International Journal on Applications in Engineering and Technology
Volume 4: Issue 1: March 2018, pp 36 - 39. www.aetsjournal.com ISSN (Online) : 2455 - 0523

NOVEL PRIVACY-AWARE PUBLIC AUDITING SCHEME FOR SHARED CLOUD DATA WITH DYNAMIC GROUPS

K.KALAIVANI , R.VETRIVENTHAN, SENTHIL KUMARAN

Abstract— Nowadays, cloud storage area turns out to be one of the critical services, for the reason that users can certainly modify and share data with others in the cloud. However, the integrity of distributed cloud data is susceptible to certain hardware errors, software failures or individual mistakes. To guarantee the integrity of the shared data, some techniques have been made to allow general population verifiers (i.e., third-party auditors) to effectively audit data integrity without retrieving the whole users' data from the cloud. Regrettably, public auditing on the integrity of shared data may uncover data owners' hyper-sensitive information to the third party auditor. In this paper, we propose a new privacy-aware public auditing mechanism for shared cloud data by making a homomorphic valid group signature. Unlike the existing solutions, our plan requires at least team professionals to recover a track key cooperatively, which removes the mistreatment of single-authority ability and provides no flammability. Moreover, our scheme means that group users can trace data changes through the specified binary tree; and can recover the latest right data stop when the existing data stop is destroyed. Also, the formal security analysis and experimental results reveal that our system is probably secure and efficient.

Keywords— Data Integrity; Homomorphic Verifiable; Nonframeability; Provable Security.

I. INTRODUCTION

Due to the increasing number of applications of shared data, such as iCloud, Google Docs, and so on; users can upload their data to a cloud and share it with other peers as a group. Unfortunately, since cloud servers are vulnerable to certain hardware faults, software failures or human errors, data stored in the cloud may be spoiled or lost . In the worst cases, a cloud owner may even conceal data error accidents to preserve its reputation or avoid profit losses. Also, users who lose direct control over their data are not sure whether their cloud- stored data is intact or not. Therefore, integrity verification for the shared data in the cloud is an important, yet timely issue for a large number of cloud users. To ensure the integrity of data stored in cloud servers, some mechanisms based on various techniques have been proposed. In particular, to reduce the burden on users, a trusted third-party auditor (TPA) is engaged to conduct the verification, which is called public auditing . However, the TPA may have additional access to private information during the auditing process. Therefore, researchers proposed some new schemes to protect privacy, including data privacy , and identity privacy. To be specific, the TPA cannot learn each block that is signed by a particular user in the group by constructing Homomorphic authenticable ring signatures or computing tags based on common group private key. However, since both methods concern about absolute privacy, the real identity of the signer can no longer be traced. A later development is the homomorphic authenticable group signature scheme based on group signatures , which is designed to protect privacy. On the one hand, the identity of each signer is anonymous; and on the contrary, the group manager can trace a signer's real identity after a dispute. Unfortunately, in all existing public auditing schemes, the tracing process is accomplished by a single entity. As a result, that entity has the privilege of tracing, which may lead to abuse of single authority power. Therefore, an innocent user may be framed, or a malicious user may be harbored. Meanwhile, to support data dynamics, the data structure based on index hash table or Merkle Hash Tree (MHT) has been utilized.However, this kind of data structure merely records the newest data block with the corresponding signature, which prevents users from tracing the changes of the data blocks. When the current data has been corrupted, users cannot recover the old data from the records. Therefore, the problem of data traceability and recoverability also should be considered. Moreover, a necessary authentication process is missing between the auditor and the cloud in most existing public auditing schemes. Hence anyone can challenge the cloud for the auditing proofs. This problem will trigger network congestion and unnecessary waste of cloud resources. Although Liu et al. [12] designed an authorized public auditing scheme to solve the problem, it is only suitable for a single client, and cannot be applied to group-shared data. Since the malicious or pretended auditors/users might constantly request cloud access for the auditing proof by utilizing TPA, unauthorized auditing is another important issue that should be addressed in integrity verification for shared cloud data. At present, all the existing public auditing schemes only consider a single group manager

K.Kalaivani , Master of Computer Applications , Meenaakshi Ramasamy Engineering College , Thathanur , Ariyalur Dt , Tamil Nadu .

R.Vetriventhan , BE , MTech , MISTE , Head of the department , Department of MCA , Meenaakshi Ramasamy Engineering College , Thathanur , Ariyalur Dt , Tamil Nadu .

Dr.Senthil Kumaran , ME Phd , Managing Director , Meenaakshi Ramasamy Engineering College , Thathanur , Ariyalur Dt , Tamil Nadu.

when applied to shared data with group users. However, in real-world applications, there might be multiple managers in a group. For instance, the common data of a project team is created by multiple managers together, whats more, any of them can maintain the shared data. Another important practical problem is that the group users should be able to dynamically enroll and revoke the group, which will be managed by the group managers. Moreover, significantly, when tracing the real identity of the signer, a specified number of executives can work together, which ensures the fairness of the tracing process. In this paper, we propose a new privacy-aware public auditing mechanism, called NPP, for the shared cloud data with multiple group managers.

