ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

A Secure Method Using Cloud in Anti-Collusion Data Sharing Scheme for Dynamic Groups

Nidhi N G, Padmashri A M, Poojitha M, Pooja S, Deepashree N S
B.E Student, Dept. of CSE, GAT, Bangalore, Karnataka, India
B.E Student, Dept. of CSE, GAT, Bangalore, Karnataka, India
B.E Student, Dept. of CSE, GAT, Bangalore, Karnataka, India
B.E Student, Dept. of CSE, GAT, Bangalore, Karnataka, India
Assistant Professor, Dept. Of CSE, GAT, Bangalore, Karnataka, India

ABSTRACT: Benefited from cloud computing, users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an un-trusted cloud due to the collusion attack. Moreover, for existing schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice. In this paper, we propose a secure data sharing scheme for dynamic members. First, we propose a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager. Second, our scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. Third, we can protect the scheme from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the un-trusted cloud. In our approach, by leveraging polynomial function, we can achieve a secure user revocation scheme. Finally, our scheme can achieve fine efficiency, 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

I. INTRODUCTION

Cloud computing, with the characteristics of intrinsic data sharing and low maintenance, provides a better utilization of resources. In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data [1]. It can help clients reduce their financial overhead of data managements by migrating the local managements system into cloud servers. However, security concerns become the main constraint as we now 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. Kallahalla presented a cryptographic storage system [3] that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file-groups 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. Other schemes for data sharing on untrusted servers have been proposed in [4], [5]. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users.

II. RELATED WORK

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

DOI: 10.15680/IJIRCCE.2017. 0505290

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 proposed a secure provenance scheme by leveraging group signatures [8] and ciphertext-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 presented a secure multi-owner data sharing scheme, named Mona [10]. It is claimed that the scheme can achieve fine-grained access control and revoked users will not be able to access the sharing data again once they are revoked. However, the scheme will easily suffer from the collusion attack by the revoked user and the cloud [13]. The revoked user can use his private key to decrypt the encrypted data file and get the 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, the revoked 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 presented a secure access control scheme on encrypted data in cloud storage by invoking role-based encryption [14] 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 presented a practical and flexible key management mechanism [15] 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 supported and the private key will be disclosed once the personal permanent portable secret is obtained by the attackers. Nabeel proposed a privacy preserving policy [16] 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.

III. PROPOSED SYSTEM

The proposed system is shown in the figure 1.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 without 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 list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.

3) We propose a secure data sharing scheme which can be protected from collusion attack. 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. Our scheme can achieve secure user revocation with the help of polynomial function.

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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

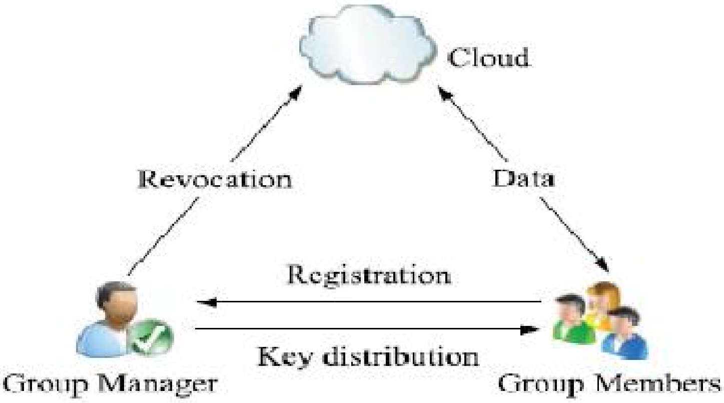


Fig.1: System Architecture

THREAT MODEL, SYSTEM MODEL AND DESIGN GOALS

Threat Model

As the threat model, in this paper, we propose our scheme based on the Delov-Yao model [17], in which the adversary can overhear, intercept, and synthesis any message at the communication channels. With the Delov-Yao model, the only way to protect the information from attacking by the passive eavesdroppers and active saboteurs is to design the effective security protocols. This means there is not any secure communication channels between the communication entities. Therefore, this kind of threaten model can be more effective and practical to demonstrate the communication in the real world.

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. The cloud, maintained by the cloud service providers, provides storage space for hosting data files in a pay-as-you-go manner. 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. Therefore, we assume that the group manager is fully trusted by the other parties. Group members (users) 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.

Design Goals

We describe the main design goals of the proposed scheme including key distribution, data confidentiality, access control and efficiency 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 Authorities. In other existing schemes, this goal is achieved by assuming that the communication channel is secure, however, in our scheme, we can achieve it without this strong assumption.

