© 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

A Survey on Privacy Preserving Public Auditing for Shared Data in Cloud

Nikita Kuchankar, Pankti Joshi, Pinky Panday, Shraddha Chopde
Computer Science & Engineering, Nagpur University, Nagpur, Maharashtra, India

ABSTRACT

Public auditing for such shared data while preserving identity privacy remains to be an open challenge. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. In this paper, we propose the first privacy-preserving mechanism that allows public auditing on shared data stored in the cloud. Our experimental results demonstrate the effectiveness and efficiency of our proposed mechanism when auditing shared data.

Keywords: Data Storage, Privacy Preserving, Public Auditability, Cryptographic Protocols, Cloud Computing, Third Party Auditor.

I. INTRODUCTION

Cloud computing has been envisioned as the next-generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history like on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. The Cloud server allows the user to store their data on a cloud without worrying about correctness & integrity of data. Cloud data storage has many advantages over local data storage.

The user can upload their data to the cloud and can access those data anytime anywhere without any additional burden. The User doesn't have to worry about storage and maintenance of cloud data. But as data is stored at the remote place how users will get the confirmation about stored data. Hence Cloud data storage should have some mechanism which will specify storage correctness and integrity of data stored in a cloud. The major problem of cloud data storage is security. Cloud is used not only for storing data, but also the stored data can be shared by multiple users. Due to this, the integrity of cloud data is subject to doubt. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to the user. Sharing data among multiple users is perhaps one of the most engaging features that motivate cloud storage.

A. Advantages

- Public auditability
- Storage correctness
- Privacy-preserving
- Batch auditing

B. Drawback

- Late to recover data loss or damage.

II. OBJECTIVES

- **Public Auditing:** The third party auditor is able to publicly verify the integrity of shared data for a group of users without retrieving the entire data.
- **Correctness:** The third party auditor is able to correctly detect whether there is any corrupted block in shared data.
- **Unforgeability**: Only a user in the group can generate valid verification information on shared data.
- **Identity Privacy:** During auditing, the TPA cannot distinguish the identity of the signer on each block in shared data.

III. EXISTING SYSTEM

As data integrity and the security is the main important thing in a cloud, to provide full security and data integrity we are giving public auditing process. Our scheme performs both public auditing and data dynamic operation. For public auditing process, we are using here Hashing technique in which hash function is applied to the user's data. The data dynamic performs an operation like insert, update, and delete in a blockwise manner. TPA does the auditing process. Again we extend our concept in which multiple users access to cloud storage simultaneously through batch auditing. TPA batch multiple auditing task together and audit at one time. So it reduces the time for auditing process.

In our proposed work we are giving multiple TPA for auditing process. As there are problems like users load, system crash, system failure at this situation multiple TPA do the auditing process in which if there is the failure of one TPA another TPA do the auditing process by taking backup of first TPA.Again we are giving here ring signature concept in which we are using HARS (Hemimorphic Authenticable Ring Signature) scheme. In this scheme, a group of users can access the CS and they share data in the group. Any user in a group does the update, delete operations. The system model for our scheme is given below.

A. The System Model: The system model consists three different entities: the cloud user, the cloud server (CS) and the third party auditor (TPA). The cloud user is the one who has a large number of data files that are stored in the cloud; the cloud server is the one who provides the data storage service like resources, software to the user. The Cloud Server can maintain the reputation for its self-serving. The CS might even decide to hide these data correction incidents to the user. So that's why here we are giving third- data files that are stored in the cloud; the cloud server is the one who provides the data storage service like resources, software to the user. The cloud server is managed by cloud service provider; the third- party auditor is the one who has a belief to access the cloud storage service for the benefit of the user whenever user request for data access. The TPA has capabilities and competence that the user does not have. They can also interact with cloud server to access the stored data for the different purpose in different style. Every time it is not possible for the user to check the data which is stored on a cloud server that arrives online burden to the user .so that's why to reduce online burden and maintain that integrity cloud Figure 1.The architecture of cloud data

Storage. The user may resort to TPA. The data stored on the cloud server comes from internal and external attacks, which is having data integrity threads like hardware failure, software bug, hackers, and management errors. party auditing service for users to gain belief in the cloud.

B. Design Goals: The data integrity and security can be achieved by enabling privacy public auditing for cloud data storage as given below:

1. Privacy-preserving: TPA can't see the user's data content during the auditing process.

2. Public Auditability: To allow TPA to verify the correctness of cloud data without demanding the copy of whole data.
3. Batch Auditing: TPA handles multiple users for multiple tasks during the auditing process.
4. TPA performs auditing process with minimum communication.
5. Identity privacy: The TPA cannot identify the identity of the signer of each block when auditing process going on.

IV. LITERATURE SURVEY

- **A survey on Privacy-Preserving Public Auditing for Data Storage Security:** The Cloud computing is the latest technology which provides various services through internet. The Cloud server allows the user to store their data on a cloud without worrying about correctness & integrity of data. Cloud data storage has many advantages over local data storage. The user can upload their data to the cloud and can access those data anytime anywhere without any additional burden. The User doesn't have to worry about storage and maintenance of cloud data. But as data is stored at the remote place how users will get the confirmation about stored data. Hence Cloud data storage should have some mechanism which will specify storage correctness and integrity of data stored in a cloud. Many researchers have proposed their work or new algorithms to achieve security or to resolve this security problem. In this paper, we propose a new innovative idea for Privacy-Preserving Public Auditing with watermarking for data Storage security in cloud computing.

- **Privacy-Preserving Public Auditing for Secure Cloud Storage:** The cloud storage has a lot of problems with the security and data Integrity. So we need to prevent the all problems without the burden of local data storage and maintenance. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to the user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing.

- **Privacy-Preserving Public Auditing for Secure Cloud Storage:** Using Cloud Storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to the user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.

V. CONCLUSION

Using the Third party verifier our stored data are secure the server can not able to view without the client permission. If the server modifies the data the

alert message can be given by the third party verifier to the client mail.

VI. REFERENCES

[1]. Boyang Wang, Student Member, Baochun Li, Senior Member, and Hui Li, Member,"Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud".

[2]. C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage".

[3]. D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses".

[4]. N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service,".

[5]. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S Yau,"Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds,".

[6]. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems.