Survey on Privacy Preserving Public Auditing for Shared Data in Cloud

Pooja Kapadne

Computer Science, K. J. Somaiya College of Engineering, Vidyavihar, Mumbai, Maharashtra, India.

Email: pooojamk@gmail.com

Abstract --- Todays growing technologies and services have gave the profound platform to new technique called cloud computing. Cloud computing is gaining immense importance in todays' business and organizational platforms due to availability of required resources to the user anytime-anywhere. Sharing data among multiple users is perhaps one of the most engaging features that motivates cloud storage. Therefore, it is also necessary to ensure the integrity of shared data in the cloud is correct. The data stored on cloud is subject to skepticism due to existence of hardware and software failure and human errors. Moreover Cloud Service Provider (CSP) may not inform data owner about its data loss to safeguard its reputation and business. So, there is a need for a mechanism to allow data owner and public verifier to efficiently audit cloud data integrity without retrieving the entire data from the cloud. In addition it must not reveal the identity of the signer on each block of data to the public verifier. Ring signatures are used to compute the verification metadata needed to audit the correctness of shared data. The introduced mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one.

Keywords--- cloud computing, public auditing, privacy preserving, public verifier, ring signatures, homomorphic authenticable ring signatures (HARS).

INTRODUCTION

Cloud computing is one if the hottest buzzwords in technologies. It is the use of technology that provides access to its users to various services that it provides. The emergence of this new technology allows users to access their files, software and computing power over the web. Many small scale businesses and organization can establish its infrastructure without the need for implementing actual hardware and software that are needed to build entire structure as it can entirely rely on the cloud services and use its resources on pay per use basis. But as coin has two sides so do the technology, with this advent of technology where data is easily stored and available on cloud; there are various threats challenging the data security and integrity.

The data stored on cloud is in shared form which invites the threats like loss or corruption of data due to software, hardware or human errors [3]. Moreover, the cloud service providers (CSP) may be reluctant to inform the data owner about the data theft or corruption due to fear of losing their reputation and business profit. So, to address this issues, Public Verifiers are used. A public verifier could be data user who would like to utilize the owner's data via cloud or third party auditor (TPA) who can provide expert integrity checking services.

There are many approaches [9] [10] to check the correctness of the data stored on the cloud, like the traditional approach is to retrieve the entire data from the cloud to check its correctness. But, this approach wastes users' amount of computation and communication resources and of course the time and cost.

Thus the technique called Public Auditing [8] is being used to allow data owners and public verifiers to check the integrity of the data without the need to download the entire data from cloud. This mechanism divides data into many small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking. However this approach leads to an issue where the identity of the signer is revealed to public verifier leading to situation of leaked identity privacy. The public verifier will 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). As a result, public auditing may put various confidential data at risk. In order to protect the confidential information, it is essential and critical to preserve identity privacy from public verifiers during public auditing.

The proposed paper will address above issue on shared data via novel mechanism that preserves privacy of data in public auditing. Ring signatures are utilized to construct homomorphic authenticators so that public verifier can check the integrity of shared data without disclosing the identity of the singer to public verifier. The batch auditing mechanism allows to perform multiple auditing tasks simultaneously.

SYSTEM FLOW

As shown in figure 2.1, the system consists of three parties which are: cloud server, public verifier and group of users. The user can be the original user or group users. The original user is responsible for creating shared data in the cloud, and shares it with group users. Both the original user and group users are members of the group. Every member of the group is allowed to access and modify shared data. Both shared data and its verification metadata (i.e., signatures) are stored on the cloud server. A public verifier, such as a TPA who provides expert data auditing services or a data user outside the group intending to utilize shared data, is able to publicly verify the integrity of shared data stored in the cloud server. When a public verifier wishes to check the integrity of shared data, it first sends an auditing challenge to the cloud server. After receiving the auditing challenge, the cloud server responds to the public verifier with an auditing proof of the possession of shared data. Then, this public verifier checks the correctness of the entire data by verifying the correctness of the auditing proof.

