SURVEY OF PUBLIC AUDITING IN CLOUD

Ms. Bhor Priti[1], Ms. Kakade Priyanka[2], Ms. Kale Ashwini[3], Miss. Dere Archarana[4]

[1] *Student, Computer Engg., JCOE, Maharastra, India*
[2] *Student, Computer Engg., JCOE, Maharastra, India*
[3] *Student, Computer Engg., JCOE, Maharastra, India*
[4] *Assistant Prof., Computer Engg., JCOE, Maharastra, India*

ABSTRACT

A cloud computing is gaining more popularity as it provides guaranteed services like online data storage and backup solutions, Web-based e-mail services, virtualized infrastructure etc. User is able to access data stored in a cloud anytime, anywhere using internet connected device with less capital investment. Cloud storage stores replica at distributed locations to ensure fast access and fault tolerance mechanism. As cloud is third party service provider there is risk of data security and integrity, so user may encrypt data before sending it to cloud. The integrity of data can be guaranteed by signing data blocks, thus enabling users to confirm integrity of their data. To guarantee public audit, user may put ring signature on data blocks so as to hide identity of himself from third party auditor. In this paper various mechanisms used for public auditing in cloud are reviewed.

Keyword: - *homomorphic signature, ring signature, confidentiality, integrity, public auditing..*

---

1. INTRODUCTION

Cloud computing provides many virtualized resources to users as services across the entire Internet, while hiding platform and implementation details. GMAIL is one of the best examples of cloud storage which is used by most of us regularly [1]. Cloud computing uses virtualization technique and thus hiding platform and implementation details. This provides unlimited resources to users on their devices with just internet connection. Cloud service providers offer highly available storage and massively parallel computing resources at relatively low costs.

Even if cloud provides such amazing services to its clients, there are some problems related to cloud such as security of data stored in cloud and integrity of data. The data security can be guaranteed using encryption technique before sending data to cloud server and integrity of data can be guaranteed by signing data blocks using users signature such that, except user no one can be able to generate similar signature. Even with this provision there is possibility of leakage of data, as the integrity of data is verified by third party auditor thus the data needs to be copied from cloud server to third party auditor and problem starts. As third party auditor can initiate brute-force attack on saved copy of data without client knowledge [1][2]. Often users may want to hide their identity while public auditing. This increases complexity of auditing process. To guaranting privacy and integrity of data various techniques were employed by various researchers and this paper makes study of some of these papers [2][3].

The rest of paper is organized as follows: Section 2 covers literature review and section 3 contains concluding remarks.

2. LITERATURE SURVEY

The traditional approach for checking data correctness in cloud includes two steps. It consists of retrieving the entire data from the cloud to auditor and then verifies data integrity by checking the correctness of signatures by RSA or hash values using MD5 of downloaded 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. 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 [4].

Enabling verifier to publicly audit the integrity of data without retrieving the entire data from cloud server, by utilizing RSA-based homomorphic authenticators or sampling strategies, is referred as a public auditing. But such mechanism is suitable for auditing the integrity of personal data. In such systems, verifier challenges the untrusted server using various ways such as merkle-hash, specific bit values, etc [5].

[2.1]. Ring Signature

Basically ring signature is a technique to hide details of signer of block from auditor, such that one can check integrity of data by computing signatures on block, but he has no way to detect who is real signer of the data block. In this technique, user puts all the signature of group members with its own signature, thus whenever third party auditor sees signature on block he finds all the signature of group members [6].
To make things work in paper [2][6] an approach was used in which each user signs blocks with global private key which is assumed to be distributed to each group member and kept secretly by group members. If one user from the group is leaving the group or compromised, then new global private key is generated and shared among the rest of the group members. This introduces large overhead on users in terms of key distribution and key management.

[2.2]. Trusted Proxy

Another way to hide identity privacy is by employing trusted proxy who manages all the groups and their file uploading, downloading operations. Users uploads there data to proxy server which stores user signatures and signs the data block with its own signature, thus cloud server and third party auditor only sees signature of trusted proxy server enabling identity privacy. But the limitation of this approach is that it; it's a single point failure mechanism in terms of fault tolerance and public auditing. Utilizing group signature is also an alternative way for identity privacy but it does not provide public auditing mechanism [7].
Wang et al. [8] is able to preserve users' data confidentiality from a public verifier by employing random masking. There extended mechanism supports batch auditing using aggregate signatures to operate multiple auditing tasks from different users.

[2.3]. Threat Models

Two types of threats are related to the integrity of shared data, first is adversary may try to corrupt the integrity of shared data and second one is CSP may intentionally or un-intentionally corrupt (or even remove) data from its storage. This may happen due to hardware failures or because of human errors. In such situation, CSP may inform users about such damage to save their reputation [1][8]. Threat model related to privacy focuses on the third party auditor who is chosen for verifying the correctness of stored data integrity. The third party auditor may try to reveal the identity of the signer on each block to gain some information about data or identity of signer of block [1][8].

[2.4]. Homomorphic Authenticators

Homomorphic authenticators (also called homomorphic verifiable tags) are basic tools to construct public auditing mechanisms. The unforgeability, a homomorphic authenticable signature scheme, which denotes a homomorphic authenticator based on signatures, should also satisfy the following properties [8].
Block less verifiability

It allows a verifier to audit the correctness of data stored in the cloud server with a special block, which is a linear combination of all the blocks in data. If the integrity of the combined block is correct, then the verifier believes that the integrity of the entire data is correct. In this way, the verifier does not need to download all the blocks to check the integrity of data [1] [8].
Non-malleability

It indicates that an adversary cannot generate valid signatures on arbitrary blocks by linearly combining existing signatures [8].

