A Survey of Privacy Preserving Auditing Techniques for Shared Data in Cloud Computing

Ridham Kapadiya
Research Scholar
Department of Computer Science
Parul Institute of Technology, Vadodara, Gujarat

Jignesh Prajapati
Assistant Processor
Department Of Computer Science
Parul Institute of Technology, Vadodara, Gujarat

ABSTRACT
Now a days, cloud computing can be termed as service provider on demand. It has become centralized data storage for the huge amount of data. A user must be concerning about the protection and correctness of his data when he outsources his data to remote data storage as a cloud. Public auditing mechanism enables a user to verify the correctness and integrity of his data with the use of Third Party Auditor (TPA). Public auditing techniques perform auditing task without downloading the whole file. This reduces server overhead. Privacy preserving public auditing do not reveal the identity of the user. This paper describes various privacy preserving public auditing techniques. It also shows comparative study among them.

Keywords
Cloud computing, Shared Data, public auditing, identity, privacy

1. INTRODUCTION
Cloud computing is the computing of the large number of connected devices in terms of data storage and online access. It can be stated as an internet service provider in terms of software/application, platform or infrastructure which are known as Software-As-a-Service(SAAS), Platform-As-a-Service(PAAS) and Infrastructure As a Service(IAAS) corresponding. Cloud computing has number of benefits like Scalability, Reliability, Reduction in cost, Availability, Data Storage, Online access, Pay Per Use, Device diversity and location independent etc.

On the other hand, cloud computing has several threats as Security , Load balancing, Task scheduling etc. Data stored at remote device faces number of threats like unauthorized access, data loss, data leakage, in secure API, Abuse use of cloud etc. Cloud provides ease of integration of data but it also faces threats related to integration. Remotely stored data should be tested in such a way that it can clarify the TPA if the data is retrievable or not. Privacy Preserving Public auditing works on the same principle. It checks the integrity of data and also verify the correctness of the data without disclosing the identity of the user.

Recently, these mechanisms [5], [6], [7], [8], [9], [10], [11], [12], [13] have been proposed public auditing which can verify the data without retrieving the whole data a client's data can be checked by Provable data possession (PDP), proposed by Ateniese et al. [9]. It allows a verifier to stored at an untrusted server.

This paper includes the study of various privacy preserving public auditing techniques. The rest of the paper is organised as follows. Section II contains system and threat model of privacy preserving public auditing techniques and their design objectives. After that detailed description of various existing mechanism for privacy preserving public auditing techniques in section III. Section IV gives the comparative study of all the mechanisms described. Finally, the whole paper is concluded in section V.

2. THE SYSTEM AND THREAT MODEL [1]
System Model [1]:

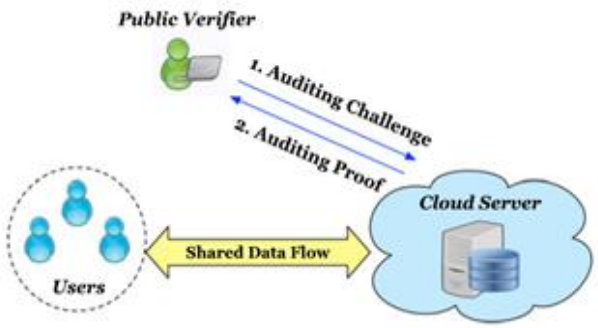

Figure:1 System Model that includes cloud server, a group of users and public verifier[1]

As shown in the figure (1), the system model includes three parties: 1)Cloud server, that stores the data, 2)Public verifier: It verifies the correctness and integrity of data, stored at remote server. 3)Group of users: It involves the number of users.

There are two types of users in the group: 1)The original user, who creates initial file initially that is shared across the group in the cloud, 2)Group users, are the users which uses the shared file.

when a public verifier wants to check the integrity of the data, it sends auditing challenge to the cloud server. The cloud server sends the auditing proof,in the response of that which contains possession of shared data. Than by verifying the correctness of the auditing proof, public verifier checks the correctness of the data.

Threat Model:
1)Integrity Threats: Two kind of threats are possible about integrity. One is, a attacker may try to corrupt the data that is remotely stored in the cloud. The another is, cloud server provider may corrupt data inadvertently due to hardware failure and human errors.

2)Security Threats :A public verifier can diclose the user's identity during the process of auditing which can easily distinguish a high-value target, may be a particular user in the group from others.

Design Objectives:
Privacy preserving mechanisms should achieve following properties:

1)Identity Privacy: A public verifier cannot disclose the identity of user.

2)Correctness: A public verifier should verify the integrity of shared data correctly.

3)Public auditing: The integrity of the shared data must be verified publically without retrieving the entire data from the cloud server.

3. VARIOUS EXISTING MECHANISM FOR PRIVACY PRESERVING PUBLIC AUDITING TECHNIQUES

First of all, Oruta[1] was introduced as a privacy preserving public auditing mechanism. It is a public auditing with identity privacy which does not reveal the identity of the user. Oruta uses the HARS (Homomorphic Autheticable Ring signature) scheme which is the digital signature based on bilinear map. Homomorphic authenticators are used to store the blocks of the data which has unique properties: correctness, unforgeability, block less verifiability, non malleability and identity privacy.

