RESEARCH ARTICLE OPEN ACCESS

Innovation in Privacy-Preserving Public Auditing Schemes for Secure Cloud Storage: A Study

K M Uma[1],Veena A[2], Sangeetha G M[3], Jayalakshmi K[4]
[1,2,3,4] Assistant Professor,Department of Computer Science and Engineering,VTU, Dr.AIT, Bangalore.

Abstract:

Since the last few years there has been a phenomenal growth in the study of cloud computing , where users can remotely store there data into to the cloud . so as to enjoy the on-demand high quality applications and services from the cloud .cloud computing has extraordinary data storage capabilities were users can access their data from the cloud as if it is local without worrying about the need to verify its integrity and security. Thus, enabling public audit ability 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 . This paper aims at highlighting some of the concepts and innovation of different technologies along with benefits in privacy preserving public auditing for secure cloud computing.

Keywords — **Public auditing, privacy-preserving, shared data, cloud storage.**

I. INTRODUCTION

Cloud computing technology is very similar in providing an environment that is dynamically allocated to meet organization/user needs. Nowadays, information is one of the most valuable possessions of companies, organizations and individuals. From the beginning of time, people try to secure information saved on various kinds of storages. Cloud computing is rapidly emerging due to the provisioning of elastic, flexible, and on-demand storage and computing services for customers. As a recent phenomenon, Cloud computing is perceived as a virtual cloud with unlimited possibilities of providing service in a field of information technology. The Organization of National Institute of Standards and Technology (NIST) defines cloud computing as a service model which enables instant, simple and on request available network access to shared offer of configurable computing resources (networks, servers, applications, service and data). In case of need, they can be provided or loosened for minimal administrative expenses and it also provides coordination needs of the service providers.

Storing data remotely into the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc [1]. While these advantages of using clouds are unarguable, due to the opaqueness of the Cloud—as separate administrative entities, the internal operation details of Cloud Service Providers (CSP) may not be known by cloud users—data outsourcing is also relinquishing user’s ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Examples of outages and security breaches of noteworthy cloud services appear from time to time [2–3]. Secondly, for the benefits of their own, there do exist various motivations for cloud service providers to behave unfaithfully towards the cloud users regarding the status of their outsourced data. Examples include cloud service providers, for monetary reasons, reclaiming storage by discarding data that has not been or is rarely accessed or even hiding data loss incidents so as to maintain a reputation [4–5]. In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the successful deployment of the cloud architecture. Recently, the notion of public auditability has been proposed in the context of ensuring remotely stored data integrity under different systems and security models [4, 5, 6, 7]. Public auditability allows an external party, in addition to the user himself, to verify the correctness of remotely stored data. However, most of these schemes [4, 5, 6] do not support the privacy protection of users' data against external auditors, i.e., they may potentially reveal user data information to the auditors, From the perspective of protecting data privacy, the users, who own the data and rely on TPA just for the storage security of their data, do not want this auditing process introducing new vulnerabilities of unauthorized information leakage towards their data security [8]. Exploiting data encryption before outsourcing [7] is one way to mitigate this privacy concern, but it is only complementary to the privacy-preserving public auditing scheme to be proposed in this paper. Thus, it does not completely solve the problem of protecting data privacy but just reduces it to the one of managing the encryption keys. Unauthorized data leakage still remains a problem due to the potential exposure of encryption keys. Here the paper gives you different technologies to tackle all these problems.

II. SYSTEM DESIGN

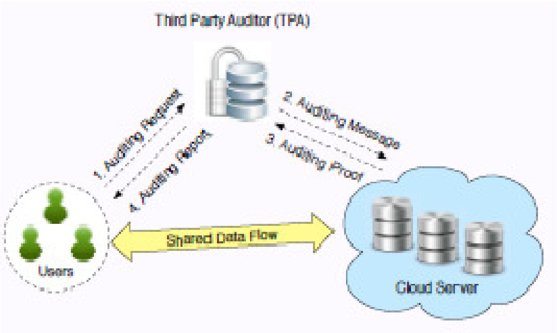

Fig. 2: System Design Includes TPA, Cloud Server & Users

As illustrated in Fig. 2, system design involves three parties: 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 [8]. 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.

