of data in the entire data file shared by the company.

Third issue is that, subgroups are normally dynamic in practice, e.g., new user participation and current employee revocation in a company. The change of membership make secure data sharing is extremely difficult. The anonymous system challenges that new granted users to learn the content of data files stored before their participation, because it is an impossible for new granted users to contact with the nameless data owners, and obtain the corresponding decryption keys. On the other hand, efficient membership revocation mechanism without updating the secret keys of remaining users is also desired to minimize the complexity of key management.

Several security schemes for data sharing on untrusted servers have been proposed [4], [5], [6]. In these approaches, data owners will store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Therefore, 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 revocation and complexities of user participation in these schemes are linearly increasing with the number of revoked users and the number of data owners, respectively. By setting a group with a single

attribute, Lu et al. [7] proposed secure provenance scheme based on the ciphertext-policy attribute-based encryption technique [8], which allows any member in a group to share data with others. However, issue of user revocation is not addressed in their scheme. Yu et al. [3] presented scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique [9]. Unfortunately, the single-owner manner hinders the adoption of their scheme into the case, where any user in the subgroup is granted to store and share data.

## **II. Related Work**

To achieve secure data sharing for dynamic subgroups in the cloud, we combine the dynamic broadcast encryption and group signature techniques. Specially, the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users, and the group signature scheme enables users to anonymously use the cloud resources.

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 both the computation overhead of the encryption and the size of the ciphertext increase with the number of revoked users. Thus, the tedious overhead and large ciphertext size may hinder the adoption of the broadcast encryption scheme to capacity-limited users. To accomplish this challenging issue, we let the group manager to 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 ciphertext size. Specially, computation overhead of users for encryption operations and the ciphertext size is constant and independent of the revocation users.

### **A. Group Signature**

A Group signature scheme is a method for allowing a member of a group to anonymously sign a message on behalf of the group. The concept is first introduced by David Chaum and Eugene van Heyst in 1991. For example, group signature scheme could be used by an employee of a large company where it is sufficient for a verifier to know a message was signed by employee, but not which particular employee signed it. Another application is for the keycard access to restricted areas where it is inappropriate to track individual employee's movements, but necessary to the secure areas to only employees in the group.

Essential to a group signature scheme is a group manager, will takes charge of adding group members and has the ability to reveal the original signer in the event of disputes occurs. In some systems the responsibilities of adding members and revoking signature anonymity are separated and given to a membership manager and revocation manager respectively.

### **B. Dynamic Broadcast Encryption Techniques.**

Broadcast encryption is the cryptographic problem of delivering encrypted content over a broadcast channel in such a way that only qualified users can decrypt the content. The challenge occurs from the requirement that the set of qualified users can change in each broadcast emission, and therefore revocation of particular users or user groups should be possible using broadcast transmissions, only, and without affecting the any remaining users. As efficient revocation is primary objective of broadcast encryption solutions are also referred to as revocation schemes.

Broadcast encryption enables a broadcaster to transmit encrypted data to a set of users so that only a privileged subset of users can decrypt the data. In addition to the above characteristics, dynamic broadcast encryption also permits the group manager to dynamically include new members while preserving previously computed information, i.e., user decryption keys need not to be recomputed, morphology and size of ciphertexts are unchanged and the group encryption key requires no modification. The formal definition and construction of dynamic broadcast encryption are introduced based on the bilinear pairing technique in which will be used as the basis for file sharing in dynamic groups.

## **III. Problem Statement**

### **A. Existing System**

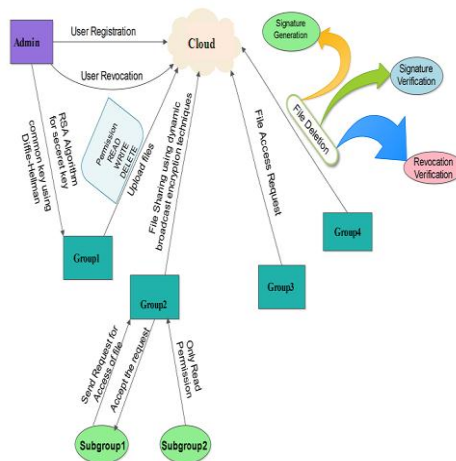
To preserve data privacy, a basic solution is to encrypt the data files, and then upload the encrypted data into the cloud. Unfortunately, designing an capable and secure data sharing scheme for subgroups in the cloud is not an easy task.

In the existing System data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Therefore, 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 revocation and user participation in these schemes are linearly increasing with the number of revoked users and the number of data owners, respectively.

**B. Proposed System**

1. We propose a secure multi-owner data sharing scheme. It implies that any user in the subgroup can securely share data with others by the untrusted cloud.
2. Our proposed scheme is able to support dynamic subgroups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily accomplished through a novel revocation list without updating the secret keys of the remaining users. The computation overhead and size 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 subgroup to anonymously utilize the cloud resource. Moreover, the real identities of the data owners can be revealed by the group manager when disputes occur.
4. We provide very sever security analysis, and perform comprehensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

**IV. System Design**



**Figure 1. System Design**

We consider a cloud computing architecture by combining with an example that a company uses a cloud to enable its staffs in the same subgroup or department to share files. The system design consists of three different entities: the cloud, a group manager (i.e., the company manager), and a large number of group and subgroup members (i.e., the staffs).

