International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 6 4100 - 4103

Secure Dynamic Groups Auditing Service with Group Signature for Cloud Storage

Komal Waykole
M.E Scholar, Information Technology,
Shah and Anchor Kutchhi Engineering College,
Mumbai, India
komal25291@gmail.com

Shivani Deosthale
Dept. of Information Technology,
Shah and Anchor Kutchhi Engineering College,
Mumbai, India.
sakec.shivanid@gmail.com

Smita Bansod
Dept. of Information Technology,
Shah and Anchor Kutchhi Engineering College,
Mumbai, India.
sakec.smitab@gmail.com

Abstract—Cloud storage has become a commonplace of storing and sharing data across multiple users. It is a challenge to preserve confidentiality and maintain identity privacy while sharing data within multiple dynamic groups, due to frequent change in the membership. Also, maintaining data integrity is an issue as data is stored and audited by untrusted cloud service provider (CSP). In this paper, we propose, third party auditor (TPA) auditing scheme to maintain data integrity and enabling TPA to perform audits for multiple users efficiently and simultaneously. By exploiting group signature scheme any member can anonymously share data within the group. The efficiency and the computation cost of the proposed system are independent with the number of users revoked and the data stored on the cloud.

Keywords—*cloud computing; cloud storage; group signature; user revocation; third party auditor; dynamic groups; data integrity.*

****

I. INTRODUCTION

Cloud Storage is the fundamental services provided by cloud service providers (CSP). Cloud service providers like Microsoft Azure, Amazon, Dropbox offers users scalable and reliable environment to store and access data at lower marginal costs. It has become a routine for users to share data with other team members as data sharing has become standard feature in most of the cloud offerings including GoogleDocs and Dropbox.

While cloud storage advantages are appealing it also brings challenge to security threats to the users outsourced data. Let us consider a company staff or departments share data within their group over cloud environment. The group member's store and share files over cloud which is accessible to each group member of same group. By utilizing cloud the company is completely released from the trouble of local data storage, its infrastructure and their maintenance. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not easy due to challenging issues like identity privacy of the user, confidentiality of the data, traceability of the misbehaved group member, providing equal access to each member rather than single owner manner and providing data integrity check by auditing the cloud storage [1].

In this paper, we overcome the above challenges by utilizing group signature scheme so that only authorized group member is able to store, access and modify data in dynamic group where the membership changes and provide secure data sharing. The auditing of the cloud storage is outsourced to a third party auditor (TPA) for checking the integrity of the data without retrieving the whole file content i.e. maintaining confidentiality of sensitive data at TPA side. Also the identity of the user is not disclosed to TPA, thus preserving the identity.

The paper is organized as follows: Section II gives us an insight to the available schemes; Section III describes the existing system and its disadvantages; Section IV describes the proposed system; Section V describes the modules; Section VI gives us the advantages of the proposed system and conclusion is drawn in the Section VII.

II. LITERATURE REVIEW

A. Group signature

A group signature is an identity anonymization cryptographic scheme introduced by Chaum and Heyst [2]. In this scheme a verifier may know that the message is signed by an authorized group member but could not disclose the identity of the member. The identity disclosure of a particular message originator is done by the group manager. Group manager can also add a member and revoke the group members in case of disputes in the group. In some systems, adding and revoking mechanism can be separated and given to membership manager and revocation manager respectively.

In [3], the groups are considered as static. In their system, the number of group members and their identities are fixed. A trusted entity chooses not only the group public key and an opening key for the opening authority, but also, for each group member, chooses a signing key and hands it to the member in question. Within this framework, they formalize two (strong) security requirements that they call full anonymity and full-traceability. They then present a static group signature scheme shown to meet these requirements. J. Camenisch and M. Michels designed a new group signature scheme that is well suited for large groups, i.e., the length of the group's public key and of signatures do not depend on the size of the group. This scheme is based on a variation of the strong RSA assumption [4].

M. Bellare *et al.*, a group signature scheme is implemented for dynamic groups. Here group public key is initialized by trusted party, keys for the two authorities i.e. issuer and opener, and a join protocol so that the private signing key of any group member, as well as the signature created. The scheme here provides correctness of signatures by authorized group member, traceability of the partial corrupt user, anonymity of the signer of the message, non-frameability where the honest user could not be framed for the misbehaviour of corrupt user [5].

Lu et al. [6] proposed a secure provenance scheme, which is built upon group signatures and cipher text-policy attribute-based encryption techniques. Particularly, the system in their scheme is set with a single attribute. Each user obtains two keys after the registration: a group signature key and an attribute key. Thus, any user is able to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys. Meanwhile, the user signs encrypted data with her group signature key for privacy preserving and traceability. However, user revocation is not supported in their scheme.

