Sharing Secure Data in The Cloud To Multiple users Among a Dynamic Group

Mahesh A.
Department of Computer Science and Engineering
Jain Global Campus, Jain University, Jakkasandra Post
Kanakapura Taluk, Ramanagara District-562112

S. Balaji
Centre for Emerging Technologies
Jain Global Campus, Jain University, Jakkasandra Post
Kanakapura Taluk, Ramanagara District-562112

Abstract: **Cloud computing provides an economical and efficient solution for sharing group resources among cloud users. When sharing the data in a group while preserving data, identity privacy is still a challenge because of frequent changes in the membership. To overcome this problem, a sharing secure data scheme among multiple users among a dynamic group is proposed so that any user within a group can share the data in a secure manner by leveraging both the group signature and dynamic broadcast encryption techniques. It enables authorized users to anonymously share data with others within the group. It supports efficient member revocation and new member joining the group. User revocation list is performed by group manager and it is given to the cloud service provider to check the active users within the group before giving access to the cloud.**

Keywords: Cloud, Data Sharing, Dynamic Groups, Revocation List

1. INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and characteristics of low-maintenance. In cloud computing, many computing resources are provided as services over the Internet. One of the main services provided by cloud is storage, which allows users to upload and store their data in the cloud. Storing data in cloud provides many advantages such as reliability and availability, but it also brings many other challenges such as secure data sharing.

An organization allows its group members to store and share their data files by utilizing the cloud. Group members can be completely relieved from local data storage and maintenance, but significant risk arises in confidentiality of those stored files. The cloud users are not fully trusted since the cloud servers are operated by cloud service providers. Confidentiality of the data is very important because of the sensitive data stored in the cloud. To preserve the data confidentiality, a basic solution is to encrypt data files and then upload the encrypted data into the cloud.

Firstly, identity privacy is one of the major issues in cloud. Without the identity privacy, users are not willing to join the cloud because their real identities could be easily disclosed to cloud providers and attackers.

Secondly, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined in the multiple-owner manner. Compared with the single-owner manner, where only the group manager can store and modify data, in multiple-owner manner each user in the group is able to not only read the data but can also modify the part of data in the entire data file shared by the users.

Thirdly, groups are normally dynamic in practice. It does not support new user participation and current employee revocation within the group. So the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users.

Lastly, group owner must be able to trace if any disputes occurs within the group.

2. RELATED WORK

Junod and Karlov [1], propose a "CP-ABE based broadcast encryption" scheme that supports direct user revocation. In this scheme, each broadcast receiver's identity is mapped to an individual attribute. The access policy consists of a set of system attributes with a set of identity attributes. Individual user revocation is achieved by updating the set of identity attributes in the access policy.

B. Wang et. al. [4], focuses on "cloud computing and storage services". Accordingly, cloud data is not only stored in the server, but routinely shared among a large number of users in a group. In this paper, the authors propose Knox, a privacy-preserving auditing mechanism for data stored in the cloud and shared among a large number of users in a group.

S. Yu, C. Wang, K. Ren, and W. Lou [6] present a "scalable and fine-grained data access control" scheme in cloud computing based on the Key Policy Attribute Based Encryption (KP-ABE) technique. In this scheme, the data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Then, the group manager assigns an access structure and the corresponding secret key to authorized users such that a user can decrypt a cipher-text if and only if the data file attributes satisfy the access structure

Kamara et. al. [10] propose a framework of a "Cryptographic Storage Service (ACSS)" which considers

the issue of building a secure cloud storage service on cloud infrastructure where the service provider is not fully trusted by the user. It is made up of three basic components (DP, DV, TG) and realizes encryption storage and integrity validation by a group of protocols. However, ACSS is hard to build since it deals at a high level and requires modification of large amount of source code of cloud storage platform.

3. PROPOSED SCHEME

The proposed scheme is to secure the data against unauthorized access by enforcing access control mechanisms. To achieve secure data sharing for dynamic groups in the cloud we combine both the group signature and dynamic broadcast encryption techniques. The short group signature introduced by Chaum and van Heist is used, which enables any users in a group to anonymously use the cloud resources provided by cloud service provider. It supports efficient user revocation and provides secure and privacy-preserving access control to users that guarantee any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur within the group using the group signature. Group manager will have the list of active users and also maintains the list of revoked users. Only the members of the group can create valid group signatures. Figure1 shows how the group members register with the group owner and how the data is shared among the group members from the cloud server.

The dynamic broadcast encryption is another technique which allows data owners to securely share their data files with other users in the group including newly joined users. It supports new member joining the group without updating private keys of remaining users in the group.

The Dynamic broadcast encryption allows broadcaster to distribute the data only to set of users who requested the data and each user has to compute revocation parameters to protect the confidentiality of the data from the revoked users. The dynamic broadcast encryption scheme is used such that revoked users cannot access the data once they are revoked from the group. Group manager can enable the revoked users to rejoin the group again. The group manager is allowed to compute the revocation parameters, which includes the list of revoked users and make this revocation list available to public by migrating them into the cloud. Each time when users request for data, cloud service provider verifies the revocation list and then provide access to data only to active users in the group. Such a design significantly reduces the computation overhead.

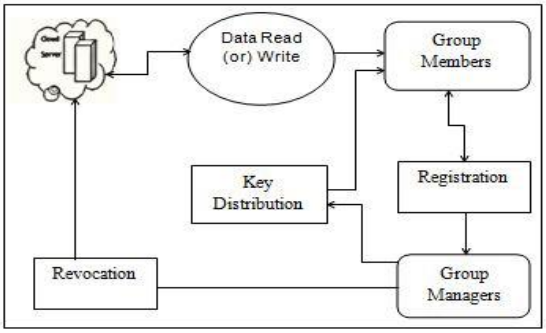

Figure 1: System Architecture

Group manager takes charge of system initialization, signature generation, user registration, user revocation, and revealing the real identity of a user when the dispute occurs.

