ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

Efficient Access and Revocation System for Dynamic Groups in the Cloud

[1] Dr.B R Prasad Babu, Prof.& head dept.cse [2] Kavya.H, [3] Nimisha Antony, [4] Sneha.P

***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. First, 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. Second, 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. Third, 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.

***Index Terms*— Access control, privacy-preserving, key distribution, cloud computing.**

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 [1]. 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 [2]. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud.

Kallahalla et al. [3] presented a cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into filegroups 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 in [4], [5].

However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users.

Yu et al. [6] exploited and combined techniques of key policy attribute-based encryption [7], 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. [8] proposed a secure provenance scheme by leveraging group signatures and cipher text-policy attribute based encryption techniques [9]. 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. Liu et al. [10] presented a 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 [13].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

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

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. [14] 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 See http:// www.ieee.org/publications_standards/publications/rights /index.html for more information. 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. [15] 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 te private key will be disclosed once the personal permanent portable secret is obtained by the attackers. Nabeel et al. [16] 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 haring 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. There voked 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 group sefficiently, 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. The remainder of the paper proceeds as follows. In Section 2, we describe the system model and our design goals. Our proposed scheme is presented in detail in Section 3, followed by the security analysis and performance evaluation in Section 4 and 5, respectively. Finally, the conclusion is made in Section 6.

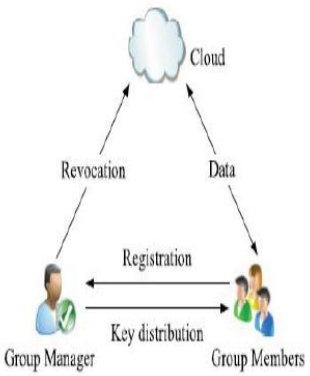
2 THREAT MODEL, SYSTEM MODEL AND DESIGN GOALS

2.1 Threat Model

As the threat model, in this paper, we propose our scheme based on the Delov-Yao model [17], in which the adversary can overhear, intercept, and synthesis any message at the communication channels. With the Delov-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

As illustrated in Fig. 1, the system model consists of three different entities: the cloud, a group manager and a large number of group members.



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 revocationcan be achieved without involving the others, which means that the remaining users do not need to update their private keys.

The cloud, maintained by the cloud service providers, provides storage space for hosting data files in

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

a pay-asyou-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.

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 hat 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

3. THE PROPOSED SCHEME

3.1 Preliminaries

3.1.1 Bilinear Maps
Let G1 and G2 be additive cyclic groups of the same prime order q [18]. Let e : G1*G1 G2 denote a bilinear map constructed with the following properties:
1) Bilinear: For all a,b € and P,Q € G1; e(αP,bQ) ( )
2) Non degenerate: There exists a point Q such that
E(Q;Q) ≠ 1.
3) Computable: There is an efficient algorithm to compute
E(P,Q) for any P;Q € G1.

3.1.2 Complexity Assumptions

Definition 1 (Basic Diffie-Hellman Problem (BDHP)Assumption [19]). Given base point P and a value ɣ.€ ,it is easy to compute ɣ . P: However, given P, ɣ P, it is infeasible to compute ɣ because of the discrete logarithm problem.

Definition 2 (Decisional Diffie-Hellman Problem (DDHP)Assumption [20]). Similar to definition 1, given base point P and aP; (a+ b)P; it is infeasible to compute bP.

Definition 3 (Weak Bilinear Diffie-Hellman Exponent(WBDHE) Assumption [21]). For unknown a € , givenY, aY, a2Y, . . . , alY; P € G1; it is infeasible to compute eðY; PÞ
1a
:

3.1.3 Notations

Each user has a pair of keys ðpk; skÞ; which is used in the asymmetric encryption algorithm, and pk needs to be negotiated with the group manager on the condition that no Certificate Authorities and security channels are involved in. KEY is the private key of the user and is used for data sharing in the scheme. UL is the group user list which records part of the private keys of the legal group users. DL is the data list which records the identity of the sharing data and the time that they are updated.

3.2 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.

Cloud module
Local Cloud gets created and provide priced abundant storage services. We develop this module, where the cloud storage can be made secure. It is possible to learn the content of the stored data and the identities of cloud users.

Group manager module
System parameters generation, User registration, User revocation, and Revealing the real identity of a dispute data owner.

Group member module
Such that registered users store their private data into the cloud server Share them with others in the group. 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.

File security module
Encrypting the data file.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).

Group signature module
A group signature scheme allows any member of the group to sign messages. Keeps the identity secret from verifiers. The designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

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

Security Comparison
In general, our scheme can achieve secure key distribution, fine access control and secure user revocation. For clearly seeing the advantages of security of our proposed scheme, as illustrated in Table 3, we list a table compared with Mona, which is Liu et al.'s scheme, the RBAC scheme, which is Zhou et al.'s scheme and ODBE scheme, which is Delerablee et al.'s scheme. The p in the blank means the scheme can achieve the corresponding goal.

Security Performance Comparison

	Secure key distribution	Access control	Secure user revocation	Anti-collusion attack	Data confidentiality
Mona		√			
RBAC scheme		√			
ODBE		√	√	√	
Our scheme	√	√	√	√	√

Performance evaluation
We make the performance simulation with NS2 and compare with Mona in [10] and the original dynamic broadcast encryption (ODBE) scheme in [12]. Without loss of generality, we set p ¼ 160 and the elements in G1 and G2 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 216 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 2 G, Ubuntu 12.04 X86. The cloud
process is implemented on a laptop with Core i7-3630 2.4 GHz, DDR3 1600 8 G, Ubuntu 12.04 X64. We select an elliptic curve with 160 bits group order.

Member Computation Cost
Asillustrated in 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 100 Mbytes are illustrated in . 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.

5.2 Cloud computation cost
As illustrated in we list the comparison on computationcost 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 numberof 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. The computation cost of the cloud for file download operations with the size of 10 and 100 Mbytes are illustrated in 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, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.

[4] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005, pp. 29–43.

[6] 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.

[7] 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.

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[9] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53–70.

[10] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

[11] 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.

[12] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size Ci-phertexts or decryption keys," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 39–59.