In this paper, 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. Another interesting problem is how to audit the integrity of shared data in the cloud with **dynamic** groups — a new user can be added into the group and an existing group member can be revoked during data sharing — while still preserving identity privacy. We will leave this problem to our future work. 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.

III. AUDIT PROTOCOL BLOCKER

3.1 Overview

In cloud public auditability allows an external party, in addition to the user himself, to verify the correctness of remotely stored data. However, most of these schemes [4, 5, 6] do not support the privacy protection of users' data against external auditors, i.e., they may potentially reveal user data information to the auditors, This drawback greatly affects the security of these protocols in Cloud Computing. From the perspective of protecting data privacy, the users, who own the data and rely on TPA just for the storage security of their data, do not want this auditing process introducing new vulnerabilities of unauthorized information leakage towards their data security[8].

So Audit Protocol Blocker is used to overcome this problem independent to data encryption. Here the public key based homomorphic authenticator is utilized and uniquely integrate it with random mask technique and automatic blocker to achieve a privacy-preserving public auditing system for cloud data storage security.

3.2 Advantages of Audit Protocol Broker

1) Audit Protocol Blocker is used to find the unauthorized user ,to prevent the unauthorized data access for preserving data integrity. This scheme monitors the user requests according the user specified parameters and it checks the parameters for the new and existing users .The system accepts existing validated user, and prompts for the new users for the parameter to match requirement specified during user creation for new users. If the new user prompt parameter matches with cloud server, it gives privileges to access the Audit protocol otherwise the system automatically blocks the Audit protocol for specific user.

2) In this protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by a Pseudo Random Function (PRF). With random mask, the TPA no longer has all the necessary information to build up a correct group of linear equations and therefore cannot derive the user's data content, no matter how many linear combinations of the same set of file blocks can be collected. Meanwhile, due to the algebraic property of the homomorphic authenticator, the correctness validation of the block-authenticator pairs will not be affected by the randomness generated from a PRF. In this protocol, the system use public key based homomorphic authenticator, specifically, the one in [6], which is based on BLS signature [9], to equip the auditing protocol with public auditability. Its flexibility in signature aggregation will further benefit for the multi-task auditing.

IV. PUBLIC AUDITABILITY & DATA INTEGRITY

Outsourcing data to the cloud is economically attractive for long-term large scale storage but it does not immediately offer any guarantee on data integrity and auditability . Another disadvantage of public key based homomorphic algorithm is , we cannot always depend on cryptographic solutions for data integrity to secure users data in cloud also it is insufficient to detect the data corruption only when accessing data, as it does not give users correctness assurances for those un accessed data and might be too late to recover the data loss or damage. Thus to overcome all these problems Public auditing and data integrity is proposed.

4.1 Advantages of this Scheme

1) This scheme enables an external auditor to audit users cloud data without learning the data content.

2)support scalability, efficient privacy preserving public storage auditing in cloud. This scheme also supports batch auditing which allows TPA to perform the multiple auditing tasks simultaneously and greatly reduces the computation cost on the TPA side.

3) Storage correctness.

4) Light weight.

V. ORUTA

5.1 Problem Statement

1.In cloud an adversary may try to corrupt the integrity of shared data and prevent users from using data correctly.

2. the cloud service provider may inadvertently corrupt or even remove data in its storage due to hardware failures and human errors. Making matters worse, in order to avoid jeopardizing its reputation, the cloud server provider may be reluctant to inform users about such corruption of data.

3. 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. Once the TPA 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).

Thus ORUTA is designed to enable the TPA efficiently and securely verify shared data for a group of users.

5.2 Properties of ORUTA

1) Ring Signatures: The concept of ring signatures is first proposed by Rivest *et al.* [10] in 2001. With 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. This property can be used to preserve the identity of the signer from a verifier.The ring signature scheme introduced by Boneh *et al.* [11] is constructed on bilinear maps.further ring signature scheme is extended to construct our public auditing mechanism .here we intend 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 the TPA. However, traditional ring signatures [10], [11] cannot be directly used into public auditing mechanisms, because these ring signature schemes do not support blockless verification. Without blockless verification, the TPA has to download the whole data file to verify the correctness of shared data, which consumes excessive bandwidth and takes long verification times. Therefore, we first construct a new homomorphic authenticable ring signature (HARS) scheme, which is extended from a classic ring signature scheme [11], denoted as BGLS. The ring signatures generated by HARS is able not only to preserve identity privacy but also to support blockless verification.