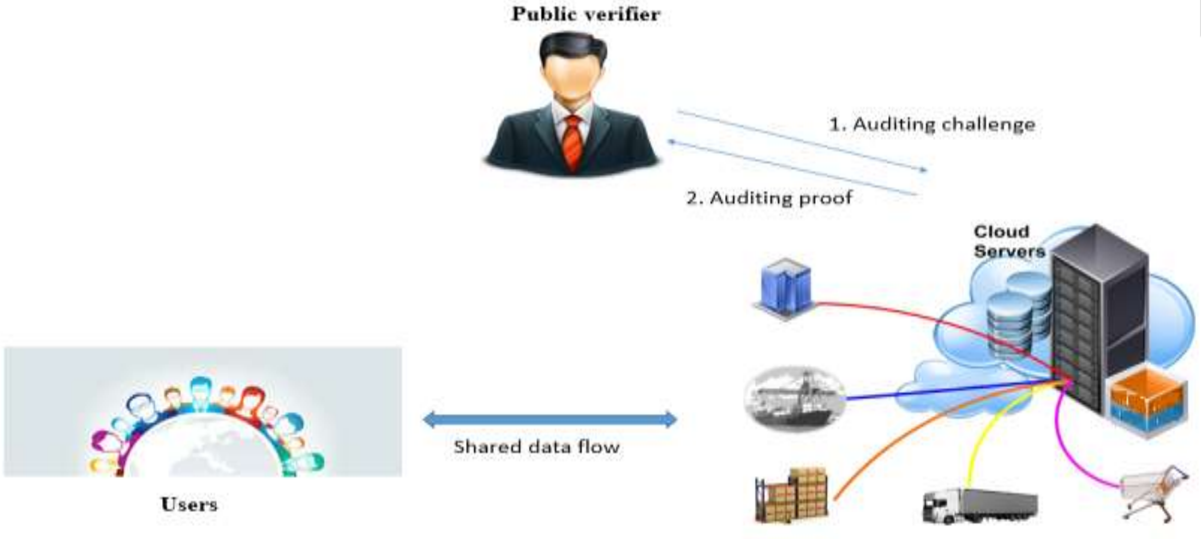

Fig 2.1 System model

Integrity Threats: There are two kinds of threats related to the integrity of shared data. In first threat, an adversary may try to corrupt the integrity of shared data. In second threat, the cloud service provider may inadvertently corrupt (or even remove) data in its storage due to hardware failures and human errors. In worse case the cloud service provider is economically motivated, which means it may be reluctant to inform users about such corruption of data in order to save its reputation and avoid losing profits of its services.

Privacy Threats: The identity of the signer on each block in shared data is private and confidential to the group. In 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. Once the public verifier reveals the identity of the signer on each block, it can easily distinguish a high-value target from others.

Design goals: The main design objective is to design a system that will allow the public verifier to verify the integrity of shared data without retrieving the entire data from the cloud and without revealing the identity of the signer of each block. It must allow only a group users to generate valid metadata on shared data.

In order to preserve the identity of signer, we are creating the global private key which will be formed on behalf of all users in the group. This key can be used by all users of the group to sign the block. However, if any user leaves the group, it leads to regeneration of the global key which will be securely shared among the rest of the group. This however involves huge overhead of key management and key distribution.

Possible alternatives: Another possible approach to achieve identity privacy, is to add a trusted proxy between a group of users and the cloud in the system model. More concretely, each member's data is collected, signed, and uploaded to the cloud by this trusted proxy, then a public verifier can only verify and learn that it is the proxy signs the data, but cannot learn the identities of group members. Yet, the security of this method is threatened by the single point failure of the proxy. Besides, sometimes, not all the group members would like to trust the same proxy for generating signatures and uploading data on their behalf. Utilizing group signatures is also an alternative option to preserve identity privacy.

Trusted Computing offers another possible alternative approach to achieve the design objectives of our mechanism. Specifically, by utilizing direct anonymous attestation which is adopted by the Trusted Computing Group as the anonymous method for remote authentication in trusted platform module, users are able to preserve their identity privacy on shared data from a public verifier. The main problem with this approach is that it requires all the users to use designed hardware, and needs the cloud provider to move all the existing cloud services to the trusted computing environment, which would be costly and impractical.

PRELIMINARIES

Ring signatures: With the concept of ring signatures, the verifier understands that the signature is computed using one of the group members' private key but is not able to know which one. More concretely, given a ring signature and a group of users, say d, a verifier cannot distinguish the signer's identity with a probability more than 1/d. This property can be used to preserve the identity of the signer from a verifier.

Homomorphic Authenticators: Homomorphic authenticators (also called homomorphic verifiable tags) are basic tools to construct public auditing mechanisms. Besides unforgeability a homomorphic authenticable signature scheme, which denotes a homomorphic authenticator based on signatures, should also satisfy the following properties.

1. ***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.

2. ***Non-malleability*****:** It indicates that an adversary cannot generate valid signatures on arbitrary blocks by linearly combining existing signatures.

MODERN RING SIGNATURE SCHEME

Overview: The main motto of ring signatures [12] [13] is to hide the identity of the signer on each block in order to keep private and sensitive information un-disclosed to public verifier. However, the traditional ring signatures does not support block less verifiability and so the verifier needs to download the entire data from the cloud to check the correctness of the shared data which in turn consumes more bandwidth and more time.

Therefore, it designs a new homomorphic authenticable ring signature (HARS) scheme, which is extended from classic ring signature scheme. HARS generated ring signatures are not only able to preserve identity privacy but are also able to support block less verifiability.

Construction of HARS: The HARS contains three algorithms: KeyGen, RingSign and RingVerify. In KeyGen algorithm each user in the group generates his/her public key and private key. In RingSign algorithm 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; it distinguishes the corresponding block from others. A verifier can check whether a given block is signed by a group member in RingVerify.

PUBLIC AUDITING MECHANISM

Overview: Using HARS and its properties, a privacy-preserving public auditing mechanism for shared data on cloud is constructed. In this scheme, the public verifier can verify the integrity of shared data without retrieving the entire data. The identity of the signer on each block in shared data is kept private from the public verifier during the auditing.