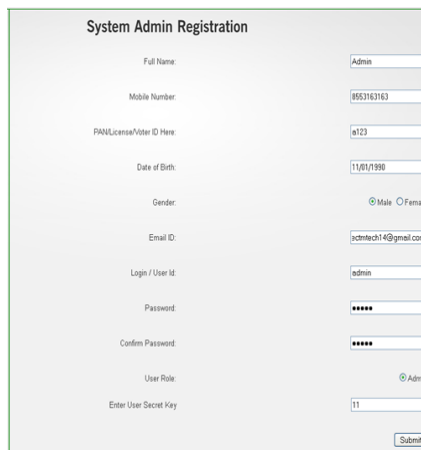
Cloud is operated by CSPs and provides priced abundant storage services. However, cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users’ trusted domain. Similar to we assume that cloud server is honest but curious. i.e, the cloud server will not maliciously 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 takes charge of system parameters generation, user revocation, user registration, and revealing the real identity of dispute data owner. In the given example, group manager is acted by the administrator of the company. Therefore, we assume that group manager is fully trusted by the other parties.

Group members and Subgroup 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, staffs play the role of group and subgroup members. Note that, the group and subgroup membership is dynamically changed, due to the staff resignation and the new employee participation in the company.

## V. Results

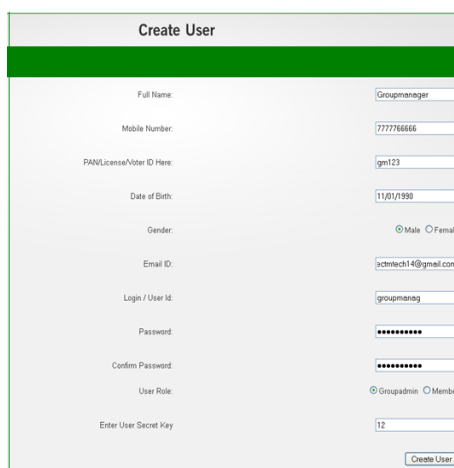
### 1. System Admin Registration.



The screenshot shows a 'System Admin Registration' form with the following fields and values: Full Name: Admin; Mobile Number: 953163163; PAN/License/Voter ID Here: a123; Date of Birth: 11/01/1998; Gender: Male (selected); Email ID: jcdmtecht14@gmail.com; Login / User Id: admin; Password: \*\*\*\*\*; Confirm Password: \*\*\*\*\*; User Role: Admin (selected); Enter User Secret Key: 11. A 'Submit' button is at the bottom right.

Initially create the system admin, by entering the secret message and fill the following fields. Give same name as login name and make it as admin. He acts as a cloud administrator according to the paper.

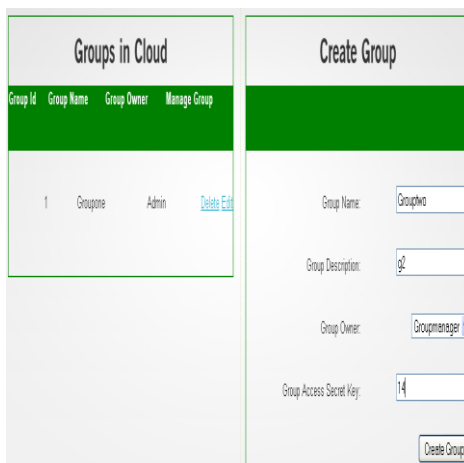
### 2. Group Manager Registration.



The screenshot shows a 'Create User' form with the following fields and values: Full Name: Groupmanager; Mobile Number: 7777766666; PAN/License/Voter ID Here: gm123; Date of Birth: 11/01/1998; Gender: Male (selected); Email ID: jcdmtecht14@gmail.com; Login / User Id: groupmanag; Password: \*\*\*\*\*; Confirm Password: \*\*\*\*\*; User Role: Groupadmin (selected); Enter User Secret Key: 12. A 'Create User' button is at the bottom right.

Login with that admin name and password, after login create a user and mark him as group manager (note: Group manager access key must be delete access)

### 3. Create Groups and Subgroups.



The screenshot shows two side-by-side forms. The left form, titled 'Groups in Cloud', is a table with columns: Group Id, Group Name, Group Owner, and Manage Group. It contains one row: 1, Groupone, Admin, and a 'Delete Edit' link. The right form, titled 'Create Group', has fields: Group Name: Grouptwo; Group Description: g2; Group Owner: Groupmanager (dropdown); Group Access Secret Key: 14. A 'Create Group' button is at the bottom right.

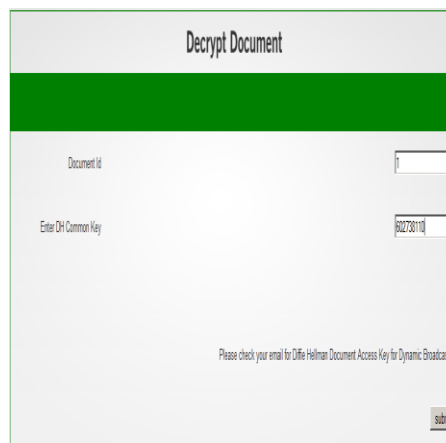
Create the group, after creating a group that will show in the group list. Then edit the group and enable the group dynamic broadcast encryption. Then create users and make them access key delete / read / write.

4. Upload the documents.



To upload a document login from group manager id and upload the document. The document is only uploaded if Group manager access key is delete access and group is enabled with dynamic broadcast encryption. We can check by login with other group members id and their document uploaded by Group manager can be downloaded.

5. To decrypt the document.



To decrypt the document enter the document id and Diffie Helleman common key which is send to the corresponding user Email id and press submit button.

## VI. Conclusion

Finally we conclude that user is able to share data with others in the subgroup without revealing identity privacy to the cloud. It supports efficient user revocation and new user joining. 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 the files stored in the cloud before their participation. Extensive analyses show that this 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. 136149, 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," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.
- [7]. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.
- [8]. B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, <http://eprint.iacr.org/2008/290.pdf>, 2008.
- [9]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.