ISSN XXXX XXXX1 © 2017 IJESC

Research Article Volume 7 Issue No.6

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

Sandeep Sagar M[1], Vivek K M[2], Samarth M[3], Sanjay G S[4], Hemanth Kumar K[5]
B.E Students[1, 2, 3, 4], Assistant Professor[5]
Department of ISE
East West Institute of Technology, Bengaluru, India

Abstract:
The Benefited from Cloud Computing, clients can achieve a flourishing and moderate methodology for information sharing among gathering individuals in the cloud with the characters of low upkeep and little administration cost. Then, security certifications to the sharing information records will be given since they are outsourced. Horribly, due to the never-ending change of the enrolment, sharing information while giving protection saving is still a testing issue, particularly for an untrusted cloud because of the agreement attack. In addition, for existing plans, the security of key dispersion depends on the safe communication channel, then again, to have such channel is a solid feeling and is difficult for practice. In this paper, we propose a safe information sharing plan for element individuals. Firstly, we propose a safe route for key dispersion with no safe correspondence channels, and the clients can safely acquire their private keys from gathering administrator. Besides, the plan can accomplish fine-grained access control, any client in the gathering can utilize the source in the cloud and refused clients can't get to the cloud again after they are rejected. Thirdly, we can protect the plan from trickery attack, which implies that rejected clients can't get the first information record regardless of the possibility that they scheme with the untrusted cloud. In this methodology, by utilizing polynomial capacity, we can achieve a protected client denial plan. At long last, our plan can bring about fine productivity, which implies past clients need not to overhaul their private keys for the circumstance either another client joins in the gathering or a client is give up from the gathering.

Keywords: Access Control, Privacy-Preserving, Key Distribution, Cloud Computing.

I. 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. 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 fileblock 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 finegrained data access control without disclosing data contents without any Certificate Authorities due to the verification for the public key of the user.

- Our scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can

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. 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:

- We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager use the source in the cloud and revoked users cannot access the cloud again after they are revoked.
- 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.
- 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.
- We provide security analysis to prove the security of our scheme. In addition, we also perform simulations to demonstrate the efficiency of our scheme.

II. EXISTING AND PROPOSED SYSTEMS

A. Existing System

- Kallahalla et al presented 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.
- Yu et al exploited and combined techniques of key policy attributebased encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents.

B. Proposed System

In this paper, we propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. 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 as shown in Fig.1. Our scheme can achieve finegrained 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. 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. 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. We provide security analysis to prove the security of our scheme.

Advantages of Proposed System:

- 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 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.
- 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.

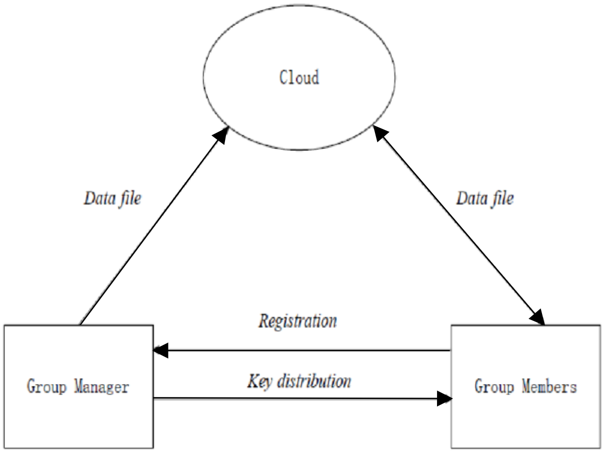


Fig.1. System Architecture

III. SYSTEM MODEL

A. Threat Model

In this paper, we propose our plan taking into account the Dolev-Yao model, in which the attacker can catch, capture and combination any message at the correspondence channels with the Dolev-Yao model, the best way to protect the data from attack.

B. System Model

Here the proposed model is illustrated in Fig.1; the system model consists of three different entities: the cloud, a group manager and a large number of group members. The cloud, sustaining by the cloud service providers, provides storage space for hosting data files in a pay-as-you-go manner. on the other hand, 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 will obtain charge of system parameters generation, user registration, also, client repudiation. Bunch individuals (clients) are an arrangement of sign up clients that will store their own particular information into the cloud and impart them to others. In the plan, the gathering enrollment is powerfully changed, because of the new client call-up and client denial.

C. Design Goals

We depict the principle plan objectives of the proposed plan including key circulation, information secrecy, access control and effectiveness as takes after:

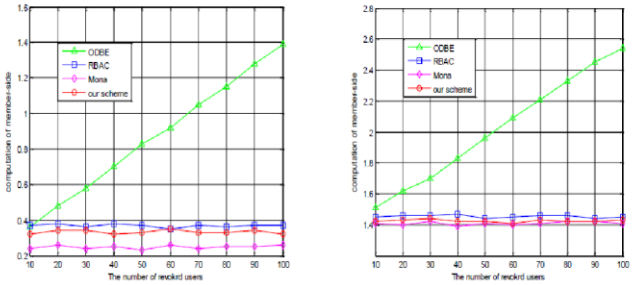
- **Key Distribution:** The prerequisite of key transportation is that clients can safely get their private keys from the gathering director with no Certificate Authorities. In other existing plans, this purpose is skilful by expecting that the communication channel is secure, on the other hand, in our plan, we can accomplish it without this solid thought.
- **Access Control:** First, collect individuals can make use of the cloud asset for information stockpiling and information sharing. Second, unapproved clients can't get to the cloud asset whenever, and disavowed clients will be unfitted for utilizing the cloud asset again once they are renounced.
- **Information Classification:** Data secrecy requires that unapproved clients including the cloud are unequipped for taking in the substance of the put away information. To keep up the accessibility of information secrecy for element gatherings is still an essential and testing issue. In particular, renounced clients can't unscramble the put away information document after the denial.