Data files are encrypted using key policy attribute based encryption. Private and public keys are generated by the users. Public key for encrypting the data and private key is kept secret and is used for decrypting the data files.

The proposed scheme also supports new member joining the group and user revocation from the group. User revocation is performed by the group manager via a publicly available Revocation List (RL) without updating the private keys of remaining users. Each user must follow the revocation parameters before revoking from the group.

4. ALGORITHMS USED

The algorithms used in the proposed system are as follows:

Algorithm 1: Signature Generation

This algorithm is used to generate the signature for the members in the group, through this group signature users are allowed to login into the group.

Step1: start
Step2: Input: Private Key (Ai, xi), system parameter (P, U, V, H, W) and data M.
Step3: Output: Generate a valid group signature on M.
Step4: begin
Step5: Select random numbers Set (t1, t2, t3, r1, r2, r3)
And set x1=a and x2= b
Step6: Compute the following values t, t2, t3, r1, r2, r3.
Step7: compute the challenging c
c<- h (m, t1, t2, t3, r1, r2, r3, r4, r5) using Hash function.
Step8: using c construct the Values s, s2, s3, s4, s5
Step9: Output the signature computed as gsp<-(t1,t2,t3,c,s1,s2,s3,s4,s5)
Step10: stop.

Algorithm 2: Signature Verification

Algorithm 2 is used to verify the group sign and individual user sign during the data sharing from the cloud server.

Step1: start
Step2: Input: System Parameter (P, U, V, H, W),M and a Signature
Step3: σ = (T1, T2, T3, c, sα, sβ, sx, sδ1, sδ2)
Step3: Output: True or False.
Step4: Begin
Compute the following values
R1 = sα. U – c. T1
R2 = sβ. V – c. T2
R3 = (e(T3,W)/e(P,P))c e(T3,P)s
x e(H,W)
R4= sx .T1 - sδ1 .U
R2 = sx .T2 - sδ2 .V
Step5: if c = f(M, T1, T2, T3,R1, R2, R3, R4, R5)
Step6: Return True
Step7: Else
Step8: Return False
Step8: End.

Algorithm 3: Revocation Verification

This algorithm is used to verify active users in the group. Cloud service provider verifies the revocation list before giving access permission to the data.

Step1: Input: System parameter (p, q, r), a group signature M and a set of revocation keys A1.. Ar.
step2: Output: Valid or Invalid.
Step3: begin
Step4: set temp = e = (T1,Q)
e2 = (t2.R)
For i=1 to n
If e (t3-Ai,p)
Return null
Step5: else return temp
Step6: stop

5. EXPERIMENTAL ANALYSIS

In the proposed system, the group manager needs to store the user list and share data. Group manager takes charge of system initialization,

A system with 200 users with an assumption that each user shares 50 files on an average is considered. Then, the total storage of the group manager could be not more than 28.5Kbytes, which is acceptable. Group members need to store only their individual private key which is about 60 bytes. The extra storage overhead to store the file in the cloud is about 248 bytes only.

Therefore, the analysis on the proposed approach shows that the utilization of storage space among different models is low. Thus, it is acceptable for practical usage.

In the proposed scheme, the revocation of user from the group does not increase the computation cost irrespective of the number of revoked users. Revoked users are periodically updated and hence there is no chance of accessing the cloud once they are revoked from the group.

6. CONCLUSION

Sharing secure data in a cloud to multiple users among dynamic groups allows users to share their data with other users in a group without revealing data and identity privacy to the cloud. Additionally, it supports efficient user revocation and new member joining. More specifically, efficient user revocation can be achieved through a publicly available revocation list without updating the private keys of the remaining users and new users can directly decrypt the files from the cloud before their participation by contacting the group manager. Moreover, storage overhead and encryption computation costs are independent of the number of revoked users.

REFERENCES

[1]. P. Junod and A. Karlov, "An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies in Tenth annual ACM workshop on digital rights management. ACM, 2010, pp. 13–24.
[2]. Lam, S.S-zebeni, and L.Buttyan, "Invitation-oriented: Key management for Dynamic groups in an asynchronous communication model," Submitted to 4th International Workshop on Security in Cloud Computing, 2012.
[3]. N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-based Secure and Reliable Cloud Storage Service," in the Proceedings of IEEE INFOCOM 2012, 2012, pp. 693–701.
[4]. B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with large Groups in the Cloud," in the Proceedings of ACNS 2012, June 2012,
[5]. B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," Information Theory, IEEE Transactions on, vol. 57, no. 3, pp. 1786–1802, march 2011.
[6]. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.
[7]. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in the Proceedings of ACM SAC 2011, 2011,
[8]. H. Abu-Libdeh, L. Prince-house and H. Weather-spoon, RACS: a case for cloud storage diversity, ACM, 2010, pp. 229-240.
[9]. Taka-bi , H.; Joshi, J.B.D.; Ahn, G.; , "Security and Privacy Challenges in Cloud Computing," Security & Privacy, IEEE, vol.8, no.6, pp.24-31, Nov-Dec.2010. doi:10.1109/MSP.2010.186.
[10]. Kamara, Seny and Lauter, Kristin, Cryptographic cloud storage, FC'10 Proceedings of the 14th international conference on Financial Cryptography and data security, pp.136-149, 2010.