Our contributions can be summarized as follows.

1. We establish a model for data (in a group) shared with various group managers and propose a new privacy preservation public auditing scheme for different group managers in shared cloud storage. Our proposed scheme can not only provide multi-levels privacy-preservation abilities (including identity confidentiality, traceability, and non-flammability) but also can well support group user revocation.
2. We design Problem statement.
3. We design Design Objectives.
4. Conclusion

II. PROBLEM STATEMENT

In this section, we describe the system model and the threat model of this paper and give the design objectives of our public auditing scheme.

1) System Model

As shown in Fig. 1, the system model contains four entities: cloud, TPA, trusted private key generator (PKG), and group users. The cloud has great storage space and computing capacity and provides services (e.g., data storage, data sharing, etc.) for group users. The TPA can verify the integrity of the shared data on behalf of the group users. The PKG generates the public system parameters and group key pair for group users. The group users include two types of users: GMs (Group Managers) and ordinary members. Unlike existing system models, the GMs contain multiple members who create the shared data together and share them with the regular members through the cloud. Therefore, the GMs act as the joint owners of the original data, and their identities are equal. Meanwhile, any of the GMs can add new members or revoke members from the group. Also, either a GM or an ordinary member can access, download, and modify the shared data in the cloud. Note that multiple managers in a group are very common in practice. For instance, the common data of a project team is created by multiple managers together. Later, any of the GMs can maintain the shared data and manage the group users. When tracing the real identity of the signer, a given number of managers can cooperate to trace the true identity, which ensures the fairness of the tracing process. When a group user wants to check the integrity of the shared data, she/he first submits an auditing request message to the TPA. After receiving the request, the TPA challenges the cloud for an auditing proof. Once the cloud receives the auditing challenge, it firstly authenticates the TPA. If valid, the cloud will return the auditing proof to the TPA. Otherwise, the cloud will refuse the request. Finally, the TPA verifies the validity of the proof and sends an auditing response to the group user.

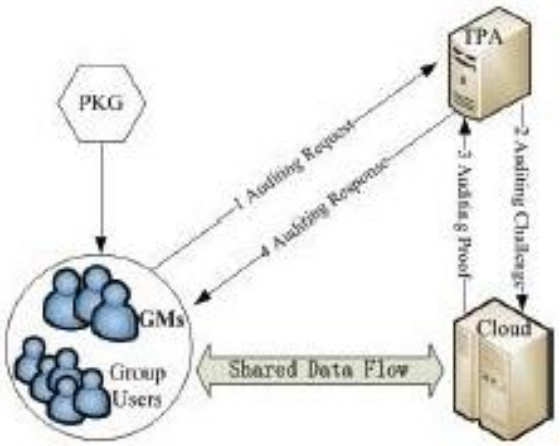

Figure 1: The system model of NPP

2) Threat Model

A. Integrity Threat

There are two kinds of threats related to shared data integrity. One is that external attackers might corrupt the shared data in the cloud so that group users can no longer access the correct data. The other is that the cloud may corrupt or delete the shared data due to the hardware/software faults or human errors. What's worse, the cloud may conceal the fact of data damage from users to maintain self-interest and service reputation.

B. Privacy Threat

As a trusted and inquisitive verifier, a TPA might obtain some privacy information from the verification metadata during the auditing process. For instance, the TPA might analyze which data block has been modified most or which user has modified the data most, and finally conclude which particular data block or which group the user is of a higher value than the others. Then the TPA might directly obtain the data or the identity of the group user from the signatures of the data blocks.

C. Challenge Threat

Because the auditing challenge message is straightforward and has not been authorized, any other entity can utilize the TPA to contest the cloud for auditing proofs. In this case, a malicious entity might launch denial of service attacks on the cloud by sending massive challenge messages continuously, which will lead to network congestion and unnecessary waste of t he sources of the cloud.

III. DESIGN OBJECTIVES

To achieve integrity checking of the shared data in the cloud, NPP is expected to the following design objectives:

1) Public auditing:

Besides the group users, the TPA can also correctly check the integrity of the shared data in the cloud without retrieving entire users' data from the cloud.

2) Authorized auditing:

Only the TPA that has been authorized by the group users can challenge the cloud.

3) Identity privacy:

During the procecess of auditing, the TPA cannot learn the identity of group user from the signatures of the data blocks.

4) Traceability:

Under certain conditions, the group managers can reveal the signer's identity from the signatures and decide which group user has modified the data block.

5) Nonflammability:

Group managers can guarantee the fairness of the tracing process, i.e., innocent group user will not be framed, and the group managers will not harbor the misbehaved user.

