ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Anti-Collusion Data Sharing Scheme in Cloud Computing

K.Mounika
M.Tech Student,
Department of SE,
Vidya Bharathi Institute of Technology,
Pembarthi, Jangaon.

B.Satyanarayana
Assistant Professor,
Department of SE,
Vidya Bharathi Institute of Technology,
Pembarthi, Jangaon.

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 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.

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.

System Model

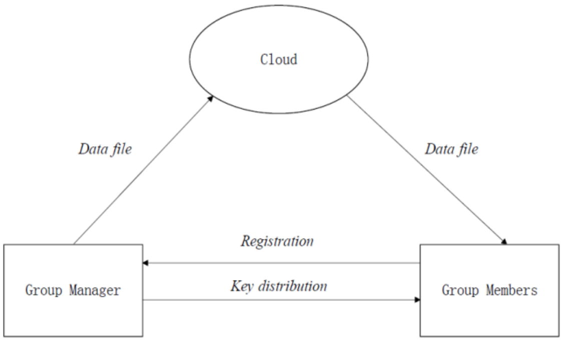


Figure 1 System model

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.

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.

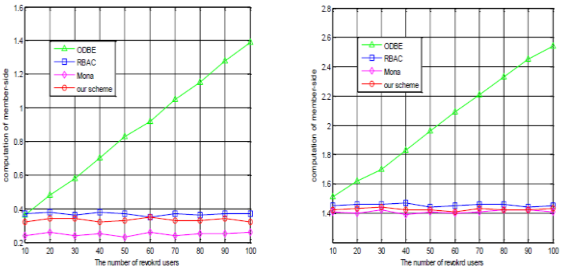
Data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. To maintain the availability of data confidentiality for dynamic groups is still an important and challenging issue. Specifically, revoked users are 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.

PERFORMANCE EVALUATION

We make the performance simulation with NS2 and compare with Mona in and the original dynamic broadcast encryption (ODBE) scheme. 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.

Member Computation Cost

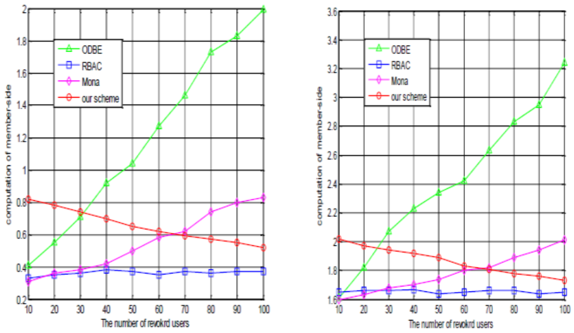


(a) Generating a 10 MB file (b) Generating a 100 MB file

Figure Comparison on computation cost of members for file upload among ODBE, RBAC, Mona and our scheme.

As illustrated in figure, 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.

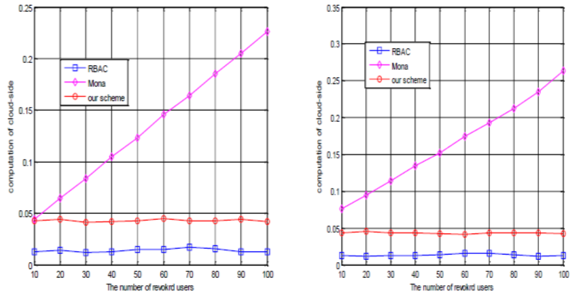


(a) Downloading a 10 MB file (b) Downloading a 100 MB file

Figure Comparison on computation cost of members for file download among ODBE, RBAC, Mona and our scheme

Cloud Computation Cost

As illustrated in below figure, 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.

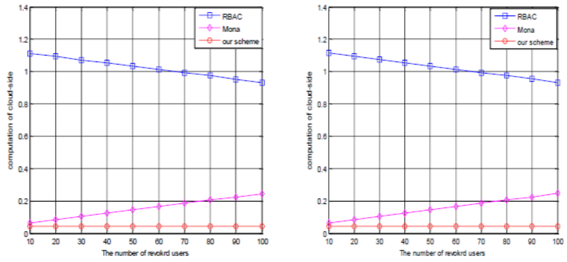


(a) Uploading a 10 MB file

(b) Uploading a 100 MB file

Figure Comparison on computation cost of members for file upload among RBAC, Mona and our scheme

The computation cost of the cloud for file download operations with the size of 10 and 100Mbytes are illustrated in below figure. 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.



(a) Downloading a 10 MB file

(b) Downloading a 100 MB file

Figure. Comparison on computation cost of the cloud for file download among RBAC, Mona and our scheme

CONCLUSION:

In this paper, we design a secure anti-collusion data sharing scheme for dynamic groups in the cloud. In our scheme, the user scan 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.

[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.