International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
www.ioirp.com ISSN: 2394-6364, Volume – 1, Issue – 6. May 2015

PRIVACY PRESERVING PUBLIC AUDITING FOR SHARED DATA WITH TRACEABILITY IN THE CLOUD

Shijina Karim
M.E.(C.S.E), Maharaja Prithvi Engineering College, Avinashi, India
shijinakarim786@gmail.com

Abstract*— Cloud computing is a novel computing model that enables convenient and on demand access to a shared pool of configurable computing resources. Auditing services are highly essential to make sure that the data is correctly hosted in the cloud. In Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services. The integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. Meanwhile, the identity of the signer on each block in Shared data is kept private from the TPA also able to perform multiple auditing tasks simultaneously instead of verifying them one by one. With this system a privacy-preserving auditing mechanism for data stored in the cloud and shared among a large number of users in a group is considering which utilizes ring signature to construct homomorphic authenticators, so that a third party auditor is able to verify the integrity of shared data for users without retrieving the entire data. Traceability – the ability of the original user to reveal the identity of the signer in somespecial situations and data freshness- the cloud possesses the latest version of shared data- can be ensured in the new system.

Keywords— Public auditing, privacy-preserving, shared data, cloud computing ,Traceability

I. INTRODUCTION

Cloud computing is a novel computing model that enables convenient and on demand access to a shared pool of configurable computing resources. Auditing services are highly essential to make sure that the data is correctly hosted in the cloud. In Cloud Storage, users can remotely store their data and enjoy the on demand high quality applications and services. The integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will supports public auditing on shared data stored in the cloud that exploit ring signature to compute verification metadata needed to audit the correctness of shared data. so that a third party auditor is able to verify the integrity of shared data for users without retrieving the entire data. Meanwhile, the identity of the signer on each block in Shared data is kept private from the TPA also able to perform multiple auditing tasks simultaneously instead of verifying them one by one.

With cloud storage services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. However, public auditing for such shared data while preserving identity privacy remains to be an open challenge. It is the first privacy preserving mechanism that allows public auditing on shared data stored in the cloud. In particular, this exploit ring signatures to compute the verification information needed to audit the integrity of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from a third party auditor who is still able to verify the integrity of shared data without retrieving the entire file.

Here it's a privacy preserving auditing mechanism for data stored in the cloud and shared among a large number of users in a group is considering. In particular, the method utilizes ring signatures to construct homomorphic authenticators, so that a third party auditor is able to verify the integrity of shared data for users without retrieving the entire data. Meanwhile, the identity of the signer on each block in shared data is kept private from the TPA. So the amount of information used for verification, as well as the time it takes to audit with it, are not affected by the number of users in the group. In addition, it exploits homomorphic MACs to reduce the space used to store such verification information.

The system will have the property of traceability, the ability of the group manager to reveal the identity of the signer and data freshness, ie the cloud possesses the latest data can be proved

II. PROBLEM FORMULATION

A. System Model

The system model involves three parties: the cloud server, a group of users and a public verifier. There are 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 original user and group users are members of the group. Every member of the group is allowed to access and modify shared data. Shared data and its verification metadata (i.e., signatures) are both 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.

.

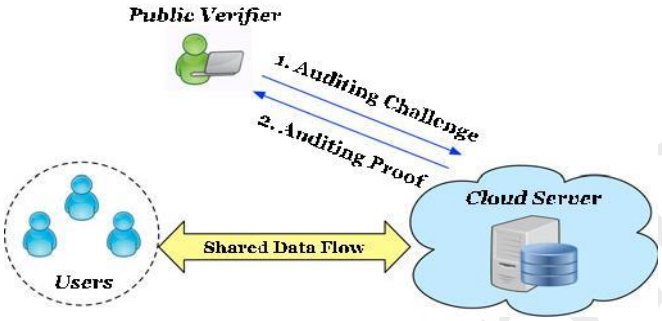

Fig.1. Architecture

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, thecloud 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. Essentially, the process of public auditing is a challenge-and-response protocol between a public verifier and the cloud server .

B. Threat Model

Integrity Threats. Two kinds of threats related to the integrity of shared data are possible. 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 ser-vice 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. 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. Once the public verifier reveals the identity of the signer on each block, it can easily distinguish a high-value target (a particular user in the group or a special block in shared data) from others.

C. Design Goals

The system, should be designed to achieve fol-lowing properties: (1) Public Auditing: A public verifier is able to publicly verify the integrity of shared data without retrieving the entire data from the cloud. (2) Correctness: A public verifier is able to correctly verify shared data integ-rity. (3) Unforgeability: Only a user in the group can generate valid verification metadata (i.e., signatures) on shared data.(4) Identity Privacy: A public verifier cannot distinguish the identity of the signer on each block in shared data during the process of auditing.(5) Traceability: The ability of the group manager to reveal the identity of the signer based on verification metadata.