Oruta works on five algorithms:

- KeyGen: users generate their own public/private key pairs.
- SigGen: a user computes ring signatures on blocks in shared data by using its own private key and all the group members' public keys.
- Modify: Each user in the group is able to perform an insert, delete or update operation on a block. It computes the new ring signature on the modified block.
- ProofGen :It is operated by a public verifier and the cloud server together to interactively generate a proof of possession of shared data.
- ProofVerify : The public verifier audits the integrity of shared data by verifying the proof.

Whenever a user updates any block of the data, a ring signature is computed by using its private key any public key. A signature on any block is computed by using SigGen algorithms. These signatures are verified by ProofVerify algorithm. As it has achieved an unforgeability, none of the user can generate the signature on the block except group user. Hence it provides security to the shared file in terms of authentication.

However, Oruta is not capable to trace the identity of any user on misbehaviour and revoke. It also fails in providing the data freshness.

Another technique Knox[2] is also introduced, which is the privacy preserving auditing technique. It is also based on homomorphic MAC which reduces the space to store the verification data, with group signature. Homomorphic MAC used in this technique uses pseudo-random function. Knox uses Homomorphic authenticable Group Signature scheme, which extends BBS group signature and BLS signature in terms of achieving block less verifiability and unforgeability correspondingly.

Knox works on six algorithms:

- KeyGen: It computes user's private and public key.
- Join: The original user adds another user in the group.
- Sign: Any user i, computes the signature.
- ProofGen: :It is operated by a public verifier and the cloud server together to interactively generate a proof of possession of shared data.
- ProofVerify : The public verifier audits the integrity of shared data by verifying the proof.

Knox is performed on the a group of users which have a group manager which can revoke the user on his misbehavior.

AFS-Authenticated File System[3] is also a privacy preserving mechanism which is the completely same as Oruta except data freshness. It works on authenticated file system. It verifies the freshness of the data while performing the file operations. They guarantee data freshness with two layers : Lower layer stores a MAC for each block that enables random access. A version number is also associated with the MAC block which is incremented by each update. The upper layer consists of Markle tree. Block verions are stored by its leaves while hashes of children are stored by internal nodes. The freshness of the file data block can be verified by the Mac block and the freshness of the block version.

The another privacy preserving technique is introduced by C. Wang in[4]. It uses the homomorphic authenticator with random masking. This scheme includes the linear block of the data sampled by random masking generated by pseudo random function in the server's response. The scheme is followed in two section:

- SetUp:
  1) System's public and private parameters are generated using KeyGen algorithm by user. While SigGen algorithm is used to generate signature on the block of the data file.
- Audit:
  2)During the auditing process, the "chal" message is generated by using the randomly chosen permutation key. "chal" message contains the location of the block that to be verified.

  3)when server receives "chal " message, it runs GenProof to generate proof of the data storage.

While on the response on server, TPA runs VerifyProof to validate the response by using the verification defined. This mechanism can be extended into multiple auditing tasks in a batch manner.

4. COMPARATIVE STUDY AMONG THE VARIOUS TECHNIQUES

As per described above, different mechanisms are introduced for privacy preserving public auditing techniques. Among all the mechanism, Oruta and AFS works on ring signature which is based on identity privacy. But both of them are unable to trace the identity of the user on the misbehavior. Knox is based on group signature, which is able to trace the identity of user on the misbehavior and can be revoked by using group manager's private key. This can be carried out by group manager only. All of above techniques uses the homomorphic authenticators with different schemes. For the data freshness,

Oruta, knox and the other mechanism[4] do not contain data freshness while AFS has achieved that feature.

Table 1: Comaparion of various mechanisms in terms of features

Privacy Preserving Mechanisms	Traceability	Data Freshness	Random Masking
Oruta			✓
Knox	✓		
AFS		✓	✓
c. Wang Technique[3]			✓

5. CONCLUSION

We have shown the various privacy preserving techniques for public auditing and their comparative study also. From that, we can conclude that all the techniques yet not achieved the batch auditing that perform multiple auditing tasks. They can be expanded further in terms of the lacking behavior or also for adding up batch auditing into them. We have shown that different techniques use different mechanism and schemes to authenticate and also verify the correctness of the blocks. Most of the techniques are protected from the attackers due to its unforgeability. Privacy preserving mechanisms are used in the applications where user's identity is most confidential.

6. REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2012.

[2] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS'12),pp. 507-525, June 2012.

[3] P. Maheswari, B. Sindhumathi, " AFS: Privacy-Preserving Public Auditing With Data Freshness in the Cloud ", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 PP 56-63

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-610, 2007.

[6] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90-107, 2008.

[7] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,"Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), pp. 213-222, 2009.

[8] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.

[10] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems,"Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.

[11] 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," Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, 2011.

[12] N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM,2012.

[13] B. Wang, B. Li, and H. Li, "Certificateless Public Auditing for Data Integrity in the Cloud," Proc. IEEE Conf. Comm. and Network Security (CNS'13), pp. 276-284, 2013.