International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
www.ioirp.com ISSN: 2394-6364, Volume – 1, Issue – 7. June 2015

A LITERATURE SURVEY ON A PRIVACY PRESERVING PUBLIC VERIFIER MECHANISM FOR SECURE CLOUD STORAGE

[1]Bharath Raj D, [2]Gangadhar M L
[1]Department of Computer Science & Engg, Akshaya Institute of Technology, Tumkur, India
[2]Asst Prof: of Computer Science & Engg, Akshaya Institute of Technology, Tumkur, India
[1]bharath04201@gmail.com, [2]ganga.hosamane@gmail.com

***Abstract*— In Cloud Computing Public verifier on the integrity of shared data is very big issue, because the public verifier scheme will predictably reveal confidential information and identity privacy to public verifiers. This survey, propose a new scheme called a novel privacy-preserving mechanism which supports public verifier on shared data stored in the cloud. In particular, this scheme takes advantage of ring signatures to compute verification metadata. The ring signature scheme is needed to audit the correctness of shared data. With this mechanism, the identity of the signer on each block in shared data is kept secret or private from public verifiers. Public verifiers are one who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, this mechanism is able to perform multiple auditing tasks simultaneously instead of single auditing task. This survey shows the effectiveness and efficiency of our mechanism when auditing shared data integrity.**

I. INTRODUCTION

A. Cloud Computing

Cloud Computing refers to the applications delivered as services. Those services provided over the Internet and the hardware and systems software in the datacenters.

B. Cloud Storage Services

In Cloud Storage Services, Cloud service providers offer users efficient and scalable data storage services.
Those services provided with a much lower marginal cost than traditional approaches. Cloud users influence cloud storage services to share data with others in a group. In cloud computing data sharing becomes a standard feature in most cloud storage offerings, including iCloud and Google Drive.

C. Integrity in Cloud Storage

The integrity of data in cloud storage, however, is subject to uncertainty. Data stored in the cloud can easily be lost or corrupted due to the unavoidable hardware/software failures and human errors. To make this matter even bad, cloud service providers may be unwilling to inform users about these data errors in order to maintain the good status of their services and avoid profit loss. Therefore, the integrity of cloud data should be verified before any data Utilization. Data utilization means search or computation over cloud data.

D. Data Correctness in Cloud

The traditional approach for checking data correctness in cloud includes two steps. The first step is to retrieve the entire data from the cloud, and the second step is to verify data integrity by checking the correctness of signatures by RSA or hash values by MD5 of the entire data. Advantage of this approach is able to successfully check the correctness of cloud data. The disadvantage of this approach is efficiency decreased while using this traditional approach on cloud data.

E. Efficient Processing in Cloud

The efficiency of processing the cloud was very big challenge. The main reason is that the size of cloud data is very huge in general. Downloading the entire cloud data to verify data integrity will increase cost also waste user's amounts of computation and communication resources, especially when data have been corrupted in the cloud. Besides, many scheme like data mining and machine learning does not necessarily need cloud users to download the entire cloud data to local devices.

F. Public Key Infrastructure

The shared file is divided into a number of small individual blocks, where each block is independently signed by one of the two users with Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing scheme. Once a block in this shared file is modified by a user, that particular user needs to sign the new block using his/her secret private key.

Finally, different blocks are signed by various users due to the modification introduced by these different users. Then, in order to correctly audit the integrity or correctness of the entire data, a public verifier needs to choose the suitable public key for each block.

Specifically, as shown in Fig. 1, after performing several auditing tasks, this public verifier can first learn that Alice may be a more important role in the group because most of the blocks in the shared file are always signed by Alice; on the other hand, this public verifier can also easily deduce that the eighth block may contain data of a higher value (e.g., a final bid in an auction), because this block is frequently modified by the two different users. In order to protect this confidential information, it is essential and critical to preserve identity privacy from public verifiers during public auditing.
As a result, this public verifier will inevitably learn the identity of the signer on each block due to the unique binding between an identity and a public key via digital certificates under public key infrastructure (PKI).