D. Ring Signatures

A verifier is convinced that messages are correct and signed by one of the group members, but cannot reveal the identity of the signer. Meanwhile, only the group manager is able to trace these group signatures and reveal the identity of the signer.

E. Homomorphic Authenticators

Homomorphic authenticators should also satisfy the blockless verifiability andnon-malleability.

III. PROPOSED SCHEME

The method is a privacy-preserving auditing mechanism for data stored in the cloud and shared among a large numberof users in a group. In particular, here utilizesring signature/group signatures to construct homomorphic authenticators, so that a third party auditor is able to verify the integrity of shared data for users without retrievingthe entire data. Meanwhile, the identity of the signer on each block in shared data is kept private from the TPA. For the purpose of privacy the data can be encrypted by using symmetric key encryption or attribute based encryption.Ring signature can be used for ensuring the data integrity.KeyGen,SigGen,Modify,proofGen, and ProofVerifyare the methods used in ring signature. Sampling strategy is used for public auditing. And also it exploits homomorphic MACs to reduce the space used to store such verification information. Traceability the ability for the group managerto reveal the identity of the signer based on verification metadata in some special situations is possible in the new system. Also data freshness can be ensured by new methodie checking cloud is having the latest copy of data or not. Multiple auditing task can perform simultaneously to improve the performance of the system. Tis can be achieved by supporting more than one TPA parallel to check the files integrity.

It includes five algorithms: KeyGen, SigGen, Modify, ProofGen and ProofVerify.

In KeyGen, users generate their own public/private key pairs. In SigGen, a user (either the original user or a group user) is able to compute ring signa-tures on blocks in shared data by using its own private key and all the group members' public keys. Each user in the group is able to perform an insert, delete or update opera-tion on a block, and compute the new ring signature on this new block in Modify. ProofGen is operated by a public ver-ifier and the cloud server together to interactively generate a proof of possession of shared data. In ProofVerify, the public verifier audits the integrity of shared data by verify-ing the proof.

A. Ring Signature

KeyGen.For a user ui in the group U, she randomly picks xi € Zp and computes wi = g2xi €G2. Then, user ui's public key is pki = wi and her private key is ski =xi.

RingSign.Given all the d users' public keys (pk1, ...,pkd) = (w1, ...,wd), a block m € Zp, the identifier of this block id and the private key sks for some user us randomly chooses ai€ Zp for all i ≠s, where i € [1, d], and let σ i = g1αi . Then, she computesβ= H1(id)g1m €G1, and setsσ s = (β/φ(πi≠swiai))1/x2

RingVerify. Given all the d users' public keys (pk1, ..., pkd) = (w1, ...,wd), a block m, an identifier id and a ring signature σ = (σ 1, ..., σ d), a verifier first computes β = H1(id)g1m∈ G1

ProofGen. To audit the integrity of shared data, a user first sends an auditing request to the TPA. After receiving an auditing request, the TPA generates anauditing message [2] as follows:

1) The TPA randomly picks a c-element subset J of set [1, n] to locate the c selected blocks that will be checked in this auditing process, where n is total number of blocks in shared data.

2) For j Є J , the TPA generates a random value yjЄZq.Then, the TPA sends an auditing message {(j, yj)}jЄJtothe cloud server

ProofVerify. With an auditing proof {_,μ,_, {idj}jЄJ}, an auditing message {(j, yj)}jЄJ , public aggregate key pak= (_1, ..., _k), and all the group members' public keys (pk1, ..., pkd) = (w1, ...,wd), the TPA verifies the correctness of this proof

IV. PERFORMANCE ANALYSIS

In this, the auditing time is independent from the group size, while the auditing time linearly increases with size of the

group in previous system. When the datain the cloud are shared by a large group, it requires less auditing time. But the auditing time and space required for signature to be stored is less in the system. But the computation cost increases with theincrease in number of members of the group.

V. CONCLUSION

The system supports traceability and data freshness of data shared among users across cloud..It is, a privacy-preserving public auditing mechanism for shared data in the cloud. Here utilize 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. To improve the efficiency of verifying multiple auditing tasks, implementing batch auditing too.Traceability and data freshness is implemented effectively in the system.Scheduling on the auditing tasks that occurred at the same time can be done as a future work on this.Experimental evaluation demonstrates the efficiency and effectives of the scheme.

References

[1] Oruta: privacy preserving public auditing for shared data in the cloud"Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li, Member, IEEE

[2] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf.Comm. and Network Security (CNS '13), pp. 90-99, 2013

[3] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in CloudComputing," Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality ofService (IWQoS'09), pp. 1-9, 2009.

[5] Certificateless Public Auditing for Data Integrity in the Cloud" [Boyang Wang, Baochun Li, Hui Li and Fenghua Li].

[6] 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.

[7] B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Trans.Services Computing, 20 Dec. 2013, DOI: 10.1109/TSC.2013.2295611.