ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

Authorized Public Auditing Scheme for Shared Data with Cloud Users

Dhanalakshmi.G[1], Nandhini.P[2], Rajeswari.N[3], Raveena.B[4]

Assistant Professor, Department of Information Technology, Panimalar Institute of Technology, Chennai, India.[1]

B.Tech Student, Department of Information Technology, Panimalar Institute of Technology, Chennai, India[2].

B.Tech Student, Department of Information Technology, Panimalar Institute of Technology, Chennai, India[3].

B.Tech Student, Department of Information Technology, Panimalar Institute of Technology, Chennai, India[4].

ABSTRACT: Cloud storage becomes one of the critical services,because users can easily modify and share data with others in cloud.To ensure the integrity of the shared data, some schemes have been designed to allow public verifiers to efficiently audit data integrity without retrieving the entire users'data from cloud.In this project, we propose a new privacy-aware public auditing mechanism for shared cloud data by constructing a homomorphic verifiable group signature. In order to reduce the burden on users, a trusted third party auditor(TPA) is engaged to conduct the verification, which is called public auditing.It can verify the accessed data without looking what the data is ,hence privacy is preserved.The TPA is plays an intermediate role between the data owner who is uploading the files into the cloud and the ordinary member who is downloading the files from the cloud.

KEYWORDS: Data Integrity; Homomorphic Verifiable; Non-Frameability; 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 inevitable hardware faults, software failures or human errors, data stored in the cloud may be spoiled or lost [1]. In the worst cases, a cloud owner may even conceal data error accidents in order to preserve its reputation or avoid profit losses [2],[3]. In addition, users who lose direct control over their data are not sure whether their cloud-stored data is intact or not. To ensure the integrity of data stored in cloud servers, a number of mechanisms based on various techniques have beenproposed. Integrity verification for the shared data in the cloud is an important, yet timely issue for a large number of cloud users.

In particular, in order to reduce the burden on users, a trusted third-party auditor (TPA) is engaged to conduct the verification, which is called public auditing [4]. However, the TPA may have unnecessary access to private information during the auditing process [5]. Therefore, researchers proposed some new schemes to protect privacy, including data privacy [6], and identity privacy [7]-[9]. 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 [7] or computing tags based on common group private key [8]. However, since both methods concern about unconditional 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 [9], which is designed to protect privacy. On one hand, the identity of each signer is anonymous ;and on the other hand, 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 singleauthority power. Therefore, an innocent user may be framed or a malicious user may be harbored. It establish a model for data (in a group) shared with multiple group managers, and propose a new privacy aware public auditing scheme for multiple group managers in shared cloud storage. It contains a data structure based on a binary tree for clouds to record all the changes of data blocks. Group users can trace the data changes through the binary tree and recover the latest correct data block when the current data

DOI: 10.15680/IJIRCCE.2018.0602083

block is damaged. It utilize an authorized authenticate process to verify TPA's challenge messages. Therefore, only the TPA who has been authorized by the group users can pass the authentication and then challenge the cloud, which protects clouds from malicious challenges. Our proposed scheme cannot only provide multi-levels privacy-preservation abilities (including identity privacy, traceability and non-frameability), but also can well support group user revocation. Our formal security analysis and experimental results show that NPP is provably secure and efficient.

II.RELATED WORK

Considering the application of cloud data shared by group users, Wang et al. [7] proposed a privacy-preserving public auditing scheme, called Oruta, for shared data in the cloud. Their scheme was based on a homomorphic authenticable ring signature, which allows a public auditor to audit the shared data without retrieving all data from the cloud. However, the auditing overhead linearly increases with the number of group users, hence it is not suitable for large groups in the cloud. Tosupport large groups, Wang et al. [8] proposed a new auditing scheme, called Knox. The auditing overhead is independent of then number of group users ,hence Knox can support shared data with large groups. Moreover, any group manager can reveal the identity of the signer. Unfortunately, the scheme cannot support user revocation. Many schemes have been proposed in order to deal with this problem. In [9]-[11], homomorphic authentications based on proxy re-signature were constructed. In this proposed system the data owner can upload their files in the cloud storage by registering as a cloud user. .Each user has a private key to access their files. The uploaded files will be encrypted and stored in the cloud .If many user has uploaded the same files ,then it will be group into one group and only one copy of files will be stored in the cloud storage. If any user wants to download the file ,then the auditor will authenticate the user and provide the decrypted file to the requested user. Thus, the file can be securely shared.Each file can be access and modified by the data owner by using private key,so that we can maintain the key efficienty.

III.IMPLEMENTATION

1.GROUP USERS

The group users include two types of users: GMs (Group Managers) and ordinary members. GMs contain multiple members who create the shared data together and share them with the ordinary members through the cloud. Group manager acts as a common owners for the original data and their identities are equal.

2.THIRD PARTY AUDITOR

TPA is used to conduct the verification and for uploading the data files ,the auditor first check the file is duplicated then group will be formed for those data owners ,the auditor convert the plaintext to encrypted text .For downloading the files the ordinary members submit a request to TPA .TPA first check whether the file is available and if it is available it check requested user is a authenticated person and then convert encrypted text to plaintext.