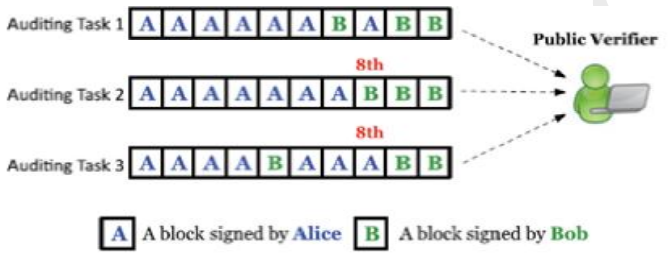

Fig. 1. Alice and Bob share a data file in the cloud, and a public verifier audits shared data integrity

II. EXISTING SYSTEM

[1] In 2007 G. Ateniese, R. Burns, R. Urtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, worked on "Provable Data Possession at Untrusted Stores" This paper explains about Provable data possession (PDP) scheme which allows a verifier to check the correctness of a client's data stored at an un trusted server by utilizing RSA-based homomorphic authenticators and sampling strategies. The advantage of this scheme is the verifier is able to publicly audit the integrity of data without retrieving the entire data, which is referred to as public auditing.

A. Drawback

x This mechanism is only suitable for auditing the integrity of personal data.
[2]In 2009 C. Wang, Q. Wang, K. Ren, and W. Lou, worked on "Ensuring Data Storage Security in Cloud Computing" This method use leveraged homomorphic tokens to ensure the correctness of erasure codes-based data distributed on multiple servers. The major contribution of this mechanism is able support dynamic data, identify misbehaved servers.

- The leakage of identity privacy to public verifiers.

[3][4] In 2010 ,B. Chen, R. Curtmola, G. Ateniese, and R. Burns, worked on "Remote Data Checking for Network Coding-Based Distributed Storage Systems" This paper introduced a mechanism for auditing the correctness of data under the multi-server scenario, where these data are encoded by network coding instead of using erasure codes. This scheme minimizes communication overhead in the phase of data repair.

- This scheme requires two improved schemes.

The first scheme is BLS signatures, and the second one pseudo-random function.
[6] In 2008 G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik worked on, "Scalable and Efficient Provable Data Possession to support dynamic data" This paper presented an efficient PDP mechanism based on symmetric keys. This mechanism can support

update and delete operations on data; however, insert operations are not available in this mechanism. It exploits symmetric keys to verify the integrity of data, it is not public verifiable.

- This scheme provides a user with a limited number of verification requests.

[5][7]In 2007 A. Juels and B.S. Kaliski, worked on "PORs: Proofs of Retrievability for Large Files" .This paper provide POR's scheme which is also able to check the correctness of data on an untrusted server. The original file is added with a set of randomly-valued check blocks called sentinels. The verifier challenges the untrusted server by specifying the positions of a collection of sentinels and asking the untrusted server to return the associated sentinel values. Sentinel Based POR protocol is amenable to real-world application.

- Only focus on personal data in the cloud.

Integrity Threats: First, an adversary may try to corrupt the integrity of shared data. Second, the cloud service provider may inadvertently corrupt (or even remove) data in its storage due to hardware failures and human errors. Making matters worse, the cloud service provider is economically motivated, which means it may be unwilling to inform users about such corruption of data.

Privacy Threats: The identity of the signer on each block in shared data is private and confidential to the group. During the process of auditing, a public verifier, who is only allowed to verify the correctness of shared data integrity, may try to reveal the identity of the signer on each block in shared data based on verification metadata.

