ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 3, May 2015

Survey on Privacy Preserving Public Auditing Techniques for Shared Data in the Cloud

Kedar Jayesh Rasal[1], Dr. S.V.Gumaste[2], Sandip A. Kahate[3]
Computer Engineering, Pune University, SPCOE, Otur, Pune, Maharashtra, India.
Professor and Head of Computer Engineering Department,
SPCOE, Otur, Pune, Maharashtra, India
SPCOE, Otur, Pune, Maharashtra, India

Abstract:- A cloud computing is become more popular as it provides guaranteed services like infrastructure management, online data storage and backup solutions, Web-based e-mail services, database processing, managed technical support services, virtualized infrastructure etc. By using the cloud services, the user can access data stored in a cloud anytime and at anywhere using any device and ensure about less capital investment. To provide promised always on 24/7 access, the cloud service provider (CSP) stores data replicas on multiple geographically distributed servers. It is necessary to compute signatures on the blocks in shared data for users in a particular group, so the shared data integrity can be confirmed publicly. Various blocks in shared data are usually signed by various vast numbers of users due to data alterations performed by different users. 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 difficulty with this approach is that it requires all the users using 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. This paper has made a survey on various privacy preserving techniques in cloud. Here Homomorphic Authenticable Ring Signature (HARS), privacy-preserving public auditing System for data storage security are discussed.

Keywords: **- Ring Signature, Homomorphic Authenticable Ring Signature (HARS), Privacy Preserving, Public Auditing, Cloud Computing.**

I. INTRODUCTION

In the cloud storage model the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a web-based content management or cloud storage gateway systems [7].

To preserve the identity of the signer on each block during public auditing, one possible alternative approach is to ask all the users of the group to share a global private key [2], [3]. Every user is able to sign blocks with this global private key. Once one user of the group is compromised or leaving the group, a new global private key must be generated and securely shared among the rest of the group, which clearly introduces huge overhead to users in terms of key management and key distribution. While here, each user in the rest of the group can still utilize its own private key for computing verification metadata without generating or sharing any new secret keys.

To achieve identity privacy other possible approach 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, and 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. The security of this method is still threatened by the single point failure of the proxy. Sometimes some of the group members would like to trust the same proxy for generating signatures and uploading data on their behalf. Utilizing group signatures [13] is also an alternative option to preserve identity privacy. Unfortunately, how to design an efficient public auditing mechanism based on group signatures remains open in the recent paper. Trusted Computing offers another possible alternative approach to achieve the design objectives of this mechanism.

Specifically, by utilizing direct anonymous attestation [8], 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

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 3, May 2015

identity privacy on shared data from a public verifier. This approach has the main problem as it requires all the users using 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. The sharing data among multiple users is perhaps one of the most engaging features that motivate cloud storage. So that , it is necessary to ensure the integrity of shared data in the cloud is correct. A new significant privacy issue introduced in the case of shared data with the use of existing mechanisms is the leakage of identity privacy to public verifiers [1].

II. LITERATURE SURVEY

Provable data allows a verifier 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 [4].

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.

Wang et al. [8] utilized Merkle Hash Tree and BLS signatures to support dynamic data in a public auditing mechanism.

Erway et al. [9] had introduced dynamic provable data possession (DPDP) with the help of authenticated dictionaries, which are based on rank information.

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. [4] 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. [4] 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. [3] constructed an LT codes-based secure and reliable cloud storage mechanism. Compare to previous work [12], [14], this mechanism can avoid high decoding computation cost for data users and save computation resource for online data owners during data repair.

III. SYSTEM MODEL

In this paper the system model involves three parties: the cloud server, a group of users and a public verifier. Here, two types of users in a group: the original user and a number of group users. The original user initially creates shared data in the cloud, and shares it with group users. Both the group user and original users are members of the group. It is allowed to access and modify shared data for every member of the group. Shared data and its verification metadata (i.e., signatures) are stored in the cloud server. A public verifier, such as a third-party auditor providing 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. As shown in Fig. 1. Alice and Bob share a data file in the cloud after receiving the auditing challenge and a public verifier audits shared data integrity with existing mechanisms. With an auditing proof of the possession of shared data the cloud server responds to the public verifier. Then, this public verifier checks the correctness of the

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 3, May 2015

entire data by verifying the correctness of the auditing proof. Essentially, the process of public auditing is a challenge and- response protocol between a public verifier and the cloud server.