3.PRIVATE KEY GENERATOR

KeyGen algorithm randomly generates a private key to cloud users during registration process.Private key is used to authenticate each cloud user by TPA.For each data owner and ordinary members ,a separate private key is generated eventhough they upload as many files using single private key.

4.CLOUD STORAGE

Cloud storage becomes one of the critical services, because users can easily modify and share data with others in cloud.It has a powerful storage space and computing capacity capacity and provide services(e.g,data storage, data sharing)for users.

IV.SYSTEM DESIGN

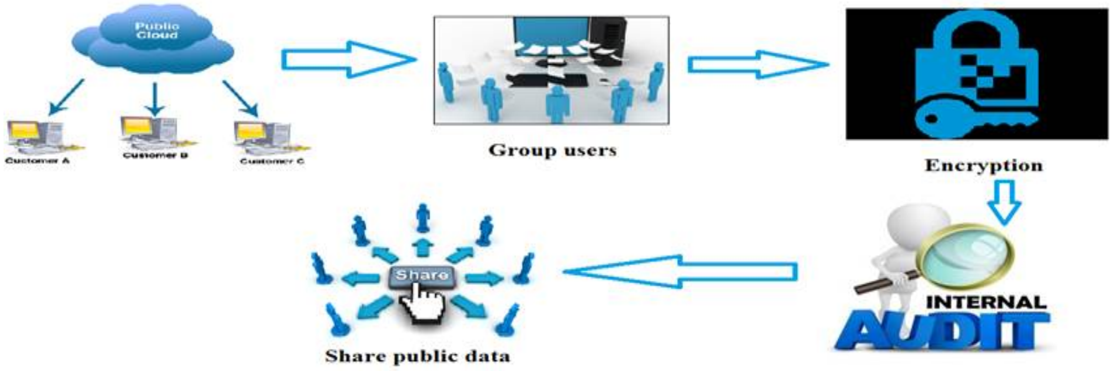

Fig1:Architectural diagram of shared data with cloud users

In **Fig. 1,** the system model contains following entities: cloud, TPA, cloud users and group users. The cloud has powerful storage space and computing capacity,andprovidesservices(e.g.,datastorage,datasharing, etc.) for group users. The TPA can verify the integrity of the shared data on behalf of the group users. The PKG generates the system public parameters and group key pair for group users.Thegroupusersincludetwotypesofusers: 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 ordinary members through the cloud.

Therefore, the GMs act as the common 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. In addition, 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 is very common in practice. For instance, the shared 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 real 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.

V.PROBLEM STATEMENT

A.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 cloud.

2)Authorized auditing: Only the TPA that has been authorized by the group users can challenge the cloud.

3)Identity privacy: During the process of auditing, the TPA cannot learn the identity of the 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)Nonframeability: Group managers can guarantee the fairness of the tracing process, i.e., innocent group user won't be framed and the misbehaved user won't be harbored by the group managers.

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 efficiently excluded from the group.

B. Threat Model :
1) 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 in order to maintain self interest and service reputation.
2) 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 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.
3) Challenge Threat: Because the auditing challenge message is very simple and has not been authorized, any other entity can utilize the TPA to challenge the cloud for auditing.

VI.ACKNOWLEDGEMENT

We thank our Head of the Department (IT) **Dr.A.Joshi** for providing us all the necessary facilities.We express our sincere thankfulness to our Project Guide **Mrs.G.Dhanalakshmi** for her successful guidance to our project. Without the help it would be a tough job for us to accomplish this task. We thank our guide for her consistent guidance, encouragement and motivation throughout our period of work.

VII.CONCLUSION

We propose a novel multi-level privacy 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 non-frameability. 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. In addition, 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.
7.B. Wang, B. Li, and H. Li, "Oruta: privacy-preserving public auditing for shared data in the cloud," IEEE Transactions on Cloud Computing, vol.2, no.1, pp.43-56, 2014.
8.B. Wang, B. Li, and H. Li, "Knox: privacy-preserving auditing for shared data with large groups in the cloud," Applied Cryptography and Network Security. Springer Berlin Heidelberg, pp. 507-525, 2012.
9.B. Wang, H. Li, and M. Li, "Privacy-preserving public auditing for shared cloud data supporting group dynamics," Proceedings of IEEE ICC, pp. 1946-1950, 2013.

10.B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," Proceedings of IEEE INFOCOM, pp. 29042912, 2013.
11.B. Wang, B. Li, and H. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Transactions on Services Computing, vol.8, no.1, pp. 92-106, 2015.
12.C. Liu, J. Chen, L. Yang, et al, "Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates," IEEE Transactions on Parallel and Distributed Systems, vol.25, no.9, pp. 2234-2244, 2014.
13.H. Wang, and Y. Zhang, "On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multicloud Storage," IEEE Transactions on Parallel and Distributed Systems, vol.25, no.1, pp. 264-267, 2014.
14.L. Huang, G. Zhang, and A. Fu, "Privacy-preserving public auditing for dynamic group based on hierarchical tree," Journal of Computer Research and Development, vol.53, no.10, pp. 2334-2342, 2016.
15.Y. Yu, J. Ni, M. Au, et al, "Comments on a public auditing mechanism for shared cloud data service," IEEE Transactions on Services Computing,vol.8, no.6, pp. 998-999 2015.