ISSN 2395-1621

A Novel Secure Group Sharing Framework For Public cloud

[#1]Sandhya Chavare, [#2]Prof.Deepak Uplaonkar

[1]Sandhya.chavare@gmail.com

[#12]Computer Engineering Department, Pune University
JSPM NTC, India

ABSTRACT

In public cloud computing, services have appeared for data sharing in group application. The privacy and security are the main issues that arises when sharing group data in public cloud. Due to the semi-trust nature of the third party, the cloud provider cannot be treated as a trusted third party .Therefore security models used traditionally cannot be directly applied to the framework of cloud based group sharing. We propose a novel secure group sharing framework for public cloud. This framework is created by combining Proxy signature, enhanced TGDH and proxy re-encryption together into protocol. The group leader can grant privilege of group management to one or more chosen group member by adopting proxy signature scheme. By using the enhanced TGDH scheme with the help of cloud servers enables the group to update and negotiate group key pairs thus all group members need not to be online all the time. By using proxy re-encryption most of intensive operations which are to be performed computationally can be handed over to the cloud servers without leaking of any private information. Our proposed scheme shows security and performance analysis.it is highly efficient and satisfies the security requirements for public cloud based secure group sharing.

Keywords— Secure group sharing, forward secrecy, backward secrecy, public cloud computing, group key agreement, TGDH(Tree-based Group Diffie-Hellman).

ARTICLE INFO

Article History

Received :24th December 2015

Received in revised form :

26th December 2015

Accepted: 29th December , 2015

Published online :

30th December 2015

I. INTRODUCTION

With the development of cloud services and social networks, a group can be easily organized between some people over Internet due to the same interests, so that group applications with the aid of cloud servers become possible and attract more and more attentions. Cloud computing is recognized as an alternative to traditional information technology due to its in-trinsic resource-sharing and low-maintenance characteristics. Data storage and high performance computation are the main needs which have to be fulfilled. Many cloud computing service providers have to provide data storage in cloud. When group data is stored in the cloud , the data owner can share their data with the desired members in the group. The cloud is managed by cloud service provider. Due to semi-trust nature Cloud service provider cannot be treated as trusted. Finally, traditional security storage
technologies cannot be directly applied in the public cloud storage application The cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. So valid users can download and decrypt the file. But the session key updating and distribution is a major problem. Another method is the use of Digital Envelope. In these methods, the computing and communication overhead of digital envelopes generation and the computational and communication overhead of session key updating are major problems. The efficiency of these schemes depends on the fact that cloud servers should be trusted otherwise they can launch the collusion attack with some leaving group members. The normal group application plan in cloud can be formed as follows. The group leader in the cloud to form a group application.

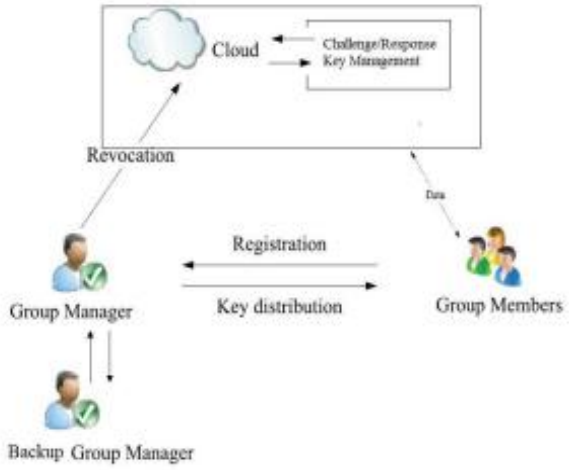

Fig.1 System architecture.

1.Group Leader

The group leader opens up a sharing area in the cloud to form a group application. Then, he/she grants the group members the right to implement data management. All the data in this group are available to all the group members, while they remain private towards the outsiders of the group including the cloud provider. The group leader can authorize some specific group members to help with the management of the group, and this privilege can also be revoked by the group leader. When a member leaves the group, he/she will lose the ability to download and read the shared data again.

2.Admin Authentication

The group leader can authorize some specific group members to help with the management of the group, and this privilege can also be evoked by the group leader. And the Admin can accept the New user request.

3.Group Member

Each group member can implement file download and upload operations in the authenticated group. Each *GM* can get some related public information from Cloud Servers and compute the specific set of security parameters, such as group key pair.

II. LITERATURE SURVEY

K. Ren, C. Wang, and Q. Wangpresents [1] Authorized users can download the encrypted files and decrypt them with the given keys. But in this scenario, how to distribute and update session keys is one of the most important but hard problems. Digital Envelope is used to address this task in : the data is encrypted with a randomly chosen session key by using symmetric encryption, and then the session key is encrypted with the public key of the specific user by using public-key encryption.

P. Tysowski and M. Hasan[4] works on the privacy preserving data sharing issue in cloud based on various cryptographic tools, such as attribute based encryption (ABE), proxy re-encryption.