H. Chen et al. [7] presented a group signature scheme based on strong RSA assumption, DCR assumption, and collision resistant hash function, which is proved on their implemented random oracle model. The signature length is short.

B. Third Party Auditor (TPA)

Third party auditing scheme for data integrity checking was introduced by C. Wang *et al*. for auditing process that perform audits on multiple users simultaneously.in this scheme the utilize public key based homorphic linear authenticator with random masking, which reduces the computation and communication cost, by enabling TPA to audit data which demanding the local copy of the data [8].

Q. Wang *et al*. [9] implemented a scheme that provides audits over dynamic data by TPA. The integrity of the data is verified for data dynamics by manipulating Merkle Hash Tree construction for block tag authentication. Bilinear aggregate signature technique is explored to support multiple auditing tasks simultaneously.

An auditing framework for cloud storage systems was designed by K. Yang *et al.* [10]. The auditing protocol supports the data dynamic operations, which is efficient and provably secure in the random oracle model. The auditing protocol is extended to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer.

In [11], dynamic audit service is constructed based on the techniques that include fragment structure, random sampling, and index-hash table, supporting provable updates to outsourced data and timely anomaly detection. In addition, a method based on probabilistic query and periodic verification is implemented for improving the performance of audit services. The audit system verifies the integrity with lower computation overhead and requires less storage for audit metadata.

Wang et al. utilizes the idea of proxy re-signatures. For security reasons if any user is revoked from a group the block of data signed by the revoked user should be re-signed by an existing user. The existing users do not need to download the data blocks of the revoked user during user revocation. The signatures are re-computed for all the data blocks during user revocation. In addition a public verifier i.e. TPA is appointed to verify the integrity of the data without retrieving the entire data from the cloud. The mechanism also supports batch auditing by verifying multiple data blocks simultaneously [12].

III. Existing System

In existing system, multiple users store the data in the cloud storage. These users are a group of users where the group is static in nature. The auditing of the system is outsourced to a third party auditor (TPA) to save the computational cost of the user and to check the data integrity of the stored data. There may be motivations to CSP to behave unfaithfully toward the cloud users regarding their outsourced data status [8]. The auditing scheme utilizes ring signature scheme to constructs homorphic authenticators. This scheme computes the verification information needed to audit the integrity of the shared data without retrieving entire data from the file. The signer of the data block is kept private from the TPA. It supports batch auditing i.e. audits multiple shared data simultaneously in single auditing task.it also supports dynamic data operations like insert, delete and modify over the shared data blocks [13].

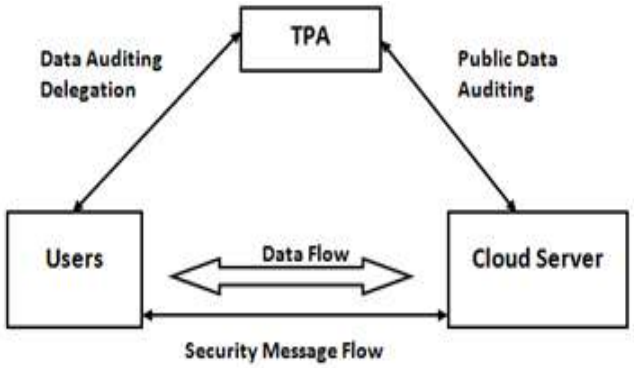

Figure. 1 Architecture of Existing System

The existing system has the following disadvantages:

1. The group is static. No new member can be added in the system.
2. Ring signature does not support traceability i.e. cannot identify the group members identity if dispute occurs in a group.
3. Re-computing of signature is not supported in case of deletion of a group member in case any dispute occurs.
4. Not all members in the group are able to access the shared data; the data owner decides who can access the data.
5. Data owners file gets updated without his permission if any modifications are made to the file by one of the group member with its signature.
6. Dynamic groups are not supported where members can be added and deleted while preserving the privacy of the group member's identity.

IV. PROPOSED SYSTEM

In the proposed system, we overcome the problems of existing system. We introduce multiple dynamic groups in storage system whose auditing is outsourced rather then it being done by untrusted CSP or the user. Group signature scheme is utilized; it computes signatures for each group and its group members. On revocation of any group member from a particular group, all the signatures including signature of the file is recomputed, thus making the system more secure in lower computation speed. The revoked member cannot access the data of its group with his existing signature. All the group members have the ability to share and modify data in the same group rather than only group manager sharing and modifying the data and other members only view the shared data. The

 ISSN: 2321-8169
4100 - 4103

group members of another group cannot access other group data i.e. group B member is denied from accessing data of group A. The auditing service is outsourced to a third party auditor (TPA). TPA audits shared data without retrieving the whole data from the cloud storage, thus maintain the confidentiality of sensitive data. Full anonymity is maintained by preventing discloser of the identity to TPA during auditing process.

