A Secure Data Sharing Scheme for Dynamic Groups in the Cloud

Sampath Kumar Tatipally[1], Dr. K.Shahu Chatrapathi[2]
Department of CSE
[1]M.tech,School Of Information Technology (JNTUH), Village Kukatpally, Dist Ranga reddy, Telangana, India.
[2] Professor,School Of Information Technology (JNTUH), Village Kukatpally, Dist Ranga reddy, Telangana, India.

Abstract-*One of the most important feature of cloud computing is user can achieve an economical and effective approach of data sharing among group of people in the cloud with minimum maintenance and with little management cost. And the cloud servers must provide security guarantees for the shared data files since they are outsourced. Regrettably, because the user changes frequently, privacy- preservation is still a challenging issue for sharing data, especially for an untrusted cloud. Moreover, in the present existing schema, the security of key allocation is depended on the secure connection channel, conversely having that type of secure channel is strong assumption and it is difficult to practice in real time. In this paper I would like to propose a secure data sharing schema for dynamic users. In this paper first I propose a secure way to distribute key without using any secure communication channel, and the member can get their private key securely from group manger. Second, through my schema we can achieve fine grained access control, any member of the group can access the source in the cloud and the users can revoke only once, a revoked user cannot access the cloud again after they are revoked. In the final step we protect the scheme from the collusion attack, which means that the revoked user will not get the original data even if they are scheme with the untrusted cloud. In our loom, we can achieve a secure revocation schema by leveraging the polynomial function. Finally, our technique can accomplish fine efficiency, which means that there is no need of updating the private key of the old users when a new users join the group or a user revoke from the group.*

I. INTRODUCTION

Cloud computing, with the characteristics of low maintenances and cloud data sharing, it provides a better utilization of resources. The cloud server provides a infinite storage of data for clients to host the data. It is very help full to the organization through cloud storage they can reduce the financial overhead on data management by migrating the local organization system into the cloud servers.

On the other hand, security concerns turn into the main limitation as we now outsource the storage of data, which is maybe sensitive, to cloud providers. We can achieve the data privacy by a common approach by encrypting the data before the client upload the data to the cloud. But it is difficult to design effective and secure data sharing scheme, for dynamic group in the cloud.

Kallahalla et al designed a new cryptography storage system which is used to secure the data sharing in the untrusted servers by a technique that divided the file block into group and encrypt each file block with a file block key. And the file block key need to be updated for each user revocation, because of this the system has heavy key distribution. The complexity of users revoked and number of participates in this schema increases with the number of revoked user and the data owners.

Yu et al. exploited a combination technique of key policy proxy re encryption, attribute based encryption and lazy re encryption these are proposed to achieve fine grained data access without disclosing any data contents. The single owner manner may delay the execution of application, where the cloud data can be shared and stored by any member of the group.

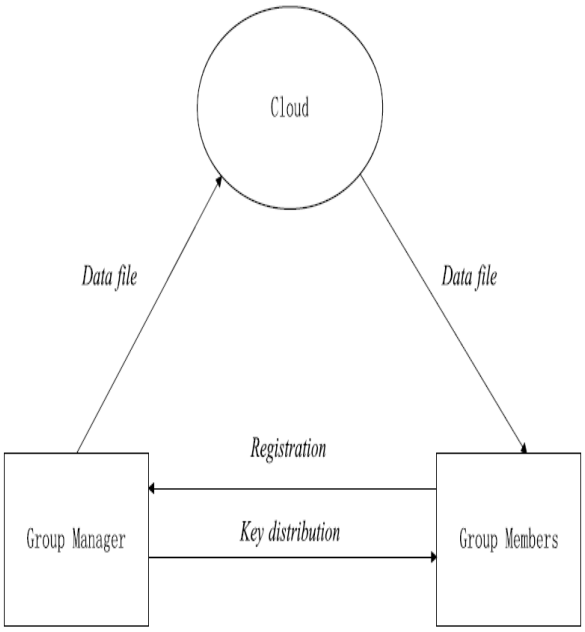
Lu et al. proposed a secure attribution scheme by leveraging ciphertext-policy attribute based encryption and group signatures technique. In this technique the user obtains two key after registration while the data is decrypted using the attribute key which is encrypted by the attribute based encryption and the group of signature key is used for traceable and privacy preserving. In this technique revocation is not possible.

Liu et al in his paper he proposed a secure multi owner data sharing technique named mona. It is claimed that it can achieve fine grained access control and in this scheme if a user is revoked once then they will not be able to access the shared data again. But this scheme can be easily collusion attacked by the revoked user and the cloud. The revoked user can get the encrypted data by using this secrete key after revocation by conspiring with the cloud. In the phase of file access, first of all, the revoked user sends his call for to the cloud, then the cloud responds to the consequent 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.

