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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Secured Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

Kishor Kumar E D, Dara Raju

M. Tech Student, Dept. of CSE, Krishna Murthy Institute of Technology and Engineering, Hyderabad, India

Asst. Professor, Dept. of CSE, Krishna Murthy Institute of Technology and Engineering, Hyderabad, India

ABSTRACT: In cloud providing security, guarantees for the sharing data file. 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. In this research work, 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

This 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: Cloud computing, Security, Private keys, public keys, fine-grained access control.

I. INTRODUCTION

As cloud computing becomes prevalent, more and more sensitive information By storing their data into the cloud, the data owners can be relieved from the burden of data storage and maintenance, so as to enjoy the on-demand high quality data storage service cloud server are not in the same trusted domain may put the outsourced data at risk.

In this work, a secure data sharing scheme, which can achieve secure key distribution and data sharing for a dynamic group in the cloud. The main contributions of this scheme include:

- A way for key distribution without any secure communication channels. The users secure can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.
- This 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.
- A secure data sharing scheme can be protected from collusion attack. The revoked users cannot be able to get original data files once they are revoked even if they conspire with the untrusted cloud. This scheme can achieve secure user revocation with the help of polynomial function.

II. RELATED WORK

A.CRYPTOGRAPHIC CLOUD STORAGE

Many researchers have proposed stored encrypted data in the cloud to define against CSP. S. Kamara and K. Lauter [2] in their work "Cryptographic cloud storage" considered the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer.Its core, the architecture consists of three components: a data processor (DP), that processes data before it is sent to the cloud; a data verifier (DV), that checks whether the data in the cloud has been tampered with; and a token generator (TG),

Under this approach, users are revoked by having a third party to re encrypt data such that previous keys can no longer decrypt any data.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

B.PLUTUS: SCALABLE SECURE FILE SHARING ON UNTRUSTED STORAGE

which uses a lockbox to protect only the keys. Mechanisms that Plutus uses to provide basic file system security features-(1) To detect and prevent unauthorized data modifications, (2) To differentiate between read and write access to files, and (3) To change users access privileges.

In encrypt-on-disk file systems, the clients encrypt all directories and their contents. Which used a single key to encrypt an entire directory of files.

Mahesha et al [3] in their work "Plutus: Scalable secure file sharing on untrusted storage" introduces a new secure file system which strives to provide strong security even with an untrusted server. The main feature of Plutus is that all data is stored encrypted and all key distribution is handled in a decentralized manner. All cryptographic and key management operations are performed by the clients, and the server incurs very little cryptographic overhead.

C.MONA: SECURE MULTI-OWNER DATA SHARING FOR DYNAMIC GROUPS IN THE CLOUD

With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose a secure multi owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments[4].

III. EXISTING SYSTEM

The Existing techniques of key policy attribute is based on "encryption, proxy re-encryption and lazy re-encryption" to achieve fine-grained data access control without disclosing data contents. However, the single owner manners 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. A secure provenance scheme by leveraging group signatures and cipher text policy attribute based encryption techniques. Each user obtains two keys after the registration while the attribute key is used to decrypt the data[5]. 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.

there are some disadvantages with the existing system they are as follows.

1. This scheme has secret key between the user and the server, it is not supported and the private key will be disclosed once the personal permanent portable secret key is obtained by the attackers.
2. This scheme easily suffer from attacks, for example collusion attack, this attack can lead to disclosing sensitive data files.

IV. PROPOSED SYSTEM

A secure data sharing scheme proposes, which can achieve secure key distribution and data sharing for dynamic group. The main contributions of this scheme include:

1. This 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. This 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. This 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. This scheme can achieve secure user revocation with the help of polynomial function.
4. This 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.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

5. This scheme provides a security analysis to prove the security of our scheme. In addition, it also perform simulations to demonstrate the efficiency of our scheme.

We can get some advantages from this scheme, they are:

1. This scheme achieve a secure key distribution and data sharing for dynamic group.
2. In this scheme the users can securely obtain their private keys from group manager without any Certificate Authorities.
3. This scheme can be protected from collusion attack.
4. This scheme is able to support dynamic groups efficiently.

