ISSN 2319-2720
Volume 7, No.2, April – June 2018
International Journal of Computing, Communications and Networking
Available Online at http://www.warse.org/ijccn/static/pdf/file/ijccn55722018.pdf
https://doi.org/10.30534/ijccn/2018/55722018

# A SECURE ANTI-COLLUSION DATA SHARING SCHEME FOR DYNAMIC GROUPS IN THE CLOUD

**Rajashekhar S A[1],Vandana V[2], Vathsala P M[3], Vidya R[4], Vijaylaxmi[5]**
[1]Assistant professor EWIT, India, rajshekhar@ewit.edu
[2]Student, EWIT, India, vanduv96@gmail.com
[3]Student, EWIT, India, v.pradhaan.ce@gmail.com
[4]Student, EWIT, India, vidyar137@gmail.com
[5]Student, EWIT, India, vijaylaxmi.maskale@gmail.com

**ABSTRACT**

Cloud computing is used to achieve an effective and economical approach for data sharing among group members with the characters of low maintenance and little management cost. Sharing data while providing privacy-preserving is still a challenging issue, especially for an entrusted cloud due to the collusion attack. First, a secured way for key distribution without any secure communication channels is created. Second, can achieve fine-grained access control. Third, we can protect the scheme from collusion attack. Finally, fine efficiency is achieved which means previous users need not to update their private keys for the situation either a new user joins in the group or a user is revoked from the group.

**Keywords: Access control, privacy-preserving, key distribution, cloud computing**

.

## 1. INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. Here, 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. Data storage is one of the most fundamental services offered by cloud providers. However, security concerns become the main constraint as we outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted data into the cloud [2]. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud due to the following challenging issues.

First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. On the other hand, unconditional identity privacy may incur the abuse of privacy. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable. Second, it is highly recommended that any member in a group should be able to not only read data, but also modify his/her part of data in the entire data file shared by the company, which is defined as the multiple-owner manner. Compared with the single-owner manner [3], where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. Last but not least, groups are normally dynamic in practice, e.g., new staff participation and current employee revocation in a company. The changes of membership make secure data sharing extremely difficult. 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.

## 2. RELATED WORK

Kallahalla et al. [3] presented a cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into filegroups and encrypting each file group with a file-block key. However, the file-block keys need to be updated and distributed for a user revocation, therefore, the system had a heavy key distribution overhead.

Yu et al. [6] exploited and combined techniques of key policy attribute-based encryption [7], proxy re- Encryption and lazy re-encryption to achieve fine- grained data access control without disclosing data contents.

However, the single-owner manner may hinder the implementation of applications, where any member in the group can use the cloud service to store and share data files with others.

Lu et al. [8] proposed a secure provenance scheme by leveraging group signatures and cipher text-policy attribute-based encryption techniques [9]. Each user obtains two keys after the registration while the attribute key is used to decrypt the data which is encrypted by the attribute-based encryption and the group signature key is used for privacy- preserving and

traceability. However, the revocation is not supported in this scheme.Liu et al. [10] presented a secure multi-owner data share.
The revoked user and the cloud [13]. The revoked user can use his private key to decryptthe encrypted data file and getthe secret data after his revocation by conspiring with the cloud. In the phase of file access, first of all, the revoked user sends his request to the cloud, then the cloud responds the corresponding encrypted data file and revocation list to the revoked user without verifications. Next, therevoked user can compute the decryption key with the help of the attack algorithm. Finally, this attack can lead to the revoked users getting the sharing data and disclosing other secrets of legitimate members. Zhou et al. [14] presented a secure access control scheme on encrypted data in cloud storage by invoking role-based encryption technique. It is claimed that the scheme can achieve efficient user revocation that combines role-based access control policies with encryption to secure large data storage in the cloud. Unfortunately, the verifications between entities are not concerned, the scheme easily suffer from attacks, for
example, collusion attack. Finally, this attack can lead to disclosing sensitive data files. Zou et al. [15] presented a practical and flexible key management mechanism for trusted collaborative computing. By leveraging access control polynomial, it is designed to achieve efficient access control for dynamic groups. Unfortunately, the secure way for sharing the personal permanent portable secret between
the user and the server is not sup- ported and the private key will be disclosed once the personal permanent portable secret is obtained by the attackers. Nabeel et al. [16] proposed a privacy preserving policy-based content sharing scheme in public clouds. However, this scheme is not secure because of the weak protection of commitment in the phase of identity token issuance.

