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

[a]M. Mamatha, [b]K. Ramakanth
[a]M.tech, Department of CSE, Aurora's Scientific Technological and Research Academy, Bandlaguda, Hyderabad, 500005.
[b]Assistant Prof, Department of CSE, Aurora's Scientific Technological and Research Academy, Bandlaguda, Hyderabad, 500005.

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. Existing schemes, the security of key is based on the secure communication channel, but 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, users can securely obtain their private keys from group manager. Secondly, our scheme can achieve fine-grained access control, any user's 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.

KEYWORDS: Cloud Computing, Collusion, Data Sharing, Privacy Preserving, Key Distribution, Revoke

1. 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 .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. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud. Kallahalla et al presented a cryptographic storage system that enables secure data sharing on untrust worthy 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. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users. 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. 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. Lu et al proposed 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 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. Liuet al] present eda secure multi-owner data sharing scheme, named Mona. 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 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 et al presented 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, the scheme easily suffer from attacks, for example, collusion attack. Finally, this attack can lead to disclosing sensitive data files. Zou et al. presented a practical and flexible key management mechanism 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. Nabeeletal proposed a privacy preserving policy-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. 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.

2 THREAT MODEL, SYSTEM MODEL AND DESIGN GOALS

Given a keyword query q and an XML data T, our target is to derive top-k expanded query candidates in terms of high relevance and maximal diversification for q in T. Here, each query candidate represents a context or a search intention of q in T.

2.1 Threat Model

As the threat model, in this paper, we propose our scheme based on the Dolev-Yao model in which the adversary can overhear, intercept, and synthesis any message at the communication channels. With the Dolev-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.

2.2 System Model

System Model Cloud Group Manager Group Members Registration Key distribution Data file Data file as illustrated in figure 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.

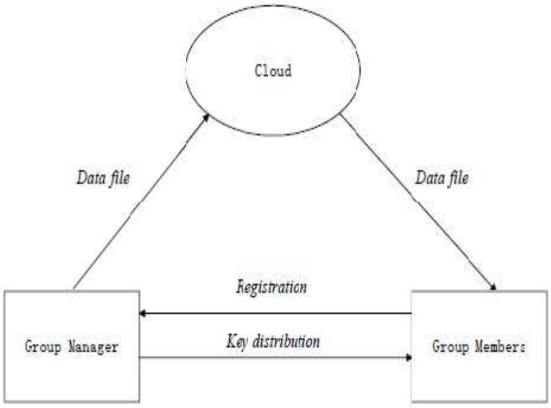

Figure 1

2.3 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 keys.

2.4 Scheme Description

The scheme of our scheme includes system initialization, user registration for existing user, file upload, user revocation, registration for new user and file download. The group manager takes charge of this operation. He generates a bilinear map group system then selects two random elements and a number then computes and At last, the group manager publishes the parameters where is hash function: is hash function: and is a symmetric encryption algorithm. This operation is performed by user, the group manager1http://www.ieee.org/publications_standards/publications/rights/index.html for more information. This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.

3 FILE UPLOAD

The operation of file upload is performed as illustrated. First of all, the group member chooses a unique data file identity and a random number then computes these parameters.

4 SECURITY ANALYSES

In this section, we prove the security of our scheme in terms of key distribution, access control and data confidentiality.

4.1 Key Distribution

Theorem 1: In our scheme, the communication entities can securely negotiate the public key *pk* and distribute the private key x *A B* to users without any Certificate

Authorities and secure communication channels. **Proof.** As illustrated in Figure 3, in the phase of user registration, the user sends his public key *pk* and a random number * the group manager with his identity *i ID* . Then the group manager computes corresponding value *U*,*R*.

Then the group manager can securely distribute the private key *KEY*, which is used for data sharing, to users with the help of negotiated public key and without any Certificate Authorities and secure communication channels. The correctness of the above verification equation is elaborated. In addition, our scheme can guarantee the user and the group manager to obtain the correct message which is sent by the legal communication entity. As illustrated in figure 3, in the third step of user registration, the group manager performs verifications after receiving the message from the user. First of all, he decrypts 1 , , *sk i AENC ID v ac* and obtains 1 , . *i ID v* Then he compares them with the received *i ID* message and the random number 1 *v* in the first step. If either of them is not equal, the manager stops the registration and informs the user to send new request in the third step. Moreover, the user sends a random number 2 *v* to the manager and the manager encrypts it with the public key *pk*. Therefore, the attacker cannot cheat the legal users and our scheme can be protected from replay attack.

4.2 Access Control

Theorem 2: Benefited from the group user list, which is generated by the group manager, our scheme can achieve efficient access control.
Proof: The access control is based on the security of the g.

