Review on Preserving Privacy Identity of Shared Data in Cloud

Deepak.A
Student (M Tech) Dept. of Computer science & Engineering
Sai Vidya Institute Of Technology
Bangalore, India
deepugowda26@gmail.com

Mary D'souza
Asst. Prof. Dept of Information Science & Engineering
Sai Vidya Institute Of Technology
Bangalore, India
marymdsouza@gmail.com

Abstract :- Cloud computing contains groups of remote servers and software networks that involve in allowing storage of data and accessing of online computer resources. Cloud contains data storage to the huge amount of data. Cloud user should be concerned with the correctness and protection of data. When user outsources remote data from storage of data as a cloud, There are Several auditing mechanism to verify the Integrity of Data. Public auditing mechanism enables the user to verify integrity of data with the help of Third Party Auditor (TPA). Public auditing mechanism start auditing task by not downloading whole file. This helps in Preserving privacy of Data. Public auditing will won't reveal identity of any user. In the paper contains various privacy preserving public auditing mechanism. It also shows comparative study among them.

Keywords:- *Cloud computing, Identity, Privacy, Data sharing, Third Party Auditor, Public auditing*

*****

I. INTRODUCTION

Cloud computing contain technology generating architecture for the enterprise due to its big advantages because of that IT based on demand it giving self service. It has got good advantage because of its location independent feature. Cloud is used in many IT industries like new technology. It maintain storage in cloud storage and it is flexible whenever user upload data in cloud storage it allow user for accessing all documents from any place in the world. Cloud also gives security to the uploaded data of the users. As a result integrity is also maintained in the cloud. For verification of integrity just downloading data is not the solution because of more expense in output, input and cost of transmission over the network. Checking Integrity is more important in enabling auditing of data in the cloud storage, here Third party auditor is responsible for auditing the data in the cloud so that user can check the correctness of data in the clod storage. Using this cloud service provider can be able to improve the platform to business. Third party auditor will not be knowing the data within it, just he/she will verify the integrity of data. By using the cloud services user can benefit of what they needs.

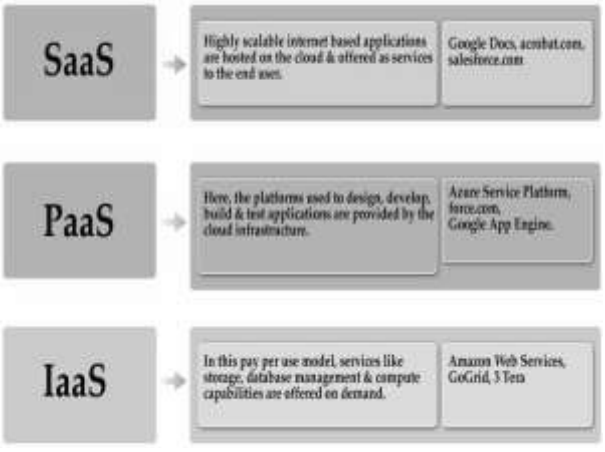

Figure 1. SERVICE MODELS

This paper includes the study of various privacy preserving public auditing mechanisms. This paper is organized as follows. Section II contains Identity Privacy and threat model of privacy preserving public auditing mechanism and their design objectives. After that detailed description of various mechanism in preserving privacy identity public auditing mechanism in section III. Section IV gives the comparison of all the mechanisms. Finally, the conclusion in section V.

II. IDENTITY PRIVACY AND THREAT MODEL[1]

A. Identity Privacy:

Preserving identity privacy from the Third party Auditor is more important, because identities of the signers on shared data says that a particular user in group or special block with in shared data has higher valuable target than others.[1]

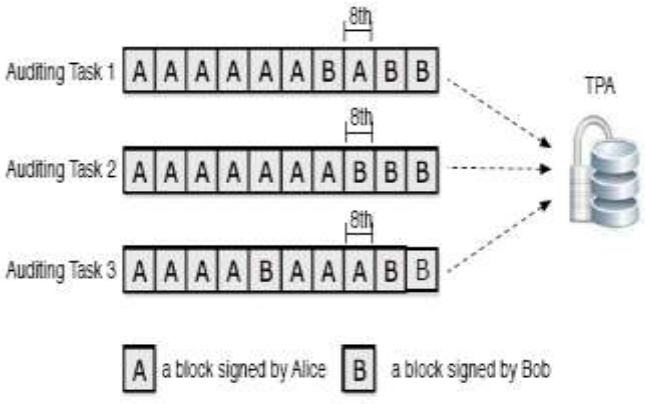

Figure 2. IDENTITY PRIVACY

In the above fig.2 showing Alice and Bob work together as the group and share the data in the cloud. The shared data is divided into a number of blocks, which are independently signed by data owner. Once the block in shared data is modify by a user, that user will have to sign in new block using his public or private keys. Third party Auditor should be knowing the identity of signer on each block in this shared data, therefore that it is able to audit integrity of the whole data

