

A Unique Method to Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

Julure Raviteja

**M.Tech- Computer Science,
Department of CSE,
SRTIST Nalgonda, Telangana.**

Chinnala Balakrishna

**Assistant Professor,
SRTIST Nalgonda, Telangana.**

T.Madhu

**HOD,
SRTIST Nalgonda, Telangana.**

ABSTRACT:

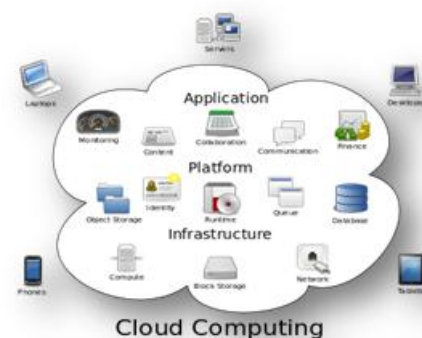
Benefited from cloud computing, users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. 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

What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.



Structure of cloud computing

How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations

per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

- **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity:** Capabilities can be rapidly and elastically provisioned, in some cases

automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

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 OF EXISTING SYSTEM:

- 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 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.

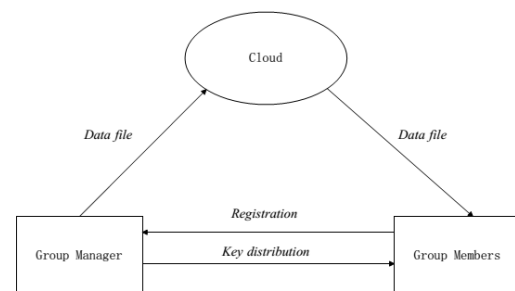
ADVANTAGES OF PROPOSED SYSTEM:

- ✓ 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:



IMPLEMENTATION

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 :

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).

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 :

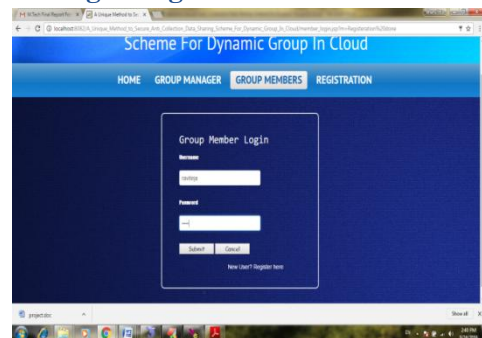
User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

SCREEN SHOTS

Home:



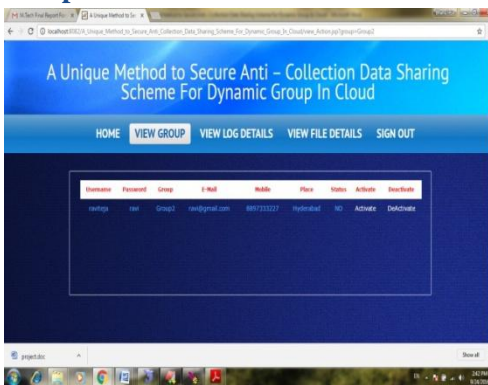
Group Manager Login:



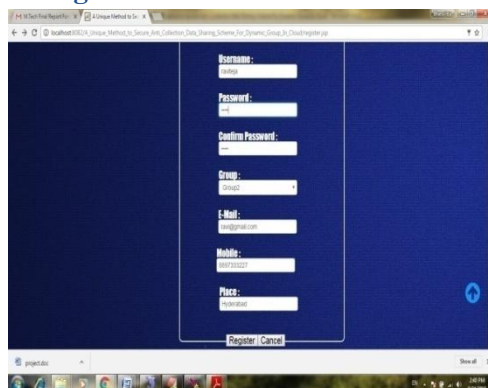
Group Manager Home:



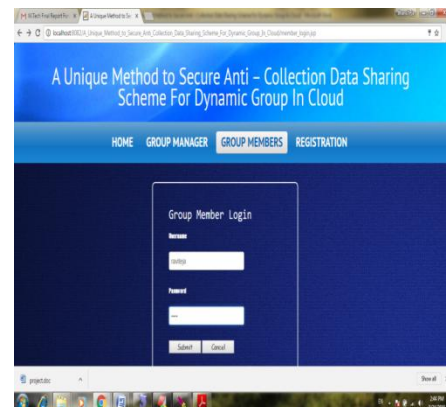
View Group:



Member Registration:



Group Member Login:



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] 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," *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 Distributed Systems 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. Deleralee, P. Paillier, and D. Pointcheval, “FullyCollusionSecure Dynamic Broadcast Encryption with Constant-SizeCiphertexts or Decryption Keys,” Proc.First Int’l Conf. Pairing-BasedCryptography, pp. 39-59, 2007.

[13]Zhongma Zhu, Zemin Jiang, Rui Jiang, “The Attack on Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud, ”Proceedings of2013 International Conference on Information Science and Cloud Computing (ISCC 2013), Guangzhou, Dec.7,2013,pp. 185-189.

[14]Lan Zhou, Vijay Varadharajan, and Michael Hitchens, “Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage,”IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, December 2013.

[15]Xukai Zou, Yuan-shunDai, and ElisaBertino, “A practical and flexible keymanagement mechanism for trusted collaborative computing,”INFOCOM 2008, pp. 1211-1219.

Author’ Details:



Mr. Julure Raviteja

Was Born on 15-JUN-1992 in Munugode Village, Nalgonda District, B.Tech specialization on Information Technology in Swami Ramananda Tirtha Institute Of Science & Technology – Nalgonda, Telangana, Year of 2010 – 2014. **M.Tech** specialization on Computer Science in Swami Ramananda Tirtha Institute of Science & Technology – Nalgonda, Telangana.



CH. Bala Krishna

Received the B.Tech degree in Information Technology and M.Tech degree in Computer Science and Engineering from J N T U Hyd-University. He is working as a Assistant Professor in Swami Ramananda Tirtha Institute of Science and technology, Nalgonda, Telangana, India. He has having 8 years of teaching Experience.



T. Madhu

(HOD) associate professor and head of the department in CSE Swami Ramananda Tirtha Institute of Science and technology, Nalgonda, Telangana.