Secure Data Sharing for Dynamic Groups in the Cloud

Mahesh A.
Department of Computer Science and Engineering
Jain Global Campus, Jain University, Jakkasandra Post
KanakapuraTaluk, Ramanagara District-562112,INDIA
mahesh.a.015@gmail.com

S. Balaji
Centre for Emerging Technologies
Jain Global Campus, Jain University, Jakkasandra Post
KanakapuraTaluk, Ramanagara District-562112,INDIA
drsbalaji@gmail.com

***Abstract*- Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource sharing and low maintenance characteristics. Cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, when sharing the data in a group while preserving data, identity privacy is still a challenging issue due to frequent change in membership. In overcome this problem, a secure data sharing scheme for dynamic groups 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 should enable any cloud user to anonymously share data with others within the group and support efficient member revocation. The storage overhead and encryption computation cost are dependent on the number of revoked users.**

Keywords-*Cloud computing, data sharing, privacy-preserving, access control, dynamic groups*

1. INTRODUCTION

In cloud computing, the Cloud Service Providers (CSPs) are able to deliver various services to cloud users with the help of powerful data centers [9]. By uploading the local data management systems into cloud servers, users can enjoy high-quality of services and can save significant investments on their local infrastructures. One of the most fundamental services offered by cloud service providers is data storage.

The cloud servers managed by cloud service providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans [8]. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Several security schemes for data sharing on un-trusted servers have been proposed. In these approaches, data owners store the encrypted data files in un-trusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers have no knowledge of the content of the data files because they have no knowledge of the decryption keys [3].

Following are the problems that exist while providing secure data sharing. Firstly, the identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to use cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy.

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 as the multiple-owner manner. Compared with the single-owner manner, where only the group manager can store and modify data in the cloud, 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.

Lastly, the groups are normally dynamic in practice. It doesnot 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, respectively.

2. RELATED WORK

Junod and Karlov [1], proposes 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. In particular, the scheme utilizes the group signatures to construct homomorphic authenticators, so that a Third Party Auditor (TPA) is able to verify the integrity of the shared data. The identity of the signer on each block in shared data is kept private from the TPA.

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. To achieve user revocation, the manager delegate's tasks of data file re-encryption and user secret key update to cloud servers.

Kamaraet. 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. In addition, users have to query data owner to access the shared data, which will make a communication bottle neck as the number of users increases rapidly. Moreover, ACSS is just a concept model and the design was not completely implemented and tested.

3. PROPOSED SCHEME

The proposed scheme is to secure the data against unauthorized access by enforcing access control mechanisms. Basic solution to secure the data over the un-trusted cloud is to encrypt the data using attribute-based encryption to achieve secure data sharing for dynamic groups in the cloud by combining both the group signature and dynamic broadcast encryption techniques. The short group signature introduced by Chaum and van Heist scheme, which enables users to anonymously use the cloud resources provided by cloud service providers is used; it also supports efficient user revocation and provides secure and privacy-preserving access control to users, which 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 through the group signature. Only the members of the group can create valid group signatures. Figure 1 show how the group members register with the group owner and how the data is shared between the group members from the cloud server.

Figure 1: System Architecture

The dynamic broadcast encryption technique allows data owners to securely share their data files with other users within the group including newly joined users.Unfortunately, each user has to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme such that revoked users cannot access the data after their revocation from the group. This results in both computation overhead of the encryption and the size of the cipher-text increases with the number of revoked users. Thus, the heavy overhead and large cipher-text size may hinder the adoption of the broadcast encryption to the limited users.

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 the data cloud service provider verifies the revocation list and provide access to data only to active users in the group. Such a design can significantly reduce the computation overhead of users to encrypt files and the cipher-text size.

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 group users.Each individual user within the group must generate a valid signature.

Step1: start
Step2: Input: Private keys (Ai, xi), system parameter (P, U, V,H,W) and data M.
step2: Output: Generate a valid group signature on M.
step3: begin
step4: Select random numbers Set
(t1, t2, t3, r1, r2, r3)
And set x1=a and x2= b
Step5: Compute the following values t1, t2, t3, r1, r2, r3.
Step6: compute the challenging c
c=h (m, t1, t2, t3, r1, r2, r3, r4, r5) using Hash function.
Step7: using c construct the
Values s, s2, s3, s4, s5
Step8: Output the signature computed
as gsp=(t1,t2,t3,c,s1,s2,s3,s4,s5)
Step9: stop

Algorithm 2: Signature Verification

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

Step1: start
Step2: perform the verification for P and q
Step3: verify that Q is a factor of p-1, if
Any of the checks fail then the
Signature cannot be verified.
Step4: verify that r and s are in the range [1,q-1]
Step5: compute w=(s^-1) modq
Step6: compute u1=m*w modq

Step7: compute u2=r* w modq
Step8: compute v = (g^u1,y^u2) modp)modq
Step9: compare v and r if they are matched signature verified
Step10: stop

Algorithm 3: Revocation Verification

This algorithm is used by the active users to check if any users within the group revoked from the group.

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 shared data. 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 model is low. Thus, it is acceptable in real practical usage.

6. CONCLUSION

A secure data sharing scheme, for dynamic groups in an un-trusted cloud scheme allows a user to share data with others within the group without revealing data and identity privacy to the cloud. Additionally, it supports efficient user revocation and new user joining. More specifically, efficient user revocation can be achieved through a public revocation list without updating the private keys of remaining users and new users can directly decrypt files from the cloud before their participation.

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 CloudComputing, 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, pp. 1550–1557.
[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 Financialcryptograpy and data security, pp.136-149, 2010.