International Research Journal of Computer Science (IRJCS)
Issue 6, Volume 2 (June 2015)
ISSN: 2393-9842
www.irjcs.com

Oruta: Public Auditing for Shared Data in the Cloud Storage

Ms.Madhuri B.Patil
M.Tech(CSE)
Department of CSE
MLRIT,Hyderabad

Mr. N. Aravind Kumar
Assistant Professor
Department of CSE
MLRIT,Hyderabad

Abstract-- Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data rather than a local server or a personal computer. The privacy preserving supports the public auditing without the retrieval access of entire data blocks. The integrity of data in cloud storage, however, is subject to skepticism and scrutiny, as data stored in an untrusted cloud can easily be lost or corrupted, due to hardware failures and human errors. To protect the integrity of cloud data, it is best to perform public auditing by introducing a third party auditor (TPA), who offers its auditing service with more powerful computation and communication abilities than regular users. In this paper, we propose Oruta, a new privacy preserving public auditing mechanism for shared data in an untrusted cloud. In Oruta, we utilize ring signatures to construct homomorphic authenticators , so that the third party auditor is able to verify the integrity of shared data for a group of users without retrieving the entire data — while the identity of the signer on each block in shared data is kept private from the TPA. We only consider how to audit the integrity of shared data in the cloud with static groups.

***Keywords*: cloud computing, public auditing, security, data integrity, cloud server.**

I. INTRODUCTION

Cloud computing has been envisioned as the next- generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history like on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk[1]. The Cloud server allows user to store their data on a cloud without worrying about correctness & integrity of data. Cloud data storage has many advantages over local data storage. User can upload their data on cloud and can access those data anytime anywhere without any additional burden. The User doesn't have to worry about storage and maintenance of cloud data. But as data is stored at the remote place how users will get the confirmation about stored data. Hence Cloud data storage should have some mechanism which will specify storage correctness and integrity of data stored on a cloud. The major problem of cloud data storage is security. Cloud is used not only for storing data, but also the stored data can be shared by multiple users. Due to this the integrity of cloud data is subject to doubt.

Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user.Sharing data among multiple users is perhaps one of the most engaging features that motivates cloud storage. A unique problem introduced during the process of public auditing for shared data in the cloud is how to preserve identity privacy from the TPA, because the identities of signers on shared data may indicate that a particular user in the group or a special block in shared data is a higher valuable target than others. Several mechanisms have been designed to support public auditing on shared data stored in the cloud. During auditing, the shared data is kept private from public verifiers, who are able to verify shared data integrity using ring signature without downloading or retrieving the entire file. Ring signature is used to compute verification metadata needed to audit the correctness of shared data. With this, the identity of the signer in shared data is kept private from public verifiers

II. SYSTEM AND THREAT MODEL

Our work involves three parties shown in Fig.1: the cloud server, the third party auditor (TPA) and users. There are two types of users in a group: the original user and a number of group users. The original user and group users are both members of the group. Group members are allowed to access and modify shared data created by the original user based on access control polices [2]. Shared data and its verification information (i.e. signatures) are both stored in the cloud server. The third party auditor is able to verify the integrity of shared data in the cloud server on behalf of group members.

© 2014-15, IRJCS- All Rights Reserved

Fig.1 System model includes A cloud server, group of users and TPA(Public Verifier)

We only consider how to audit the integrity of shared data in the cloud with static groups. It means the group is pre-defined before shared data is created in the cloud and the membership of users in the group is not changed during data sharing. The original user is responsible for deciding who is able to share her data before outsourcing data to the cloud. When a user (either the original user or a group user) wishes to check the integrity of shared data, she first sends an auditing request to the TPA. After receiving the auditing request, the TPA generates an auditing message to the cloud server, and retrieves an auditing proof of shared data from the cloud server. Then the TPA verifies the correctness of the auditing proof. Finally, the TPA sends an auditing report to the user based on the result of the verification.

1 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 and prevent users from using data correctly. Second, the cloud service provider may inadvertently corrupt (or even remove) data in its storage due to hardware failures and human errors.

2 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 semi-trusted TPA, who is only responsible for auditing the integrity of shared data, may try to reveal the identity of the signer on each block in shared data based on verification information.

III. LITERATURE SURVEY

The purpose of this review is to report, evaluate, and discuss the findings from research. A particular focus of this review is to facilitating privacy-preserving public auditing for secure shared data in cloud storage.

Cong Wang, Sherman S.M. Chow, Qian Wan, Kui Ren and Wenjing Lou,[3] Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

Boyang Wang, Baochun Li, and Hui Li,[4] 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. In this paper, we propose the first privacy-preserving mechanism that allows public auditing on shared data stored in the cloud. In particular, we 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 (TPA), who is still able to publicly verify the integrity of shared data without retrieving the entire file.

R. Rajasaranyakumari, S.Velmurugan, K.J. Nithya,[5] Cloud is used not only for storing data, but also the stored data can be shared by multiple users. Due to this the integrity of cloud data is subject to doubt. Several mechanisms have been designed to support public auditing on shared data stored in the cloud. During auditing, the shared data is kept private from public verifiers, who are able to verify shared data integrity using ring signature without downloading or retrieving the entire file. Ring signature is used to compute verification metadata needed to audit the correctness of shared data.

© 2014-15, IRJCS- All Rights Reserved

With this, the identity of the signer in shared data is kept private from public verifiers. In this paper, we propose a traceability mechanism that improves Data Privacy by achieving traceability and the data freshness(the cloud possess the latest version of shared data) is also proved while still preserving identity privacy.