V. SYSTEM ARCHITECTURE

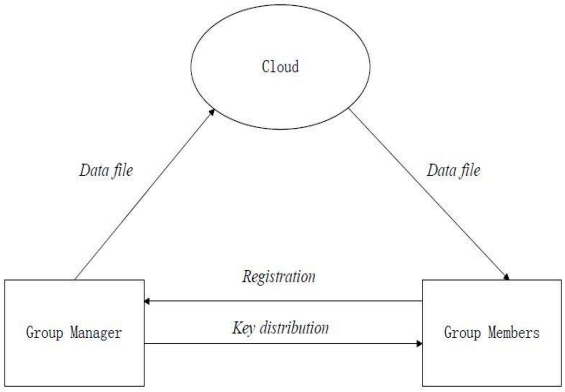


Fig: Architecture diagram for secured anti-collision data sharing.

As illustrated in the above figure , 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 practices.

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[6].

VI. SYSTEM SPECIFICATION AND SYSTEM REQUIREMENTS

A. HARDWARE REQUIREMENTS

Processor	-	Pentium –IV
Speed	-	1.1 GHz
RAM	-	256 MB(min)
Hard Disk	-	20 GB

B. SOFTWARE REQUIREMENTS

Operating System: Windows95/98/2000/XP/7.
Application Server: Tomcat6.0/7.X.
Front End: HTML, Java, JSP.
Scripts: JavaScript.
Server side Script: Java Server Pages.
Database: MYSQL 5.0.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Database Connectivity: JDBC.

VII. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing, designing of methods to achieve change over and evaluation of change over methods.

Algorithm/Technique used

Advanced Encryption Standard (AES)

Algorithm Description

AES is an iterated symmetric block cipher, which means that:

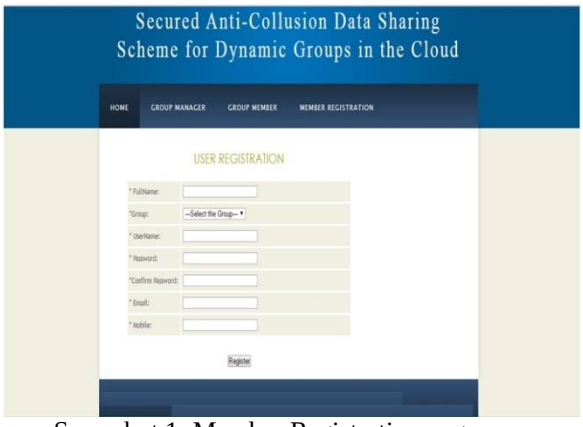
- AES works by repeating the same defined steps multiple times.
- AES is a secret key encryption algorithm.
- AES operates on a fixed number of bytes.

AES as well as most encryption algorithms is reversible. This means that almost the same steps are performed to complete both encryption and decryption in reverse order. The AES algorithm operates on bytes, which makes it simpler to implement and explain[7].

This key is expanded into individual sub keys, a sub keys for each operation round. This process is called Key Expansion.

VIII. SIMULATION AND RESULTS

Snapshot below shows the member registration page, here user enter the required user details to get membership of the group.



Snap shot 1: Member Registration page

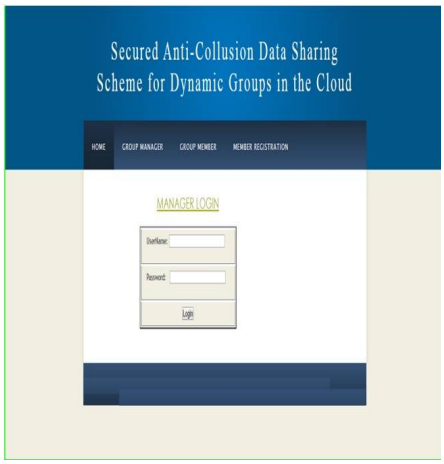
snapshot below shows the group manager login page, here group manager has to enter the username and password.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

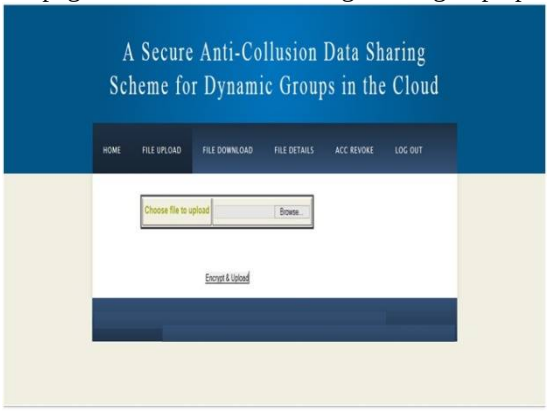


Snapshot 2: Group manager login

Snapshot below shows the Group member login page, here group member has to enter the correct email id, password and registered group.OTP is generated that is sent to the user's mail.