5. PERFORMANCE EVALUATIONS

We make the performance simulation with NS2 and compare with Mona and the original dynamic broadcast encryption (ODBE). Without loss of generality, we set and the elements in and 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 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 2G, Ubuntu 12.04 X86. The cloud process is implemented on a laptop with Core i7-3630 2.4 GHz, DDR3 1600 8G, Ubuntu 12.04 X64. We select an elliptic curve with 160 bits group order. 160 2 G 16 2 As illustrated in figure 7, we list the comparison on computation cost of members for file upload among ODBE, RBAC, Mona and our scheme. It is obviously observed that the computation cost for members in our scheme is irrelevant to the number of revoked users. The reason is that in our scheme, we move the operation of user revocation to the group manager so that the legal clients can encrypt the data files alone without involving information of other clients, including both legal and revoked clients. On the contrary, the computation cost increases with the number of revoked users in ODBE. The reason is that several operations including point multiplications and exponentiations have to be performed by clients to compute the parameters in **ODBE.**

The computation cost of members for file download operations with the size of 10 and 100Mbytes are illustrated in figure 8. 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 computation cost in Mona increases with the number of revoked users, because the users need to perform computing for revocation verification and check whether the data owner is a revoked user. Besides the above operations, more parameters need to be computed by members in ODBE. On the contrary, the computation cost decreases with the number of revoked users in our scheme because of the computation for the recovery of the secret parameter decreases with the number of revoked users.

5.1 Cloud Computation Cost

As illustrated in figure 2, we list the comparison on computation cost of the cloud for file upload between Mona and our scheme. In general, it can be obviously seen that both the computation costs of the cloud in two schemes are acceptable. In detail, the cost in Mona increases with the number of revoked users, as the revocation verification cost increases. However, in our scheme, 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.

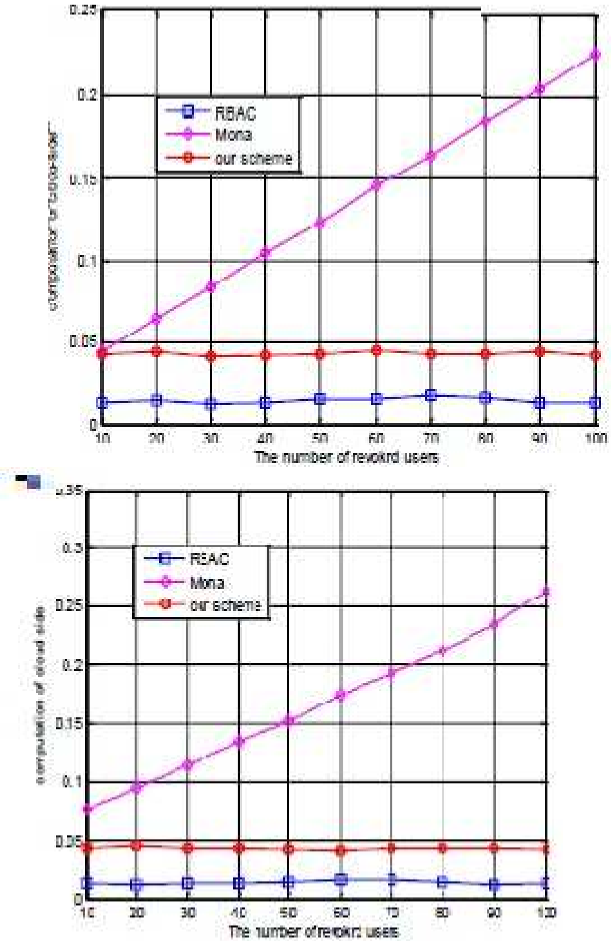

Figure 2

The computation cost of the cloud for file download operations with the size of 10 and 100Mbytes are illustrated in figure 10. Similar to the operation of file upload, the computation cost of the cloud is mainly determined by the revocation verification operation. Therefore, the cost increases with the number of revoked users.

However, in our scheme, the cloud just simply verifies the signature. Therefore, the computation cost of the cloud for file download is irrelevant to the number of the revoked users. The reason for the high computation cost of the cloud in RBAC scheme is that the cloud performs some algorithm operations to help the user to decrypt data files. In addition, it can be seen that in these schemes, the computation cost is independent with the size of the file, since both the signature in Mona and the encrypted message in our scheme are irrelevant to the size of the requested file and the operations of cloud for decryption in RBAC scheme is also irrelevant to the size of the encrypted data files.

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, 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 KeyCryptography*, 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 Identity Based Encryption 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, “Fully Collusion Secure Dynamic Broadcast Encryption with Constant-SizeCi-phertexts 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 of*2013 International Conference on Information Science and Cloud Computing (ISCC 2013)*, Guangzhou,Dec.7,2013,pp. 185-189.

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

[15] M. Nabeel, N. Shang, and E. Bertino, “Privacy preserving policybased content sharing in public clouds,”*IEEE Trans. on Know. andData Eng.*, vol. 25, no. 11, pp. 2602-2614, 2013.

[16] Dolev,D.,Yao A. C.,"On the security of public key protocols",*IEEE trans. on Information Theory*,vol. IT-29, no. 2, pp.198–208, 1983

[17] BonehDan, FranklinMatt, “Identity-based encryption from the weil pairing,”*Lecture Notes in Computer Science*, vol.2139 LNCS, pp.213-229, 2001

[18] B. den Boer, Diffie–Hellman is as strong as discrete log for certain primesin Advances in Cryptology–*CRYPTO88*, *Lecture Notes in Computer Science 403, Springer*, p.530, 1988.

[19] D. Boneh, X. Boyen, H. shacham, “Short group signature,” *Proc. Int’l Cryptology Conf. Advances in Cryptology*, pp.41-55, 2004.

[20] D. Boneh, X. Boyen, and E. Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext,” *Proc. Ann. Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT).*