based on requests from Alice or Bob. After doing several auditing tasks, Private and sensitive information will have chances to be reveal to the TPA. Some of the blocks in shared data are signed by Alice, which will indicate that Alice has a important role in the group. Previously, several mechanisms have been proposed which are [5], [6], [7], [8], [9], [10] public auditing technique, which will verify the data without obtaining the whole data a user data can be checked by Provable data possession, proposed by Ateniese et al. [9]. It allows a verifier to stored at an untrusted server. Actual user is responsible to decide who is able to share data before outsourcing data to the cloud. The 8-th block is frequently modified with different data users so that says block may having high value data, consider how auditing the integrity of shared data in cloud on static groups so that means group is predefined before sharing data created on cloud and users membership in the group not changed on th time of data sharing. Auditing of the integrity in shared data on cloud with dynamic groups [7] if any new user added into group and an existing group member can also revoked during sharing data while still preserve identity privacy of data and user. [5]

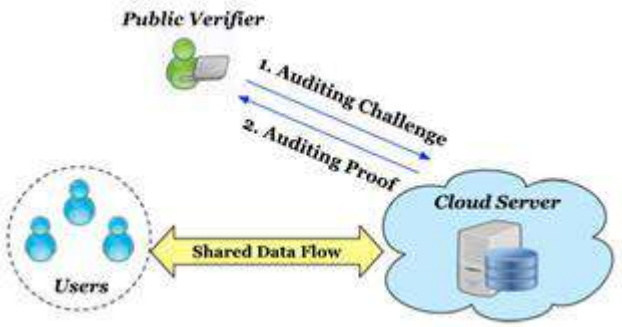

Figure 3. SYSTEM MODEL

Above shown in the fig.3 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.
Here 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, response of that which contains possession of shared data. Than by verifying correctness of auditing proof, public verifier checks the correctness of the data.

B. 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: Public verifier can disclose the user's identity during the process of auditing which can easily distinguish a high target value, may be a particular user in the group from others.

III. DIFFERENT MECHANISMS IN PRESERVING PRIVACY IDENTITY PUBLIC AUDITING

Oruta was introduced as a privacy preserving public auditing mechanism. It is a public auditing mechanism with identity privacy which does not reveal the identity of the user.[11] Oruta uses the HARS (Homomorphic Autheticable Ring signature) scheme which is the digital signature based on bilinear map. Oruta will support dynamic operations on shared data, dynamic operation contains an insert, delete, update operation on a single block. [5][6] Since the computation of a ring signature contains an identifier of block which use index of the block as its identifier[8]. Reason is when user modifies single block in data shared by performing insert or delete operation, Also that content of these blocks not modified. Homomorphic authenticators is used to store blocks of data which wil have unique properties: correctness, block less verifiability, unforgeability, non malleability and identity privacy. Oruta works on five algorithms:

- KeyGen: Here Users will generate their own public/private key pairs.
- SigGen: Here User needs to compute the ring signatures on the blocks in shared data by using private key and group members' public keys.
- Modify: Here User of group are able to perform insert, delete or update operation in the block. It computes the new ring signature on the modified block.
- ProofGen: It is operated by a public verifier, cloud server together interactively it generate proof of possession for 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[3] 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.

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 cloud server both will interactively generate a proof of possession in 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.[3] AFS-Authenticated File System 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:

A. SetUp:

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.

B. Audit:

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. when server receives "chal" message, it runs GenProof to generate proof of the data storage.[9] While on the response on server, TPA checks with by running Verify Proof for validate the response by using the verification defined. This mechanism can be extended into multiple auditing tasks in a batch manner.

IV. COMPARISON WITH THE VARIOUS MECHANISMS

In the below table.1 discussed 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[1][2][3] [4] do not contain data freshness while AFS has achieved that feature.

TABLE I. DIFFERENT MECHAMISM COMPARISON

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

V. CONCLUSION

In this paper we are showing the various public auditing mechanisms for preserving the privacy of data in the cloud. By looking into those factors all the mechanisms yet not worked on the preserving the privacy Identity of the cloud user, it is also an important factor where user identity is also to be preserved. Those factors can be expanded further in terms of the preserving identity of user privacy could give more security future. Here also have shown that different mechanism is using different technique, methods for authentication and also verifying the correctness of the blocks. Preserving user identity is more confidential there are some mechanisms used where user's identity to be preserved.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[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] 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.

[11] Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE Cloud Computing, IEEE Transactions on (Volume:2 , Issue: 1) 13 January 2014

.