The efficiency of Yu et al.'s scheme [2] relies on that there is high attribute variability between different files and high attribute variability between different users. But in group applications, different group members usually have same or similar interests, and they usually have attributes in common between them. In the scenario of interest based group sharing, if using Yu et al.'s scheme, the communication and computing overhead of user revocation will be dependent on the size of the group.

The efficiency of the scheme in[3] depends on the assumption that cloud servers must
be absolutely trusted. Otherwise, cloud servers can launch the collusion attack with some curious leaving group members.So, in order to protecting files from the prying eyes of curious cloud servers and leaving group members, the data owner needs to re-generate his key pairs and re-generate N _ 1 proxy-re-encryption keys when revoking a group member. This computing overhead is very high for the data owner, especially in the scenario of user joining and leaving
frequently in the group.

The paper scheme should satisfy the security requirements of backward secrecy and forward secrecy. The former one ensures that the revoked user cannot decrypted new ciphertexts. The later one ensures that the newly joined user can also access and decrypt the previously published
data. This two security requirements are usually used in some cloud based data sharing scenarios, such as[6].
A potential adversary may be a former group member or any one out of the group. This paper assume that an adversary can be a passive attacker who could be a man-in-the-middle to monitor the communications among the group members and cloud servers. A former group member can collude with cloud servers and try to access data contents shared in his/her former group. An active adversary is able to impersonate an legitimate group member to gain some right.

III.PROSED WORK

Our work gives the extension to it to make more operability when any member online or offline at any time. In this system, based on Cloud Servers' help, Group members can implement key synchronization when they become online in the next time.

1) The proposed scheme supports the updating of the group key pair whenever group members' joining or leaving happens, which transfers most of the computational complexity and communication overhead to Cloud Servers without leaking the privacy.

2) Privilege of group management can be granted to any specific group member, which can be revoked at any time.

3) Enhanced on the original TGDH, with the help of Cloud Servers, the proposed scheme enables the group to negotiate and update the group key pairs even though not all of the group members are online together.

Any offline group member can launch group key synchronization when he/she becomes online again in the next time.

Advantages

- Extensive security and performance analysis shows that our proposed scheme is highly efficient and satisfies the security requirements for public cloud based secure group sharing.
- A novel secure group sharing framework for public cloud, which can effectively take advantage of the Cloud Servers' help but have no sensitive data being exposed to attackers and the cloud provider.

IV. ALGORITHM

This algorithm shows that to calculate the security key after entering and leaving group member from group.

initialize SK(i) = ki, a privately generated key
calculate PK(i) = GEN(SK(i))
transmit signed = PK(i) to central authority
receive list of authenticated participants from central authority
for r = 1 ::: log2n
let g = G(i; r)
calculate PK(i) = GEN(SK(i))
if (i == C(g; r)) then
transmit PK(i)
endif
receive Y = PK(P (g; r)) from partner and checks identity
calculate SK(i) = T P (SK(i); Y)

V. CONCLUSION

A novel secure group sharing framework is designed for secure data sharing.The management of secure group sharing can be given to various group members. All the data or files to share are securely stored and protected in the cloud servers. Enhanced on the original TGDH enables the group to negotiate and update the group key pairs even though not all of the group members are online together. As all the group members are online at different time still the system works well. It also supports efficient user revocation and new user joining. To achieve the design of the goal the system the security and performance analysis of the system do well, it becomes less complex and communication becomes easy.

VI. REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012.
[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable,and fine-grained data access control in cloud computing," in Proc.IEEE 29th Conf. Comput. Commun., 2010, pp. 534–542.
[3] W. Jia, H. Zhu, Z. Cao, L. Wei, and X. Lin, "SDSM: A secure data service mechanism in mobile cloud computing," in Proc. IEEE Conf. Comput. Commun. Workshops, 2011, pp. 1060–1065.
[4] P. Tysowski and M. Hasan, "Hybrid attribute-and re-encryptionbased key management for secure and scalable mobile applications in clouds," IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 172– 186, Jul.–Dec. 2013.
[5] Y. Kim, A. Perrig, and G. Tsudik, "Tree-based group key agreement," ACM Trans. Inf. Syst. Security, vol. 7, no. 1, pp. 60–96, 2004.
[6] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in Proc. 10th Int. Conf. Trust, Security Privacy Comput. Commun., 2011, pp. 91–98.
[7]. K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proc.IEEE Conf. Comput. Commun., 2013, pp. 2895–2903.
[8]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.
[9]. Z. Wan, J. Liu, and R. Deng, "HASBE: A hierarchical attributebased solution for flexible and scalable access control in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.
[10]. L. S. Lai and E. Turban, "Groups formation and operations in the web 2.0 environment and social networks," Group Decision Negotiation, vol. 17, no. 5, pp. 387–402, 2008.
[11]. W. Yu, Y. Sun, and K. R. Liu, "Optimizing the rekeying cost for contributory group key agreement schemes," IEEE Trans. Dependable Secure Comput., vol. 4, no. 3, pp. 228–242, Jul.–Sep. 2007.
[12]. D. Boneh, "The decision Diffie-Hellman problem," in Proc. 3rd Algorithmic Number Theory Symp., 1998, pp. 48–63.