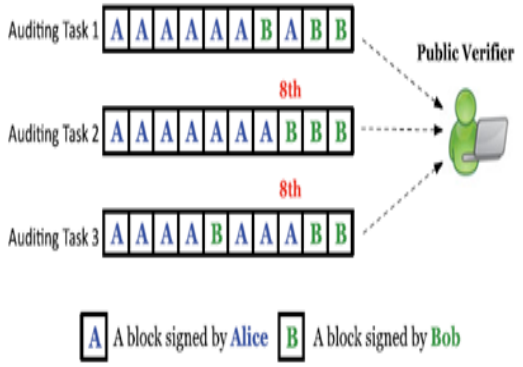

Fig. 1. Alice and Bob share a data file in the cloud, and a public verifier audits shared data integrity

IV. THREAT MODEL

A. 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.

B. 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.

V. RING SIGNATURES

The concept of ring signatures was first proposed by Rivest et al. [13] in 2001 using ring signatures, a verifier is convinced that a signature is computed using one of group members' private keys, but the verifier is not able to determine which one. More artificially, for a given ring signature and a group of d users, a verifier cannot distinguish the signer's identity with a probability more than 1=d. To preserve the identity of the signer from a verifier this property can be used. By Boneh et al. [12], the ring signature scheme introduced which is constructed on bilinear maps.

VI. 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.

A. 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.

B. Non-malleability

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

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 3, May 2015

VII. MODERN RING SIGNATURE SCHEME

A. Overview

To utilize ring signatures to hide the identity of the signer on each block, so that private and sensitive information of the group is not disclosed to public verifiers. However, traditional ring signatures, cannot be directly used into public auditing mechanisms, because these ring signature schemes do not support block less verifiability. Without block less verifiability, a public verifier has to download the whole data file to verify the correctness of shared data, which consumes excessive bandwidth and takes very long verification times.

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

B. 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.

VIII. PUBLIC AUDITING MECHANISM

A. Overview

Using HARS and its properties a privacy-preserving public auditing mechanism for shared data in the 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.

B. Reduce Signature Storage

Another important issue need to take 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 jpj-bit block requires a d _ jpj-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, it exploit an aggregated approach to expand the size of each block in shared data into k _jpj 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.

C. Support Dynamic Operations

To enable each user in the group to easily modify data in the cloud, scheme should also support dynamic operations on shared data. In dynamic operation an insert, delete or update operation performed on a single block. Since the computation of a ring signature includes an identifier of a block (as presented in HARS), traditional methods, which only use the index of a block as its identifier (i.e., the index of block mj is j), 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 that after the modified block are all changed 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 this type of re-computation on other blocks.

VIII. CONCLUSION

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.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 3, May 2015

REFERENCES

[1] 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.

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

[3] N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service,"Proc. IEEE INFO-COM, 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] 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.

[13] 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.

AUTHOR BIOGRAPHY

Mr. Kedar Jayesh Rasal. B.E.Computer from Pune University. He stayed in Govt. College of Engineering And Research, Awasari as a visiting lecturer in Computer Department. He is now studing Master Of Engineering in Sharadchandra Pawar College of Engineering, Dumbarwadi,,Otur, University Of Pune , Inc. He has published 3 papers in International Journals and presented 1 paper in cPGCON2015 conference.His areas of interest are Cloud Computing and Network Security.

Mr. S.V.Gumaste currently working as Professor and Head, Department of Computer Engineering, SPCOE-Dumberwadi, Otur. Graduated from BLDE Association's College of Engineering, Bijapur, Karnataka University, Dharwar in 1992 and completed Post-graduation in CSE

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 3, May 2015

from SGBAU, Amravati in 2007.Completed Ph.D (CSE) in Engineering & Faculty at SGBAU, Amravati. Has around 22 years of Teaching Experience

Mr. Sandip A. Kahate.B.E. in computer science and engg. From Amravati university, M.E. in Wireless Communication and Computing, from Nagpur University and preparation for Ph.D. registration. He is currently working as a Assistant Professor in Computer Department, Sharadchandra Pawar College of Engineering,Dumbarwadi,Tal-Junnar,Dist-Pune.-410504.(M.S.),India. He has 10 years of teaching experience. He has 15 papers at hs credit in international journal and 3 in international conference. His areas of interest are Wireless Communication and computing, network security and Ad-Hoc Network.