Snapshot 3: Group member login

Snapshot below shows the file upload page, here member of the registered group upload the files into cloud.



Snap Shot 4: File upload

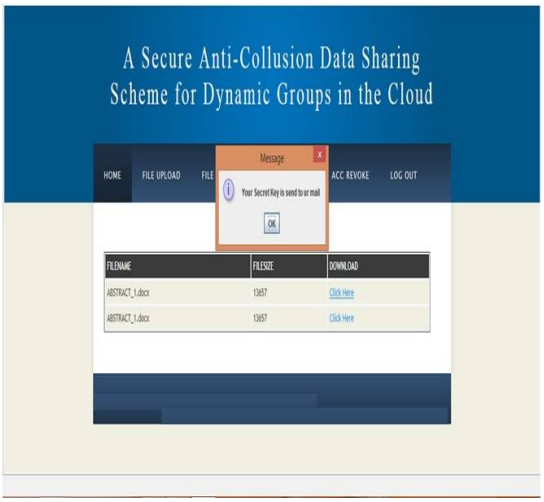
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Snapshot below shows the file download page, here OTP is generated and that is sent to the user's mail.



Snapshot 5: File download

Snapshot below shows account revocation of the group member.

Snapshot 6: Account revocation

IX. **CONCLUSION**

This scheme designs a secure anti-collusion data sharing scheme for dynamic groups in the cloud. In this scheme, the users can securely obtain their private keys from group manager without any Certificate Authorities and secure communication channels. Also, this 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, this 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.

IX. **FUTURE ENHANCEMENT**

In this research work, we have reviewed literature on ways to provide a secure environment where a data owner can share data with members of his group while preventing any outsiders from gaining any data access in case of

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

malicious activities such as data loss and theft. However, throughout this work we assume that members of the group will not carry out malicious activities on the data owner's data.

Auditing and Accountability in the Cloud is a potential for future research in the context of data sharing in the Cloud. Many users in particular organizations and enterprises gain the benefit from data sharing in the Cloud. However, there is always a likely chance that members of the group can carry out illegal operations on the data such as making illegal copies and distributing copies to friends, general public, etc in order to profit. A future research direction would be to find ways for a data owner to hold accountable any member that carries out malicious activities on their data.

Another research direction would be to give the data owner physical access control over the data. Instead of accountability, the data owner can create a set of access control rules on his data and send the data along with the access control policy. In this way, any member with access to the data can only use the data in such a way that abides by the access control policy. If a member attempts to make illegal copies of the data, the access control policy should "lock" the data to prevent the member from doing so.

Also, since data stored in the Cloud are usually stored and replicated in different geographical locations around the world, it is crucial that the legal jurisdictions are honoured and followed. A potential research direction would be to find ways to store and process data in a way that does not breach the privacy and security laws of the region.

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 Security Symp. (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].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
[9] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ci-phertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59,2007
[10]Zhongma Zhu, Zemin Jiang, Rui Jiang, "The Attack on Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," Proceedings of 2013 International Conference on Information Science and Cloud Computing (ISCC 2013), Guangzhou, Dec.7, 2013, pp. 185-189.
[11]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.
[12]Xukai Zou, Yuan-shun Dai, and Elisa Bertino, "A practical and flexible key management mechanism for trusted collaborative computing," INFOCOM 2008, pp. 1211-1219.

BIOGRAPHY

Kishor Kumar is a Student(M.Tech) in the Computer science Department, Krishna Murthy institute of technology and engineering, Hyderabad. JNT University. He received his B.E(CSE) degree in 2014 from SJM institute of technology, Chitradurga.VTU Belgaum. His research interests are Computer Networks, Cloud computing, Algorithms, etc.