Secure and Reliable Data Sharing For Dynamic Group Members through Fine-Grained Access Control in Cloud Environment

[1] KORE LAKSHMI , [2] K .SIREESHA, [3] RAVI KUMAR TENALI

[1]M. Tech Student, Andhra Loyola Institute of Engineering and Technology, Krishna District, Andhra Pradesh, India

[2,3]Assistant Professor, Andhra Loyola Institute of Engineering and Technology, Krishna District, Andhra Pradesh, India

***Abstract*—** *The 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.*

***Index Terms*-- Cloud Computing, Security, Private Keys, Public Keys, Fine-Grained Access Control;**

I. INTRODUCTION

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.

Figure 1: Architecture of Cloud Computing

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. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud. 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. However, the file-block keys need to be updated and distributed for a user revocation; therefore, the system had a heavy key distribution overhead. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users. The 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. 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. However, the scheme will easily suffer from the collusion attack by the revoked user and the cloud. 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, and 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. 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 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

Many researchers have proposed stored encrypted data in the cloud to define against CSP. S. Kamara and K. Lauter 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. This 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 user’s access privileges. In encrypt-on-disk file systems, the clients encrypt all directories and their contents. This used a single key to encrypt an entire directory of files. Mahesha et al 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. 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. 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. 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 suffers from attacks, for example collusion attack, and this attack can lead to disclosing sensitive data files.

III. FRAME WORK

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. 5. This scheme provides a security analysis to prove the security of our scheme. In addition, it also performs 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. The below figure illustrated as 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.

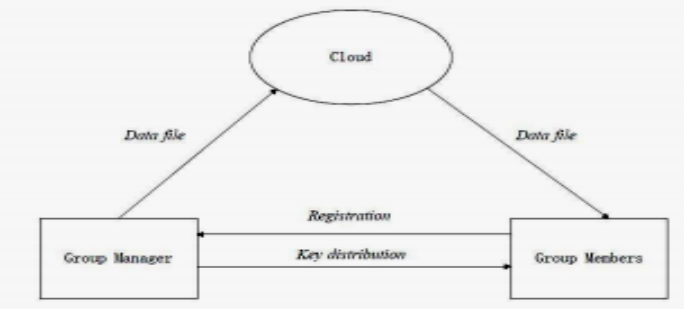
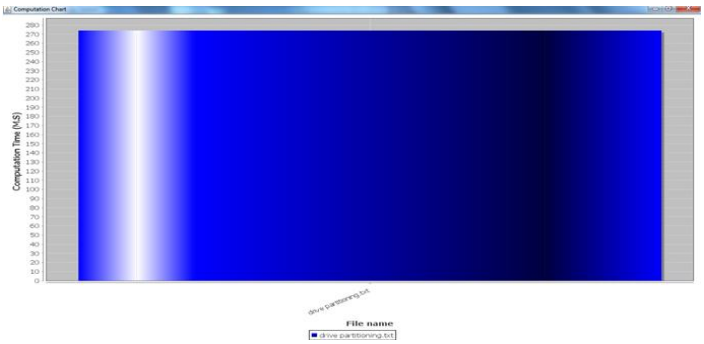


Figure 2: Architecture Diagram for Secured Anti-Collision Data Sharing

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

IV. EXPERIMENTAL RESULTS

In our experiments, any number of users registers into the system after successfully register into the system the group manager generate the secret keys for registered user after that authorized user can login into the system after login authorized user upload the file into the system after uploading the file that upload file user giving access permission through fine grained access control to other registered users, the file share into the those access permission users and file not share to the non-access permission users as well as user can revoke the access permission to the others. In the below chart we can observe that computation time



We can observe that computation chart the computation chart will be shown in the sense of Computation Time and File name. Through our implementation we have implemented an efficient data sharing scheme through fine-grained access control for dynamic members or groups and as well as revoking the users or members in dynamic groups through communication channels by using the scheme we can share the data in secure format with low cost.

V. CONCLUSION

In this paper, I design a secure data sharing scheme, for dynamic groups in an untrusted cloud. In this scheme a user is able to share data with others in the group without revealing identity privacy to the cloud. Secure policy supports efficient user revocation and new user joining. Efficient user revocation can be achieved through a public revocation list without updating the private keys of their users, and new users can directly decrypt files stored in the cloud before their participation. Extensive analyses show that the proposed scheme satisfies the desired security requirements and it guarantees efficiency as well.

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.

[13] 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, 2010, pp. 282–292.

[14] 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.

[15] 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.

Author1:

Mrs. K.SIREESHA Received her B.Tech degree in 2005 from Acharya Nagarjuna University,AP,India.Later in 2009,she received her M.Tech degree from JNTUH,Hyderabad.She has 8years of teaching experience and has published more than 6papers in national and international journals.She is pursing her PhD form K.L.University,Guntur.Her research interests include computer system ,networking ,wireless communications and networking ,network security and datamining, biometrics.she is currently working as Assistance professor in computer science and engineering department at Andhra Loyola Institute of Engineering and Technology vijayawada.

Author2:

Ms. K.LAKSHMI was born in potlapadu(v),AP on july 10, 1994 . graduated from NOVA college of Enginering and Tecnology under the Jawaharlal Nehru Technological University,kakinada . Her special fields of interest included Data mining and Image Networking. Presently She is studying M.Tech in Andhra Loyola Institute of Engineering and Technology, Vijayawada

.