2) Homomorphic Authenticable Ring Signatures: Here a new ring signature scheme is introduced, which is suitable for public auditing. Then, this scheme will show how to build the privacy-preserving public auditing mechanism for shared data in the cloud based on this new ring signature. this scheme is extended from a classic ring signature scheme [11], denoted as BGLS. The ring signatures generated by HARS is able not only to preserve identity privacy but also to support blockless verification. Using HARS and its properties, we now 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.

5.3 Advantages of HARS

1.Reduce Signature Storage
2. Support Dynamic Operations
3.Construction of ORUTA
4. Security Analysis of ORUTA
5. Batch Auditing

VI. UNPADDED RSA BASED THIRD PARTY AUDITING PROTOCOL

The design of this protocol makes use of a Unpadded RSA-based HLA, to equip the auditing protocol with public auditability. Specifically, this protocol uses the HLA proposed in [Shacham & Waters, 2008], which is based on the short signature scheme proposed by Boneh, Lynn, and Shacham (hereinafter referred as BLS signature) [Boneh et al., 2004].

6.1 Advantage

This protocol propose a secure cloud storage system supporting privacy preserving unpadded RSA based public auditing. The proposed protocol solves all the issues such as enabling worry free public auditing, user data privacy and additional online burden to users and additionally batch auditability is done. By comparing this protocols with the existing protocols of encryption the above given protocol is much better than the existing protocol in terms of data privacy and public auditability.

CONCLUSION

In this paper we have surveyed privacy-preserving public auditing schemes for secure cloud storage. here we have studied many technologies for privacy-preserving public auditing for cloud and there are lots of improved technologies in securing the cloud data. Among these technologies HARS is the efficient algorithm used for privacy-preserving, public auditing, data integrity and batch auditing. Using HARS, 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 public auditing, data integrity and batch auditing. Using HARS, 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

REFERENCES

[1] P. Mell, T. Grance (2009),"Draft NIST working definition of cloud computing", [Online]Available: http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia,"Above the clouds: A berkeley view of cloud computing", University of California, Berkeley, Tech. Rep.UCB-EECS-2009-28, Feb 2009.

[3] S. Wilson (2008),"Appengine outage", [Online] Available:http://www.cio-weblog.com/50226711/appengine outage.php.

[4] B. Krebs,"Payment Processor Breach May Be Largest Ever", [Online] Available: http://www.voices.washingtonpost.com/securityfix/2009/01/payment processor breach may b.html, Jan. 2009.

[5] M. A. Shah, R. Swaminathan, M. Baker,"Privacy-preserving audit and extraction of digital contents", Cryptology ePrint Archive, Report 2008/186, 2008, [Online]
Available: http://www.eprint.iacr.org/.

[6] Cloud Security Alliance (2009),"Security guidance for critical areas of focus in cloud computing", [Online] Available: http://www.cloudsecurityalliance.org.

[7] H. Shacham, B. Waters,"Compact proofs of retrievability", in Proc. of Asiacrypt 2008, Vol. 5350, Dec 2008, pp. 90–107.

[8] A. Juels, J. Burton S. Kaliski,"Pors: Proofs of retrievability for large files", in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.

[9] D. Boneh, C. Gentry, B. Lynn, H. Shacham,"Aggregate and verifiably encrypted signatures from bilinear maps", in Proc.of Eurocrypt 2003, Vol. 2656 of LNCS. Springer-Verlag, 2003, pp. 416–432.

[10] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag, 2001, pp. 552–565.

[11] 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 CryptographicTechniques (EUROCRYPT). Springer-Verlag, 2003, pp. 416–432.

[12] 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

[13] D. Boneh, B. Lynn & H. Shacham (2004), ―Short Signatures from the Weil Pairing‖, J. Cryptology, Vol. 17, No. 4, Pp. 297–319.

[14] H. Shacham & B. Waters (2008), ―Compact Proofs of Retrievability‖, Proc. Int'l Conf. Theory and Application of Cryptology and Information Secutity : Advances in Cryptology (Asiacrypt), Vol. 5350, Pp. 90–107.