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 that unauthorized 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 k

IV. IMPLEMENTATION

The system consists of 6 major modules. Cloud Module , Group Manager Module , Group Member Module , File Security Module , Group Signature Module , User Revocation Module .

1. Cloud Module :

In this module, we purchasing public 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

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.

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 Group Signature Module :

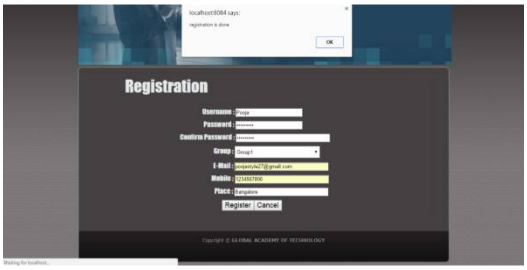
A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

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.

V. RESULTS AND PERFORMANCE EVALUATION

Group Member registers to the application by giving all the relevant details. The registration page is shown in the figure 2. A successful registration message is displayed. A login page for a group member is displayed by specifying valid username and password. The login page is shown in the figure 3



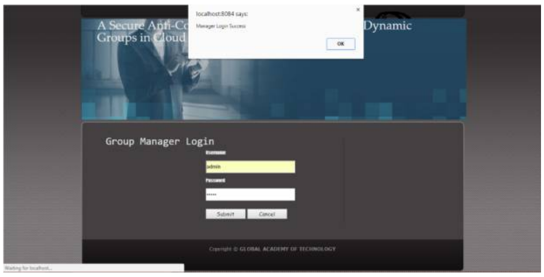
localhost:8084 says:
registration is done

Registration

Username : Pooja
Password : ••••••••••
Confirm Password : ••••••••••
Group : Group1
E-Mail : poojastyle27@gmail.com
Mobile : 1234567890
Place : Bangalore

Copyright © GLOBAL ACADEMY OF TECHNOLOGY

Waiting for localhost...



localhost:8084 says:
Manager Login Success

A Secure Anti-Co... Dynamic Groups in Cloud

Group Manager Login

Username
admin
Password
•••••

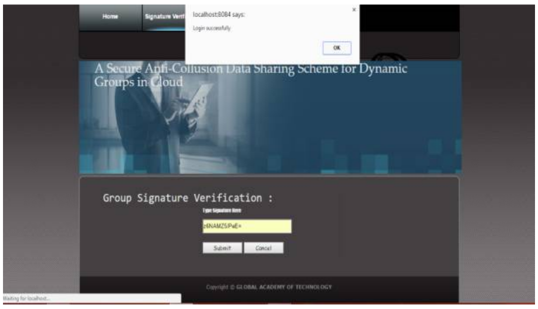
Copyright © GLOBAL ACADEMY OF TECHNOLOGY

Waiting for localhost...

Fig.2: User Registration

Fig.3: Group Member Login

Group signature key verification page is displayed and it's shown in the below figure 4.next step is to upload the file to the cloud. Group member upload file page is displayed and it's shown in the below figure 5 with specifying the file name. Next to download the file from the cloud appropriate fields are displayed in File download page is shown in figure 6.



localhost:8084 says:
Login successfully

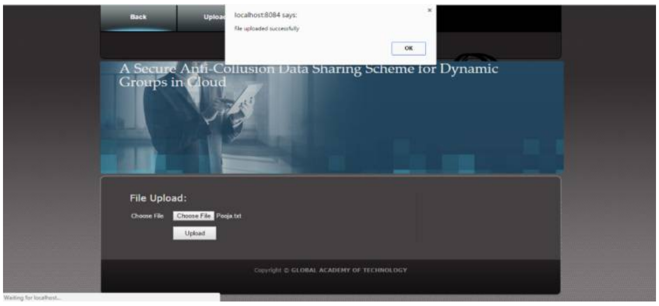
A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in Cloud

Group Signature Verification :

Type Signature Here
z6NAMZ5/PwE=

Copyright © GLOBAL ACADEMY OF TECHNOLOGY

Waiting for localhost...



localhost:8084 says:
File uploaded successfully

A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in Cloud

File Upload:

Choose File Pooja.txt

Copyright © GLOBAL ACADEMY OF TECHNOLOGY

Waiting for localhost...