## 3. PROPOSED SYSTEM

In this paper, we propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. The main contributions of our scheme include:

1) We provide a secure way for key distribution with- out any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.
2) Our scheme can achieve fine-grained access control, with the help of the group user in the group can use the source in the and revoked users cannot access the cloud after they are revoked.
3) We propose a secure data sharing scheme which can beprotected from collusion attack. The revoked users can not be able to perform.
4) Our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated.
5) We provide security analysis to prove the security of our scheme. In addition, we also perform simulations to demonstrate the efficiency of our scheme.

## 4. SYSTEM MODEL AND DESIGN GOALS

### 4.1. System Model

As illustrated in Fig. 1, the system model consists of three different entities: the cloud, a group manager and a large number of group members.

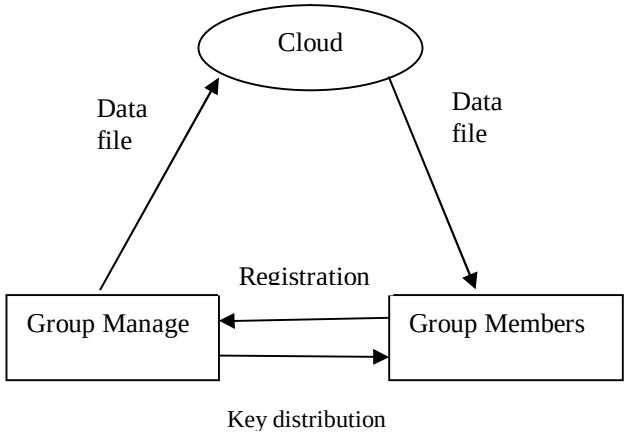


Fig. 1. System model

The cloud, maintained by the cloud service providers, provides storage space for datafiles. However, the cloud is untrusted since the cloud service providers are easily to become untrusted. Therefore, the cloud will try to learn the content of the stored data.
Group manager takes charge of system parameters Generation, user registration, and user revocation. In the practical applications, the group manager usually is the leader of the group. Hence, 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 own data into the cloud and share them with others. In the scheme, the group membership is dynamically changed, due to the new user registration and user revocation.

### 4.2. System Design

We describe the main design goals of the proposed scheme including key distribution, data confidentiality, access con- trol andefficiency as follows:
Key distribution: The requirement of key distribution is that users can securely obtain their private keys from the group manager without any Certificate Get the original data files once they are revoked authorities. In other

existing schemes, this goal is even if they con- spire with the untrusted achieved by assuming that the c loud. Access control: First, group members are able to use the cloud resource for data storage and data sharing.Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud resource again once they are revoked.Data confidentiality: Data confidentiality requires thatunauthorized users including the cloud are incapable of learning the content of the stored data. To maintain the availability of data confidentiality for dynamic groups is still an important and challenging issue. Specifically, revoked users are unable to decrypt the stored data file after the revocation.

Efficiency: 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 others, which means that the remaining users do not need to update their private keys.

## 5. MODULE DESCRIPTION

### 5.1. Cloud Module :

In this module, a real Cloud is created and provide priced abundant storage services and users can upload their data in the cloud. By this module, 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. The cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes.

### 5.2. 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.

### 5.3. 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.

### 5.4. 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).

### 5.5. 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.

### 5.6. 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.

## 6. ACKNOWLEDGEMENT

We wish to offer our sincere gratitude to our principal Dr. K Channakeshavalu, Principal, EWIT, Bangalore, for his moral support towards completing my project work. We would like to thank Dr. Arun Biradar, Head of Department, Computer Science & Engineering, EWIT, Bangalore, for his valuable suggestions and expert advice. We deeply express my sincere gratitude to my guide Prof. Rajshekhar S.A, Assoc professor Department of CSE, EWIT, Bangalore, for his able guidance throughout the project work and guiding me to organize the report in a systematic manner. We thank our Parents, and all the Faculty members of Department of Computer Science & Engineering for their constant support and encouragement

## 7. CONCLUSION

In this paper, we design a secure anti- collusion data sharing scheme for dynamic groups in the cloud. In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. Moreover, our scheme can achieve secure user revocation, the revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud.

## REFERENCES.

[1] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149. [3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42. https://doi.org/10.1007/978-3-642-14992-4_13

[2] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Secur- ing remote untrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.

[3] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distrib- uted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005, pp. 29–43.

[4] W. Lou, "Achieving

S. Yu, C. Wang, K. Ren, and secure, scalable, and fine-grained data access control in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[6] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.