6) Support data traceability and recoverability:

Group users can easily trace the data changes and recover the latest correct data once current data is damaged.

7) Support group dynamics:

Group dynamics include two aspects. One is that GMs can easily join or leave the group, the other is that new users can be easily added into the group and misbehaved users can be effectively excluded from the panel.

A. Discussions

1) Group Managers Dynamics:

• GM joining

If a new GM wants to adhere to the group, the PKG computes $S' = S+1$, and tests whether $2t-1 \geq S'$. If it holds, the PKG will calculate a new piece (S', Xs') with polynomial f(x) and distribute it to the new GM′ S ; otherwise, the PKG chooses a new $(t' - 1)$-degree polynomial $f'(x) = b'0 + b'1x + \cdots + b't'-1x\,t'-1$,
where $2t' - 1 \geq S'$, $b'0 = X$, $b'1, \cdots, b't'-1 \in Zq$,
and computes $X'l = f'(l)(l = 1, 2, \cdots, S')$, i.e. X is divided into S' pieces $X'l$ and then distributed to GMl . Also, the PKG generates a new key pair {spk', ssk'}, and broadcasts it to all the GMs, who can then share it with the existing group users. Note that the process of updating {spk, ssk} does not affect auditing, because the signing keys, the membership keys and the revocation keys of the existing users do not need to be updated. Nor do the signatures of the data blocks.

• GM leaving

If an existing GMl wants to leave the group, the PKG first sets $S' = S - 1$, chooses a new $(t' - 1)$-degree polynomial $f'(x) = b'0 + b'1x + \cdots + b't'-1x\,t'-1$,
where $2t' - 1 \geq S'$, $b'0 = X$, $b'1, \cdots, b't'-1 \in Zq$,
and then computes and distributes new $X'l = f'(l)(l = 1,2, \cdots, S')$ to each GMl . Also, the PKG generates a new key pair {spk', ssk'}, and broadcasts it to all the GMs, who can then share it with the existing group users.

2) User Revocation:

GMs maintain a users list, which is composed of each user's related key and expiration time. Once a user's service subscription expires, their signing key should become invalid from then on. In this case, any GM can invoke the Revoke algorithm by updating the membership information Ω and the key pair {spk, ssk} and setting the value of the revoked user's expiration time to be negative. There might be misbehaving users in the group. In this case, any GM can invoke the Revoke algorithm as mentioned above. Note that when a user is revoked from a group, GMs do not need to re-compute and re-distribute new keys to the valid users, since the revoked user Ui cannot find f, $b \in Zq$ such that $f_{\cdot u+b\cdot rvki} = 1$, Ui cannot compute the partial signature V2 anymore. If the revoked user Ui maliciously reveals their signing key uski = (xi , π), then the partial signature of other users can be discerned because of the common key π. However, it is not enough to forge a valid signature as the secret key xj of the other users is still unknown. Therefore, the partial signature V1 cannot be computed. As we have demonstrated, valid users do not need to update their keys and the existing signatures. Signatures belonging to the revoked users can be re- computed by the GMs. Specifically, the existing user interacts with GMs to generate a proxy signature key; then GMs use the proxy key to compute the signatures of the revoked users. That transforms them into the signatures which sign by the private key of the existing user.

IV. CONCLUSION

In this paper, we propose a novel multi-level privacy is preserving public auditing scheme for cloud data sharing with multiple managers. During the process of auditing, the TPA cannot obtain the identities of the signers, which ensures the identity privacy of the group users. Moreover, unlike the existing schemes, the proposed NPP requires at least t group managers to work together to trace the identity of the misbehaving user. Therefore, it eliminates the abuse of single authority power and ensures no-frame ability. Exceptionally, group users can trace the data changes through

the designed binary tree and recover the latest correct data block when the current data block is damaged. Also, the analysis and the experimental results show that NPP is provably secure and efficient.

References

[1] D. Fernandes, L. Soares, J. Gomes, et al, "Security issues in cloud environments: a survey," International Journal of Information Security, vol. 12, no. 2, pp. 113-170, 2014.

[2] W. Hsien, C. Yang, and M. Hwang, "A survey of public auditing for secure data storage in cloud computing," International Journal of Network Security, vol.18, no.1, pp. 133-142, 2016.

[3] J. Yu, K. Ren, C. Wang, et al, "Enabling Cloud Storage Auditing with Key-Exposure Resistance," IEEE Transactions on Information Forensics and Security, vol.10, no.6, pp. 1167-1179, 2015.

[4] Q. Wang, C. Wang, K. Ren, et al, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[5] S. Yu, "Big privacy: challenges and opportunities of privacy study in the age of big data," IEEE Access, vol.4, no. 6, pp. 2751-2763, 2016.

[6] C. Wang, Q. Wang, K. Ren, et al, "Privacy- preserving public auditing for data storage security in cloud computing," Proceedings of IEEE INFOCOM, pp.1-9, 2010.