Zhou et al also proposed a scheme of secure access control of the encrypted data in the cloud by using invoking role based technique. It is also claimed that by using this scheme we can achieve efficient user revocation that combine combines role based Access control policies with encryption to secure large data storage in the cloud. Regrettably, the verifications between entities are not anxious, the scheme easily suffer from attacks. 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



As show in the figure 1 the system model consist of three entities, group member, cloud, group manager.

In this model the cloud is maintained by the cloud server providers, who provides storage for the user to host there data in a pay as you use manner. Since the cloud servers providers are untrusted easily then easily the cloud will become untrusted. Therefore the cloud will try to study the substance of the stored data.

The cloud manager deals with the system parameters generation and user registration the manager itself take charge of the relocation. In the cloud application the cloud manager is the leader of the particular cloud group. Therefore the cloud manager is must be trusted all other parties of the group.

Group members are the users of the cloud they are registered by the cloud group manager to store their own data into cloud and to share that data. In this scheme the user membership is dynamically changed, when a new user is registered and a old user is revoked.

III. THREAT MODEL

As the threat model, in this paper, we intend our scheme based on the Delov-Yao model , in which the rival can overhear, synthesis, and intercept any message at the communication channels. With this model, there is only one way to defend the information from attacking by the passive eavesdroppers and active saboteurs is to propose the effectual security protocols. That means there should not be any secure communication channel between the entities. So, this kind of threaten model can be more practical and effective to show the communication in the real world.

IV. DESIGN MODEL

There are three main design goals for this scheme they are key distribution, access control, data confidentiality and efficiency as follows

Key distribution the necessity of this key distribution is that the user an obtain his private key without any certificate authority from the group manager. In the present existing system this is done by assuming that the channel of communication is secured, but in this paper we can achieve without any strong assumption.

Access control only the group members can access the cloud to store and retrieve the particular data from the cloud. The unauthorized users cannot use the cloud to store or retrieve the information from the cloud. The revoked user will be incapable once they are revoked from the cloud group

Data confidentiality data confidentiality Data confidentiality needs that illegal users together with the cloud are inept of erudition the content of the stored data. To preserve the availability of data confidentiality for dynamic groups is still an imperative and challenging issue. Particularly, revoked users are unable to decrypt the stored data file after the revocation.

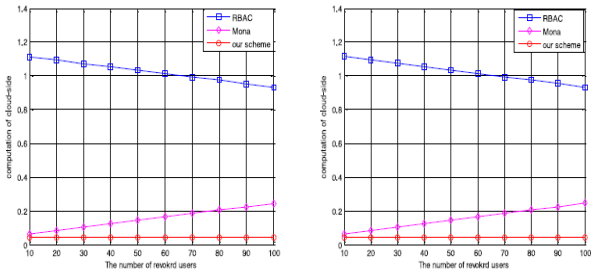
Efficiency any of the group member can store the data with other group members and they can share the data between the group members. The user revocation can be achieved without any involvement of other users. The other users need not need to update their private key revocation is not depended on the other users

V. THE PROPOSED SYSTEM

Notations Each user in the group has two pairs of keys (pk,ak), which is used for asymmetric encryption algorithm, and pk must be derelict by the group manager on a condition of that no security channel and certificate authority involved in.

5.1 Scheme Description

This scheme includes system initialization, user registration, file upload, user revocation, registration for new users. System initialization in done by the group manager, registration for the existing user this operation is done by the user, group manager and cloud. First the user send the request and on receiving the request the group manager register for the existing user. User revocation is done by the group manager and the cloud when a user is revoked from the group his identity is removed from the group and then he checks the group for the revoked user then he conforms there is no revoked user. Then the group manager selects a new random re encryption key and constructs the new key. Registration for the new user in this process also we follow the same process. File download this operation is done by the group members and the cloud any one of the group can upload the file and any member of the group can download the file.



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

Fig 2 Comparison on computation cost of the cloud for file download among RBAC, Mona and our scheme

VI. CLOUD COMPUTATIONAL COST

As shown in the fig 2, we have given the computation cost of cloud for upload a file to the cloud. For file upload between Mona and our scheme. It can be observed that both scheme computation cost is acceptable. In detail the computation cost increased as number of revoked users increased as they verify the revoked user conversely, in our scheme, the cost is unrelated to the number of the revoked users. So the computation cost is not effected on number of revoked.

VII. CONCLUSION

In this paper I have designed a anti collusion data sharing for the dynamic group in the cloud. In our cloud scheme the user can get the private key from the group manager without any secure communication and certificate authorities. And our scheme work efficiently for the dynamic cloud even when a new user joins the group or a user is revoked form the group the private keys need not to be computed and updated because its is independent to the revoked the user, 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, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[2] 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.

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

[4] 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.

[5] 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.

[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] 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.

[8] 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.