[2.5]. Batch Auditing

It also supports batch auditing through which efficiency is improved. It allows TPA to perform multiple auditing task simultaneously and it reduces communication and computation cost. Through this scheme, we can identify invalid response. It uses bilinear signature (BLS proposed by Boneh, Lynn and Shacham) to achieve batch auditing. System performance will be faster [8][9].

[2.6]. Data Dynamics

It also supports data dynamics where user can frequently update the data stored on a cloud. It supports block level operation of insertion, deletion and modification. Author of [6] proposed scheme which support simultaneous public audit ability and data dynamics. It uses Merkle Hash Tree (MHT) which works only on encrypted data. It [10] uses MHT for block tag authentication.

Abhishek Mohta proposed Virtual machines which uses RSA algorithm, for client data/file encryption and decryptions [11]. It also uses SHA 512 algorithm which makes message digest and check the data integrity. The Digital signature is used as an identity measure for client or data owner. It solves the problem of integrity, unauthorized access, privacy and consistency. Dhiyanesh [12] proposed Mac based and signature based schemes for realizing data audit ability and during auditing phase data owner provides a secret key to cloud server and ask for a MAC key for verification.

Jachak K. B. proposed privacy preserving Third party auditing without data encryption. It uses a linear combination of sampled block in the server's response is masked with randomly generated by a pseudo random function (PRF) [13]. Curtmola et al. [14] aim to ensure data possession of multiple replicas across the distributed storage system. They extend the PDP scheme in to cover multiple replicas without encoding each replica separately, providing guarantees that multiple copies of data are actually maintained. In [15], Bowers et al. utilize a two-layer erasure-correcting code structure on the remotely archived data and extend their POR model to distributed scenario with high-data availability assurance.

[2.7]. Proof of Ownership (POW)

The POW protocol allows user to efficiently prove to a cloud server about his ownership, rather than short information about the file such as a hash value. This is somewhat similar to proofs of retrievability (POR) and proofs of data possession (PDPs) with a role reversal here client is the proover is cloud server. Pietro et.al [16] proposed three correlative protocols to achieve an efficient POW. The main idea of their protocols is to challenge random K bits of file F. The probability that a malicious user is able to output the correct value of K bits of the file where each bit is selected at a random position is negligible in security parameter k, but their scheme cannot be adopted for encrypted files.

[2.8]. Proof Of Retrieveability (POR)

A proof of retrievability (POR) is a compact proof by a file system (proover) to a client (verifier) that a target files F is intact, in the sense that the client can fully recover it. As PORs incur lower communication complexity than transmission of F itself, they are an attractive building block for high-assurance remote storage systems. A POR is a protocol in which a server/archive proves to a client that a target file integrity is valid, and thus client can recover their files whenever needed. In traditional POR, client needs to download file F and check the digital signature of that file to guarantee integrity [17]. The client can pre-process the file before uploading and insert some secret in that file, such that it can be used for checking consistency of file in PORs / PDPs technique.

4. CONCLUSIONS

This paper discusses a privacy-preserving public auditing mechanism for shared data in the cloud and utilization of ring signatures to construct homomorphic authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block.

REFERENCES

[1]. 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.

[2]. 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.

[3]. 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.

[4]. R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 552-565, 2001.
[5]. K Govinda, V. Gurunath Prasad and H. sathis Kumar, "Third Party Auditing for Secure Data Storage in Cloud Through Digital Signature Using RSA", International Journal of Advanced science and Technical Research, vol4,no. 2, ISSN: 2249-9954,4 August 2012
[6]. R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 552-565, 2001.
[7]. R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems,"Comm. ACM,vol. 21, no. 2, pp. 120-126, 1978.
[8]. C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.
[9]. D. Boneh, C. Gentry, B. Lynn, and H. Shacham , "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT'03), pp. 416-432, and 2003.
[10]. Juels, B. Kaliski. "Pors: proofs of retrievability for large files[C]", Proceedings of CCS 2007. Alexandria, VA, USA, 2007. Pp 584-597.
[11]. Abhishek Mohta, Lalit Kumar Awasti, "Cloud Data Security while using Third Party Auditor", International Journal of Scientific & Engineering Research, Volume 3,Issue 6, ISSN 2229-8 June 2012.
[12]. B. Dhiyanesh "A Novel Third Party Auditability and Dynamic Based Security in Cloud Computing" , International Journal of Advanced Research in Technology, vol. 1,no. 1, pp. 29-33, ISSN: 6602 3127, 2011
[13]. D. Shrinivas, "Privacy-Preserving Public Auditing in Cloud Storage security", International Journal of computer science and Information Technologies, vol 2, no. 6, pp. 2691-2693, ISSN: 0975-9646, 2011
[14]. 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.
[15]. K.D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Proc. ACM Conf. Computer and Comm. Security (CCS '09), pp. 187-198, 2009.
[16]. Pietro, R.D., Sorniotti, "Boosting Eciency and Security in Proof of Ownership for Deduplication", ACM Symposium on Information, 2012.
[17]. A. Juels and B. Kaliski. "PORs: Proofs of retrievability for large files". Proceedings of CCS 2007 , pages 584{97. ACM Press, Oct.2007.