International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Anti-Collusion Data Sharing Scheme in the Cloud

Ayesha Majid [1], Afreen Fatima [2], Mariya Ahmed [3], Asra Begum [4]

[1] B.Tech, Department of CSE, Lords Institute of Engineering and Technology.

[2] B.Tech, Department of CSE, Lords Institute of Engineering and Technology.

[3] B.Tech, Department of CSE, Lords Institute of Engineering and Technology.

[4] Assistant Professor, Department of CSE, Lords Institute of Engineering and Technology.

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 untrusted 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. Firstly, 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. Secondly, 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. Thirdly, 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 untrusted 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.

INTRODUCTION

Cloud Computing, with the characteristics of natural information sharing and low support, gives a superior usage of resources. In Cloud Computing, cloud administration suppliers offer a reflection of boundless storage room for customers to host informatio. It can offer customers some support with reducing their money related overhead of information administrations by moving the nearby administrations framework into cloud servers. however, security concerns turn into the principle control as we now outsource the capacity of information, which is perhaps delicate, to cloud suppliers. To safeguard information security, a typical methodology is to encode information records before the customers transfer the scrambled information into the cloud. Unfortunately, it is hard to outline a protected and productive information sharing plan, particularly for element groups in the cloud. Kallahalla et al displayed a cryptographic supply framework that empowers secure information sharing on untrust servers taking into account the procedures that isolating documents into filegroups and scrambling each file_group with a record square key. In any case, the record square keys should be upgraded and circulated for a client denial, along these lines, the framework had a extensive key appropriation overhead. Different plans for information sharing on untrusted servers have been proposed. As it might, the complexities of client interest and renouncement in these plans are straightly expanding with the quantity of information owner and the repudiated clients. Yu et al altered and joined procedures of key strategy trait based encryption, intermediary reencryption and slow re-encryption to accomplish fine-grained information access control without presentation information substance. Be that as it may, the single-proprietor way might block the usage of uses, where any part in the gathering can utilize the cloud administration to store and impart information records to others.

EXISTING SYSTEM

- Kallahalla et al presented a cryptographic storage system 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.

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

DISADVANTAGES

- The file-block keys need to be updated and distributed for a user revocation; therefore, the system had a heavy key distribution overhead.
- The complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users.
- 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.

PROPOSED SYSTEM

- In this paper, we propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group.
- 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.
- 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.
- 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.
- Our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

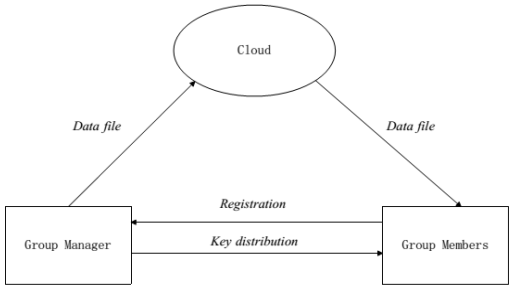
the group, the private keys of the other users do not need to be recomputed and updated.

- ❖ We provide security analysis to prove the security of our scheme.

ADVANTAGES OF PROPOSED SYSTEM:

- ✓ The computation cost is irrelevant to the number of revoked users in RBAC scheme. The reason is that no matter how many users are revoked, the operations for members to decrypt the data files almost remain the same.
- ✓ The cost is irrelevant to the number of the revoked users. The reason is that the computation cost of the cloud for file upload in our scheme consists of two verifications for signature, which is irrelevant to the number of the revoked users. The reason for the small computation cost of the cloud in the phase of file upload in RBAC scheme is that the verifications between communication entities are not concerned in this scheme.
- ✓ 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.

SYSTEM ARCHITECTURE:



MODULES:

1.Cloud Module

2.Group Manager Module

3.Group Member Module

4.File Security Module

5.Group Signature Module

6. User Revocation Module .

MODULES DESCRIPTION:

1.Cloud Module :

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

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

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).

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

5.Group Signature Module :

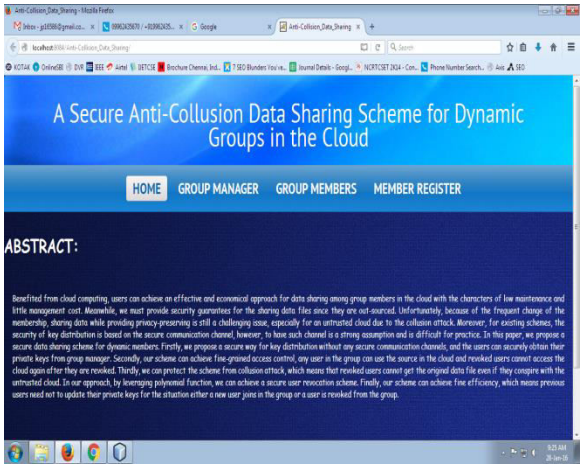
A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