The figure 2 shows the architecture of the proposed system.

Following is the description of each block:

1. *Cloud Storage*: The group members will store the data in the cloud storage. The cloud storage server will accept the auditing challenge from the TPA and calculate the corresponding auditing proof and send to TPA for verification.

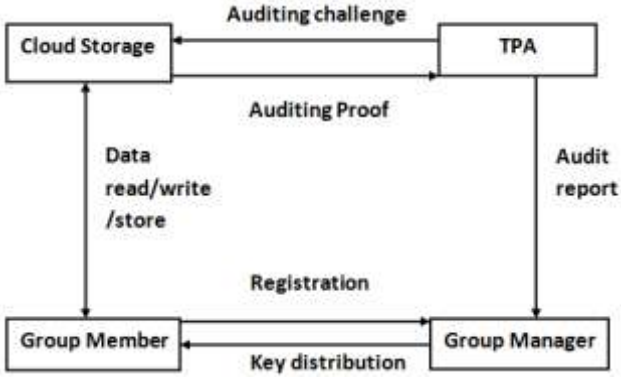

Figure. 2 Architecture of Proposed System

2. *TPA*: He will periodically initialize auditing process to check the correctness of the data stored in the storage. It will verify the proof send by the cloud storage server and send the audit report to the group manager.
3. *Group Manager*: Group manager takes charge of system parameter generation, user registration, user revocation, and revealing the real identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company. Therefore, we assume that the group manager is fully trusted by the other parties.
4. *Group member:* are a set of registered users that will store their private data into the cloud server and share them with others in the group. In our example, the staffs play the role of group members. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company [1].

Following are the advantages:

1. *Correctness*: TPA is able to check the integrity of the shared data correctly.
2. *Batch Auditing:* There may be multiple accesses to shared data in a day. At regular interval the data integrity should be checked. This property helps to audit large amount of data simultaneously in efficient and cost effective manner.
3. *Data Dynamics:* The shared data stored in the cloud supported modification and updating of the data by the authorized group member.
4. *Confidentiality of the Shared Data:* The unauthorized users, the untrusted cloud service providers and the TPA are incapable of retrieving the content stored in the cloud.
5. *Anonymity:* The group member can access the shared data from the cloud without revealing it identity.
6. *Traceability:* The identity of the user can be revealed only by the group manager in case any dispute occurs in the group. For example; a disgruntled employee whose is still a member of the group may try to modify the sensitive data stored in the cloud.
7. *Efficient user revocation:* When revocation takes place all the signatures are recomputed so that the revoked user is prevented from accessing the shared data using his signature (signature obtained while he was a part of the group) making the system more secure.
8. *Scalability*: The shared data on the cloud can be accessed by a large number of users of a particular group and the TPA is also able to handle large number of auditing tasks simultaneously and efficiently.

V. MODULES

Following are the modules in the proposed system:

A. Group Signature Module

Group signature allows a group member on behalf of the group to sign a message anonymously. Group signatures have applications in the field of privacy protection, such as voting, bidding, electronic cash system, and trusted computing [7].
Following are the properties that group signature satisfy:

1. *Traceability*: The group manager can efficiently trace which user has issued the signature, if a valid signature is provided to the manager.
2. *Anonymity*: Given a message and signature, the identity of the signer cannot be revealed by any other group member except for the group manager.
3. *Correctness*: the signatures generated will be verified and traced correctly.

In the proposed system, group signature for multiple dynamic groups consists of following steps:

1. *grpkey*: A unique key i.e. group key is generated for all the groups present in the system.
2. *keygen*: Public and private keys for each user is generated.

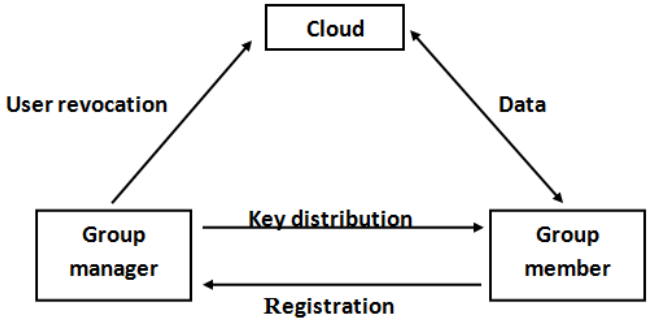

Figure. 3 Group Signature Scheme

3. *verify_sgnm*: The user signature over the message is verified to check whether he is member of the same group.
4. *trace*: Group manager can trace the user in case any dispute occurs.