Reduce Signature Storage: Another important issue need to consider in the construction of this scheme is the size of storage used for ring signatures. By the taxonomy of the ring signatures in HARS, a block m is an element of Zp and its ring signature contains d elements of G1, where G1 is a cyclic group with order p. It means a |p|-bit block requires a d * |p| -bit ring signature, which forces users to spend a huge amount of space on storing ring signatures. It will be very frustrating for users, because cloud service providers, such as Amazon, will charge users based on the storage space they use.

To reduce the storage of ring signatures on shared data and still allow the public verifier to audit shared data efficiently, we exploit an aggregated approach to expand the size of each block in shared data into k *|p| bits. With the aggregation of a block, the length of a ring signature is only d/k of the length of a block. Generally, to obtain a smaller size of a ring signature than the size of a block, it choose k > d. As a trade-off, the communication cost of an auditing task will be increasing with an increase of k.

Support Dynamic Operations: To enable each user in the group to easily modify data in the cloud, there is a need to support dynamic operations on shared data. Dynamic operation such as insert, delete or update operation are performed on a single block. Since the computation of a ring signature includes an identifier of a block, traditional methods which only use the index of a block as its identifier are not suitable for supporting dynamic operations on shared data efficiently.

When a user modifies a single block in shared data by performing an insert or delete operation, the indices of blocks are changed after the block modification and the changes of these indices require users, who are sharing the data, to re-compute the signatures of these blocks, even though the content of these blocks are not modified. This mechanism can allow a user to efficiently perform a dynamic operation on a single block, and avoid the re-computation of indices on other blocks.

Batch Auditing: Sometimes, a public verifier may need to verify the correctness of multiple auditing tasks in a very short time. Directly verifying these multiple auditing tasks separately would be inefficient. By leveraging the properties of bilinear maps, the concept of batch auditing can be supported, which can verify the correctness of multiple auditing tasks simultaneously and improve the efficiency of public auditing.

LITERATURE SURVEY

A verifier is allowed to check the correctness of a client’s data stored at an untrusted server. The verifier is able to publicly audit the integrity of data without retrieving the entire data by utilizing RSA-based homomorphic authenticators and sampling strategies, which is referred as a public auditing. But this mechanism is only suitable for auditing the integrity of personal data. 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 [1].

Shacham and Waters [11] designed two improved schemes. The first scheme is built from BLS signatures and the second one is based on pseudo-random functions. To support dynamic data symmetric keys verifies the integrity of data, it is not public verifiable and only provides a user with a limited number of verification requests.

Jia Xu , Anjia Yang introduced Lightweight and Privacy-Preserving Delegatable Proofs of Storage [15], this proof allows to audit the integrity of the data stored on cloud without keeping the local copy back of the data. The slowness of all existing proof of storage (POS) has made the systems to bottleneck. They proposed a new variant formulation that is able to construct a POS scheme, which on one side is as efficient as private key POS schemes, and on the other side can support third party auditor and can switch auditors at any time, close to the functionalities of publicly verifiable POS schemes.

Zhu et al. [5] proposed the fragment structure to reduce the storage of signatures in their public auditing mechanism. To provide dynamic operations on data they also used index hash tables.

The public mechanism proposed by Wang et al. [1] is able to preserve users' confidential data from a public verifier by using random masking.
They extended their mechanism to enable batch auditing by using aggregate signatures to operate multiple auditing tasks from different users efficiently, [13].

Wang et al. [1] used homomorphic tokens to ensure the correctness of erasure codes-based data distributed on multiple servers. This mechanism is able to support dynamic data as well as to identify misbehaved servers.

To reduce the communication overhead in the phase of data repair the Chen et al. [6] 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. Cao et al. [4] constructed an LT codes-based secure and reliable cloud storage mechanism. Compare to previous work [12], [4], this mechanism can avoid high decoding computation cost for data users and save computation resource for online data owners during data repair.

CONCLUSION

This paper efficiently utilizes ring signatures for construction of homomorphic authenticators to hide the identity of the signer on each block. The proposed work allows the public verifier to audit the integrity of the shared data without retrieving the entire data hiding the identity of the signer. Thus, this paper effectively discusses the privacy preserving public auditing mechanism for shared data in the cloud.

REFRENCES:

[1] Boyang Wang, Student Member, Baochun Li, Senior Member, and Hui Li, Member,"Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", IEEE transaction on cloud computing, vol. 2, no. 1, Jan-Mar 2014.

[2] 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.

[3] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses,"Computer, vol. 45, no. 1, pp. 39-45, 2012.

[4] 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.

[5] 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.

[6] 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.

[7] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing,"Comm. ACM,vol. 53, no. 4, pp. 50-58, Apr. 2010.

[8] 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.

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

[10] 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.

[11] 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.

[12] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)". Springer-Verlag, 2003, pp. 416432.

[14] 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.

[15] Jia Xu, Anjia Yang, Jianying Zhou and Duncan S. Wong, "Lightweight and Privacy-Preserving Delegatable Proofs of Storage", Institute for Infocomm Research, Singapore.