III. PROPOSED SYSTEM

[7] In this survey, to solve the privacy issue on shared data, this paper produce scheme called Oruta in cloud computing scenario. Oruta is a novel privacy-preserving public auditing mechanism. More specifically, this survey utilizes ring signatures. The ring signatures used to construct homomorphic authenticators in Oruta scheme, by using this public verifier is able to verify the integrity/correctness of shared data without retrieving the original data fully.

In Oruta scheme the identity of the signer on each block in shared data is kept private/secret from the public verifier. In addition, Oruta scheme is to be extensive to support batch auditing. The batch auditing can perform multiple auditing tasks simultaneously instead of doing single task. Multiple auditing tasks is used to improve the efficiency of verification methods. Meanwhile, Oruta is well-matched with random masking technique. This method was utilized in WWRL and can preserve data privacy from public verifiers. Moreover, this scheme also influence index hash tables from a previous public auditing solution to support dynamic data. The proposed ORUTA (One Ring to Rule Them All) design a new homomorphic authenticable ring signature (HARS) scheme. The HARS is extended from a classic ring signature scheme. The ring signatures generated from HARS preserve identity privacy and also able to support block less verifiability.

ARCHITECUTURE

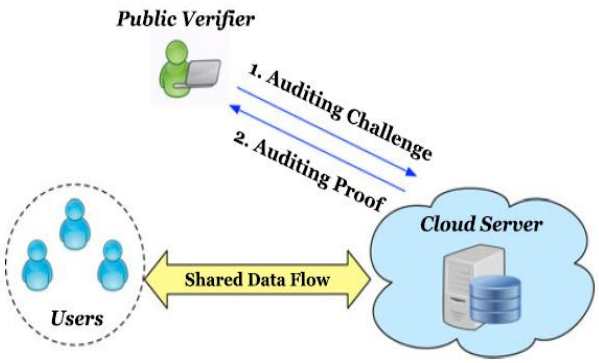

Fig 2: Verification from TPA to share the data to cloud users

HARS contains three algorithms: KeyGen, RingSign and RingVerify.

- KeyGen: Each user in the group generates his/her public key and private key.

- RingSign: A user in the group is able to generate a signature on a block and its block identifier with his/her private key and all the group members public keys. A block identifier is a string that can distinguish the corresponding block from others.

- RingVerify: A verifier is able to check whether a given block is signed by a group member in Ring Verify.

SUMMARY OF CHARACTERISTICS OF THE PRIVACY PRESERVING PUBLIC AUDITING SCHEME VS ORUTA SCHEME

SNO	METHODS	EXISTING (Privacy Preserving Public Verifier Scheme)	PROPOSED(ORUTA)
1	Technique	x Provable data possession (PDP) x Proofs of Retrievability (POR) x Dynamic Provable data possession (PDP)[5]	ORUTA(One Ring to Rule Them All)
2	Identity of signer	Kept public to public verifier[7]	Kept private from the public Verifier
3	Auditing Task	Single Auditing Task[7]	Multiple Auditing Task

A. OVERVIEW OF PROPOSED SYSTEM

- Public Auditing: A public verifier can able to publicly verify the integrity of shared data without retrieving the whole data from the cloud.
- Correctness: A public verifier is able to correctly verify shared data integrity and correctness.
- Unforgeability: Only a user in the group can generate valid verification code (i.e., signatures) on shared data.
- Identity Privacy: A public verifier cannot differentiate the identity of the signer on each block in shared data during the process of auditing.

IV. CONCLUSION

In this paper, the proposed Oruta method is used to share data in the cloud. Oruta is a privacy-preserving public auditing mechanism. We utilize ring signatures to construct homomorphic authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data. The oruta scheme cannot differentiate the signer on each block. To improve the efficiency of verifying multiple auditing tasks, the ORUTA scheme extended to support batch auditing.

References

[1] 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.

[2] 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

[3] 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 (CC SW'10), pp. 3 1-42, 2010.

[4] 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

[5] A. Juels and B.S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 584-597, 2007

[6] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm'08), 2008.

[7] 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.