On user revocation i.e. adding or deleting a user in a particular group consists of following steps:

1. *Update_grpkey*: the group key is updated for the group in which a member is added or deleted.
2. *Update_keygen*: all the keys of the users are updated.
3. *Update_sgnm*: The signatures of the earlier messages are updated for the present group members.

B. Third Party Auditor (TPA)

The auditing process of the proposed system is outsourced to a TPA. The outsourcing of auditing process helps to reduce the online burden and computational resources of the cloud users. Moreover, CSP may have some reasons to be unfaithful to cloud users regarding the status of the outsourced data [8]. TPA initiates the auditing procedure periodically and audits the data that is uploaded in that particular period. TPA compares the auditing proof generated by the cloud server with its own computation result for the uploaded data, thus maintaining the data integrity. During this procedure, TPA does not retrieve the whole data from the cloud thus maintaining the confidentiality of the data. Signature of the user is preserved during this process and TPA audits multiple data simultaneously thus providing the feature of identity preserving and batch auditing respectively.

VI. CONCLUSION

Cloud security is a challenge and an important aspect to cloud computing, as the demand for cloud storage is increasing in day to day life. While sensitive data is stored over cloud, maintaining confidentiality and data integrity of such data is a challenge. In the proposed system the data integrity is checked and the confidentiality is maintained of the shared data in the cloud storage with minimum costs and efforts. The system helps to reduce the computational and storage overhead of the client as well as to minimize the Computational overhead of the cloud storage server. The System is designed to securely share data for dynamic groups in an untrusted cloud environment. A user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, this supports efficient user revocation and new user joining.

ACKNOWLEDGEMENT

We sincerely thank the Staff members and colleagues who have directly or indirectly contributed for completion of this paper. We are grateful to our institute and management for lending support without which this would have not been possible. Last but not least we will extend our gratitude to our family members.

REFERENCES

[1] X. Liu; Y. Zhang; B. Wang; J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," *Parallel and Distributed Systems, IEEE Transactions on* , vol.24, no.6, pp.1182-1191, June 2013.

[2] D. Chaum and E. van Heyst. Group signature. In Advances in Cryptology — Eurocrypt, pages 390–407, 1992.

[3] M. Bellare, D. Micciancio and B. Warinschi, “Foundations of group signatures: Formal defnitions, simplifed requirements, and a construction based on general assumptions”, *Advances in Cryptology - Eurocrypt ‘2003 Warsaw, Poland*, Springer, pp. 614-629, May 2003.

[4] J. Camenisch and M. Michels, “A Group Signature Scheme Based on an RSA-Variant”, *Advances in Cryptology: 4th ASIACRYPT Conference on the Theory and Applications of Cryptologic Techniques, ASIACRYPT ’98 Proceedings*, pages 160–174, November 1998.

[5] M. Bellare; H. Shi; C. Zhang,"Foundations of Group Signatures: The Case of Dynamic Groups" *Topics in Cryptology CT-RSA2005 Proceedings*, Springer, vol. 3376, pp. 136-153, 2005.

[6] 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.

[7] Hefeng Chen; Wenping Ma; Youjiao Zou; Changxia Sun, "Strongly secure group signature scheme," *Communications Security Conference (CSC 2014)*, pp.1-8, May 2014

[8] C. Wang; Chow, S.S.M.; Q. Wang; K. Ren; W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," *Computers, IEEE Transactions on* , vol.62, no.2, pp.362-375, Feb 2013.

[9] Q. Wang; C. Wang; K. Ren; W. Lou; J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *Parallel and Distributed Systems, IEEE Transactions on* , vol.22, no.5, pp.847-859, May 2011.

[10] K. Yang; X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," *Parallel and Distributed Systems, IEEE Transactions on* , vol.24, no.9, pp.1717-1726, September 2013.

[11] Y. Zhu; Gail-Joon Ahn; H. Hu; Yau, S.S.; An, H.G.; Chang-Jun Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," *Services Computing, IEEE Transactions on* , vol.6, no.2, pp.227-238, April-June 2013.

[12] B. Wang; Baochun Li; Hui Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," *Services Computing, IEEE Transactions on*, vol.8, no.1, pp.92,106, Jan.-Feb. 2015

[13] B. Wang, B. Li, and H. Li, “Oruta: Privacy-preserving public auditing for shared data in the cloud,” *in Proc. of IEEE CLOUD 2012, Hawaii, USA*, pp. 295–302, June 2012.