Fig.4: Group Signature Verification

Fig.5: File Upload

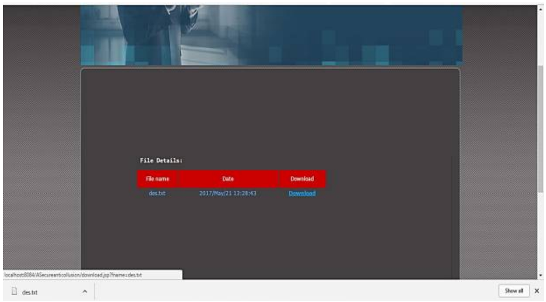
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017



File Details:

File name	Date	Download
des.txt	2017/May/21 13:28:43	Download

localhost:8084/ASecureanticollusion/download.jsp?fname=des.txt

des.txt

Fig.6: File Download

We make the performance simulation with NS2 and compare with Mona in [10] and the original dynamic broadcast encryption (ODBE) scheme in [12]. Without loss of generality, we set p = 160 and the elements in G1 and G2 to be 161 and 1,024 bits, respectively. In addition, we assume the size of the data identity is 16 bits, which yield a group capacity of 216 data files. Similarly, the size of user and group identity are also set 16 bits. Both group members and group managers processes are conducted on a laptop with Core 2 T5800 2.0 GHz, DDR2 800 2 G, Ubuntu 12.04 X86. The cloud process is implemented on a laptop with Core i7-3630 2.4 GHz, DDR3 1600 8 G, Ubuntu 12.04 X64. We select an elliptic curve with 160 bits group order.

Our scheme can achieve secure key distribution, fine access control and secure user revocation. For clearly seeing the advantages of security of our proposed scheme, as illustrated in Table 1, we list a table compared with Mona, which is Liu's scheme, the RBAC scheme, which is Zhou et al.'s scheme and ODBE scheme, which is Delerablee's scheme. The in the blank means the scheme can achieve the corresponding goal.

Table 1 :Security Performance Comparison

	Secure key distribution	Access control	Secure user revocation	Anti-collusion attack	Data confidentiality
Mona		√			
RBAC scheme		√			
ODBE		√	√	√	
Our scheme	√	√	√	√	√

VI. Conclusion and Future Work

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 un-trusted cloud.

References

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, And M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. International Conferences. 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.

[4] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., pp. 131–145,2003.
[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005,pp. 29–43.
[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc.ACM Symp.Inf., Comput.Commun. Security, pp. 282–292, 2010.
[7] 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, pp. 89–98, 2006.
[8] 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.
[9] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int.Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53–70.
[10] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiownerdata sharing for dynamic groups in the cloud," IEEE Trans ParallelDistrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.
[11] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," in Proc. Annu. Int. Conf.Theory Appl. Cryptographic Techn., 2005, pp. 440–456.
[12] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size Ci-phertextsor decryption keys," in Proc. 1st Int. Conf. Pairing-Based Cryptography,2007, pp. 39–59.
[13] Z. Zhu, Z. Jiang, and R. Jiang, "The attack on mona: Secure multi owner data sharing for dynamic groups in the cloud," in Proc. Int.Conf. Inf. Sci. Cloud Comput., Dec. 7, 2013, pp. 185–189.
[14] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage,"IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.
[15] X. Zou, Y.-S. Dai, and E. Bertino, "A practical and flexible key management mechanism for trusted collaborative computing,"in Proc. IEEE Conf. Comput. Commun., pp. 1211–1219, 2008.
[16] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. Know. Data Eng., vol. 25, no. 11, pp. 2602–2614, Nov. 2013.
[17] D. Dolev and A. C. Yao, "On the security of public key protocols,"IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

BIOGRAPHY

Padmashri A M pursuing Bachelor's degree in Computer Science and Engineering from Global Academy Of Technology College of engineering Visveswaraya Technological University Belgavi in 2017. My research interests include Cloud computing security and member of Computer Society of India (CSI).

Pooja S pursuing Bachelor's degree in Computer Science and Engineering from Global Academy Of Technology College of engineering Visveswaraya Technological University Belgavi in 2017. My research interests include Cloud computing security and member of Computer Society of India (CSI).

Poojitha M pursuing Bachelor's degree in Computer Science and Engineering from Global Academy Of Technology College of engineering Visveswaraya Technological University Belgavi in 2017. My research interests include Cloud computing security and member of Computer Society of India (CSI).

Nidhi N G pursuing Bachelor's degree in Computer Science and Engineering from Global Academy Of Technology College of engineering Visveswaraya Technological University Belgavi in 2017. My research interests include Cloud computing security and member of Computer Society of India (CSI).

Deepashree N S received Bachelor‘s degree in Information Science and Engineering from Sri Bhagwan Mahaveer Jain College of engineering Visveswaraya Technological University Belgavi in 2012. Currently pursuing MTech degree in Computer science and engineering in RV college of Engineering, Visveswaraya Technological University Belgavi. Currently Working as Assistant professor in the Department of Computer science and engineering in Global Academy of Technology Visveswaraya Technological University Belgavi. My research interests include Cloud computing security and network security and member of Computer Society of India (CSI)