  Effectiveness: Any gathering part can store and impart information records to others in the gathering by the cloud. Client repudiation can be accomplished without including the others, which implies that the remaining clients don't have to overhaul their private keys.

IV. PERFORMANCE EVALUATION

We make the performance simulation with NS2 and compare with Mona in [11] and the original dynamic broadcast encryption (ODBE) scheme. Without loss of generality, we set p =160 and the elements in G_1 and G_2 to be 161 and 1,024 bits, respectively. In addition, we assume the size of the data identity is 2^{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. A. Member

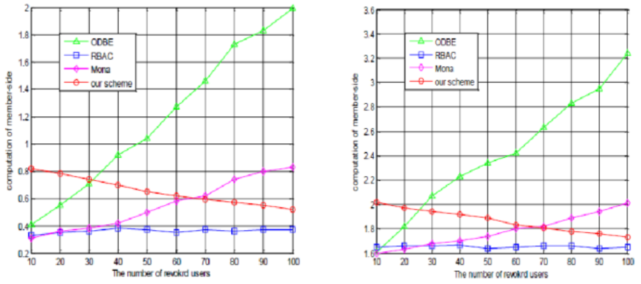
Computation Cost



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

Fig.2. Comparison on computation cost of members for file upload among ODBE, RBAC, Mona and our scheme

As illustrated in Fig.2, 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 Fig.3. 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.

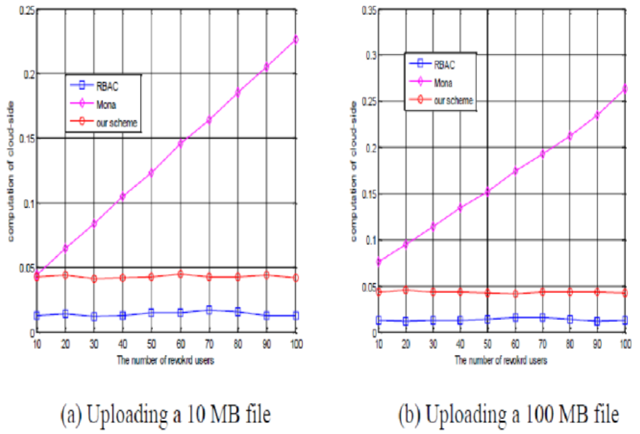


(a) Downloading a 10 MB file (b) Downloading a 100 MB file

Fig.3. Comparison on computation cost of members for file download among ODBE, RBAC, Mona and our scheme.

B. Cloud Computation Cost

As illustrated in Fig.4, 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

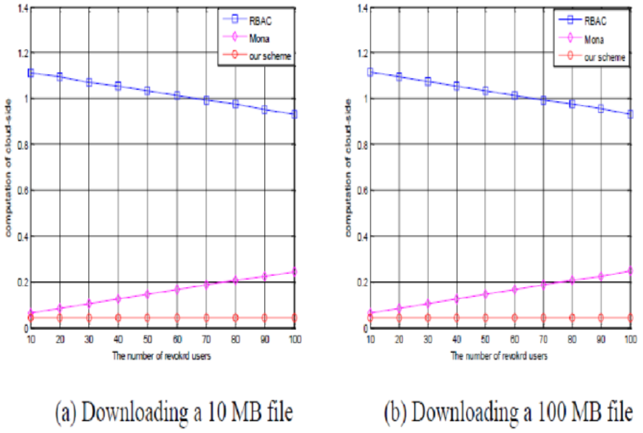


(a) Uploading a 10 MB file

(b) Uploading a 100 MB file

Fig.4. 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 Fig.5. 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 in this scheme.



(a) Downloading a 10 MB file

(b) Downloading a 100 MB file

Fig.5. Comparison on computation cost of the cloud for file download among RBAC, Mona and our scheme

V. CONCLUSION

In this paper, we outline a protected against agreement information sharing plan for element bunches in the cloud. In our plan, the clients can safely acquire their private keys from gathering director Certificate Authorities and secure correspondence channels. Likewise, our plan can bolster dynamic gatherings proficiently, when another client joins in the gathering or a client is denied from the gathering, the private keys of alternate clients don't should be recomputed and redesigned. In addition, our plan can accomplish secure client repudiation, the disavowed clients can not have the capacity to get the first information records once they are denied regardless of the possibility that they plot with the untrusted cloud.

VI. FUTURE ENHANCEMENTS

As we are sending the private keys to the person's email id, now we are planning to send the private keys to their registered mobile number.

We will send notification message to the group manager whenever a new person registers or the existing person revokes from the group.

We are planning to keep the working of the project dynamic.

We can use the latest and more secure algorithms to encrypt the files in the coming future.

REFERENCES

[1] Zhongma Zhu, Rui Jiang,"A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", IEEE Transactions on Parallel and Distributed Systems, 2015.

[2] 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.

[3] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp.136- 149, Jan. 2010.

[4] 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.

[5] [5]EGoh, H.Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131145, 2003.

[6] 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.

[7] 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.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "AttributeBased Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006

[9] 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.

[10] B.Waters, “Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,” Proc. Int’l Conf. http://eprint.iacr.org/2008/290.pdf, 2008

[11] 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. 11821191, June 2013.

[12] 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.