Survey Paper on Public Auditing Scheme providing Privacy for Cloud Data with Group Users

[1]Miss. Deliya p. Dhargalkar , [2]Prof. G.M. Kadam

[1] Deliya P. Dhargalkar. Student, Computer Engineering, SKN SIT'S Lonavala, Maharashtra, India
[2]G.M.Kadam. Guide, Computer Engineering, SKN SIT'S Lonavala, Maharashtra, India

ABSTRACT

In this paper, we propose privacy-preserving mechanism which supports public auditing on shared data stored in the cloud. In this, we exploit ring signatures to compute verification metadata needed for auditing the correctness of shared data. The identity of the signer on each block in shared data is kept to be private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. Instead of verifying auditing tasks one by one we can do it simultaneously. The propose system is, a privacy-preserving public auditing mechanism for shared data in the cloud. In this we utilize ring signatures to construct homomorphism authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, but it cannot recognize who is the signer on each block. To make improvement in the efficiency of verifying multiple auditing tasks, we extends our mechanism to support batch auditing. There are two problems we can continue to study for our future work. One is traceability, this means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations.

Keywords- *Homomorphic verifiable, Data integrity, Authorized Auditing*

1. INTRODUCTION

With the help of many shared data applications like Google docs ,Dropbox users can easily shared and access data anywhere. The data stored in cloud can be easily modify or shared by the users. These cloud servers are vulnerable to human errors, software faults and inevitable hardware failure so the data stored on cloud may be lost or corrupted. To ensure the integrity of the data some schemes allows to third party auditing on the data. In this approach the valid signature is placed with each data block and the third party auditor checks these valid signature of the data owner on each data block. But these reveals the identity and some sensitive information about data owners to the third party auditor.

2.LITURATURE SURVEY

1) Privacy-Preserving Public Auditing for Secure Cloud Storage Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou

Advantages

- Author proposed privacy-preserving public auditing system for data storage security in Cloud Computing.
- In this paper, the homomorphism linear authenticator and random masking is used to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which eliminates the burden of cloud user from the tedious and possibly expensive auditing task, and also alleviates the user's fear of their outsourced data leakage.
- It is provably secure and highly efficient.

Techniques: Homomorphism linear authenticator and random masking using MAC.

Disadvantage:

- The individual auditing of the growing tasks can be tedious.
- The technique of public key based homomorphism linear authenticator, which enables TPA to perform the auditing without demanding the local copy of data and this will reduces the computation overhead and communication as compared to the straightforward data auditing approaches.

2) Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data
(Y. Prasanna, Ramesh)
Advantages:

- The efficient and secure ranked multi-keyword search on remotely stored encrypted database model where the database users are protected against privacy violation.
- This increases the efficiency of the scheme by using symmetric-key encryption method rather than public- key encryption for document encryption.
- The ranking method proves to be efficient to return highly relevant documents corresponding to submitted search terms.

Techniques: Ranking method, Symmetric key Encryption.
Disadvantages:

- The computation and communication costs of this method are quite large since every search term in a query requires several homomorphism encryption operations both on the server and the user side.
- They retrieving all files containing the queried keyword further incurs unnecessary network traffic.

3) Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud(Boyang Wang, Baochun Li and Hui Li ,Xi'an)
Advantages:

- Oruta, the TPA is able to efficiently audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can preserve identity privacy for users.
- We perform ring signatures to compute the verification information needed to audit the integrity of shared data.
- The identity of the signer on each block in shared data is to be kept private from a third party auditor (TPA), without retrieving the entire file TPA is able to verify the integrity of shared data.
- They share the data effectively and competent.

Techniques: Ring signature
Disadvantages:

- To hide identity from the TPA, because the identities of signers on shared data may indicate that a particular user in the group or a special block in shared data is a more valuable target than others.
- The information is confidential to the group and should not be revealed to any third party.

4) Panda- Public Auditing for Shared Data with Efficient User Revocation in the Cloud
(Boyang Wang, Baochun Li, and Hui Li)
Advantages:

- The public auditing mechanism for shared data with efficient user revocation in the cloud.
- When a user in the group is revoked, proposed system allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures.
- This will save a significant amount of computation and communication resources during user revocation.

Techniques: Resigned techniques
Disadvantages:

- The revoked user should not be able to access and modify shared data.
- The integrity of the entire data can be verified with the public keys of existing users only.

5) Remote Data Checking for Network Coding-based Distributed Storage Systems(Bo Chen, , Giuseppe Ateniese)
Advantages:

- RDC scheme is secure and efficient for network coding-based distributed storage systems that rely on untrusted server..
- RDC-NC scheme can be used to ensure data remains intact when faced with data corruption, replay, and pollution attacks.
- The RDC-NC is inexpensive for both clients and servers.

Techniques: Remote Data Checking.
Disadvantages:

- The code is not systematic; it does not embed the input as part of the encoded output.

- Small portions of the file cannot be read without reconstructing the entire file.
- Online storage systems do not use network coding, because they prefer to optimize performance for read (the common operation).

3. CONCLUSION

We propose a privacy-preserving mechanism that supports public auditing on shared data which is stored in the cloud. This approach preserve the identity of the signer and shared data during third party auditor.

4.ACKNOWLEDGEMENT

I would like to thanks to our guide Prof. G.M. Kadam. & respected teachers for their great support and motivation for us. Our sincere thanks to SKN Sinhagad Institute of Technology and Science to develop our skill and capabilities.

5.REFERENCES

- 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.
- 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.
- Anmin Fu, Shui Yu, Yuqing Zhang, Huaqun Wang, and Chanying Huang," NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users"
- Y. Prasanna, Ramesh,"Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data"IJCST Vol. 3, Iss ue 3, July - Sept 2012.
- Bo Chen, Reza Curtmola,Giuseppe Ateniese, Randal Burns,"Remote Data Checking for Network Coding-based Distributed Storage Systems", CCSW'10, October 8, 2010, Chicago, Illinois, USA.