B.Banu priya, V.Sobhana, Prof.Mishmala Sushith,[6] we have made a concise survey on various privacy preserving techniques in cloud. Homomorphic Authenticable Ring Signature (HARS), privacy-preserving public auditing System for data storage security are discussed. Public key cryptosystem, the MD5 Message-Digest Algorithm are depicted. Proof-Of- Retrievability system for public verifiability is described. Dynamic Provable Data Possession (DPDP) to enlarge the PDP model is discussed in detail. LT codes based cloud storage service (LTCS) to empower efficient decoding, Merkle Hash Tree (MHT) for the block tag Authentication is discussed.

Cong Wang, Qian Wang, KuiRen, Wenjing Lou,[7] Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centres, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with woo salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s).Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks

C. Wang, Q. Wang, K. Ren, and W. Lou [8], Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

IV. PROPOSED SCHEME

The proposed system, to enable the TPA efficiently and securely verify shared data for a group of users, Oruta should be designed to achieve following design goals:

A. Design Goals:

1) **Public Auditing**: The third party auditor is able to publicly verify the integrity of shared data for a group of users without retrieving the entire data.
2) **Correctness**: The third party auditor is able to correctly detect whether there is any corrupted block in shared data.
3) **Unforgeability**: Only a user in the group can generate valid verification information on shared data.
4) **Identity Privacy**: During auditing, the TPA cannot distinguish the identity of the signer on each block in shared data.

B. Framework:

Homomorphic Authenticable Ring Signatures (HARS)

HARS contains three algorithms:

1) **KeyGen** : each user in the group generates her public key and private key.
2) **RingSign :** user in the group is able to sign a block with her private key and all the group members' public keys.
3) **RingVerify**: verifier is allowed to check whether a given block is signed by a group member in RingVerify.

© 2014-15, IRJCS- All Rights Reserved

C. Privacy-preserving Public Auditing Schema for shared data (Oruta):

Using HARS and its properties we construct Oruta, our privacy preserving public auditing mechanism for shared data in the cloud. With Oruta, the TPA can verify the integrity of shared data for a group of users without retrieving the entire data. Meanwhile, the identity of the signer on each block in shared data is kept private from the TPA during the auditing. It includes five algorithms:

1) **KeyGen**: users generate their own public/private key pairs.
2**) SigGen** : a user (either the original user or a group user) is able to compute ring signatures on blocks in shared data.
3) **Modify**: Each user in the group is able to perform an insert, delete or update operation on a block, and compute the new ring signature on this new block.
4) **ProofGen :** is operated by the TPA and the cloud server together to generate a proof of possession of shared data .
5) **ProofVerify**: the TPA verifies the proof and sends an auditing report to the user.

The group is pre-defined before shared data is created in the cloud and the membership of the group is not changed during data sharing. Before the original user outsources shared data to the cloud, she decides all the group members, and computes all the initial ring signatures of all the blocks in shared data with her private key and all the group members' public keys. After shared data is stored in the cloud, when a group member modifies a block in shared data, this group member also needs to compute a new ring signature on the modified block.

V. PROPOSED WORK.

We are going to raise the privacy level of the data owner and the confidentiality of the data in a better way through the multiple cloud environments. In proposed work consists six modules?

A**) Owner Registration:** In this module an owner has to upload its files in a cloud server, he/she should register first. Then only he/she can be able to do it. For that he needs to fill the details in the registration form. These details are maintained in a database.

B) Owner Login: In this module, any of the above mentioned people have to login, they should login by giving their email id and password.

C) User Registration: In this module if a user wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database.

D) User Login: If the user is an authorized user,he/she can download the file by using file id which has been stored by data owner when it was uploading.

E) ThirdPartyAuditor Registration: In this module, if a third party auditor TPA (maintainer of clouds) wants to do some cloud offer, they should register first. Here we are doing like, this system allows only three cloud service providers.

F) ThirdPartyAuditor Login: After third party auditor gets logged in, He/ She can see how many data owners have uploaded their files into the cloud. Here we are providing three tpa for maintaining three different clouds.

VI. CONCLUSION

We propose Oruta, the first privacy preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphic authenticators, so the TPA is able to audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can achieve identity privacy. To improve the efficiency of verification for multiple auditing tasks, we further extend our mechanism to support batch auditing. An interesting problem in our future work is how to efficiently audit the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third

REFERENCES

[1]. P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloud- computing/index.html, June 2009.
[2].S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 534–542.
[3].Cong Wang, Sherman S.M. Chow, Qian Wan, Kui Ren and Wenjing Lou, "Privacy Preserving Public Auditing for Secure Cloud storage",IEEE,Vol.62,No.2,Feb 2013
[4].Boyang Wang, Baochun Li, and Hui Li,"Oruta: Privacy Preserving Public Auditing for Shared Data in the Cloud",IEEE,2014
[5].R. Rajasaranyakumari, S.Velmurugan, K.J. Nithya, Enhanced Privacy Preserving with Data Freshness by Accomplishing Traceability over Oruta, IJRASET,October 2014
[6].B.Banu priya, V.Sobhana, Prof.Mishmala Sushith, "Concise Survey on Privacy Preserving Techniques in Cloud",IARJSET,Feb 2015.
[7].Cong Wang, QianWang, KuiRen, Wenjing Lou (2009),"Ensuring Data Storage Security in Cloud Computing".
[8]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-PreservingPublic Auditing for Data Storage Security in Cloud Computing,"in Proc. IEEE International Conference on Computer Communications(INFOCOM), 2010, pp. 525–533.

© 2014-15, IRJCS- All Rights Reserved