6. User Revocation Module :

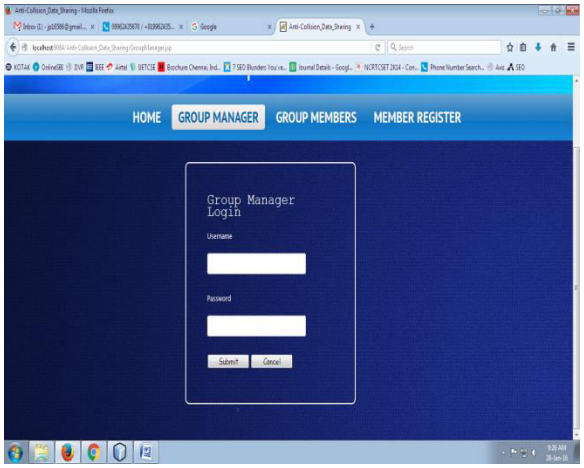
User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

SCREEN SHOTS:

Home:



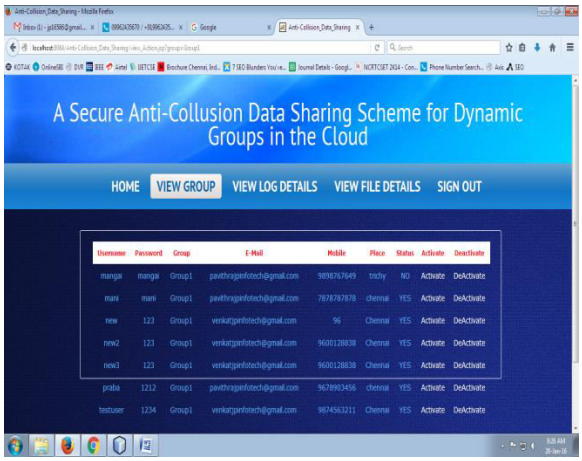
Group Manager Login:



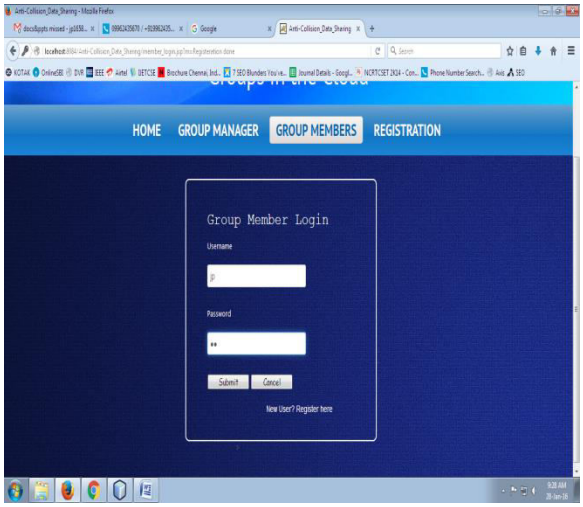
Gropup Manager Home:

View Groups:

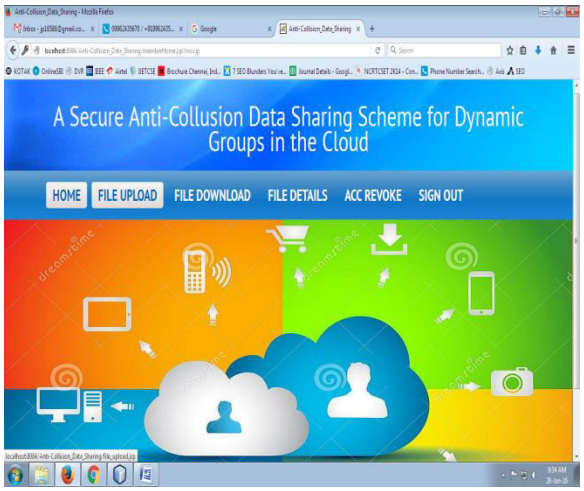
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org



Group Member Login:



Group Member Home:



CONCLUSION

In this paper, we design a secure anti-collusion data sharing scheme for dynamic groups in the cloud. In our scheme, the userscan securely obtain their private keys from group managerCertificate 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] M.Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.Katz,A.Konwinski, G. Lee, D.Patterson, A.Rabkin, I.Stoica, andM.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] 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.

[4] E.Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and DistributedSystems Security Symp. (NDSS), 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," Proc. Network and Distributed Systems SecuritySymp. (NDSS), pp. 29-43, 2005.

[6] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. 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," Proc. ACM Conf. Computer and Comm. Security (CCS), 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," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[9] 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

[10] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[11] D.Boneh, X. Boyen, and E. Goh, "Hierarchical IdentityBasedEncryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf.Theory and Applications of Cryptographic Techniques (EUROCRYPT),pp. 440-456, 2005.

[12] C. Delerablee, P. Paillier, and D. Pointcheval, "FullyCollusionSecure Dynamic Broadcast Encryption with Constant-SizeCi-phertexts or Decryption Keys," Proc.First Int'l Conf. Pairing-BasedCryptography, pp. 39-59, 2007.