IJDCST @October Issue- V-1, I-6, SW-49
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Enable Public Audit ability for Secure Cloud Storage

Leela Poornima[1], D.Hari Krishna[2]

[1]Student, Nova College of Engineering and Technology, Ibrahimpatnam,Krishna Dist., Andhra Pradesh, India

[2]Assistant Professor, Nova College of Engineering and Technology, Ibrahimpatnam,Krishna Dist., Andhra Pradesh, India

Abstract: Cloud computing makes the user convenient in the data accessing, while users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources. The fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task. The users should be able to just use the cloud storage as if it is local without worrying about the need to verify its integrity. 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. The auditing process should bring in no new vulnerabilities toward user data privacy and introduce no additional online burden to user to securely introduce an effective TPA. Here, we propose a secure cloud storage system supporting privacy-preserving public auditing. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

I. INTRODUCTION

Cloud computing has been envisioned as the next generation information technology (IT) architecture for enterprises. List of unprecedented advantages in the IT history:

a. On-demand self-service
b. Ubiquitous network access
c. Location independent resource pooling
d. Rapid resource elasticity
e. Usage-based pricing
f. Transference of risk

Cloud computing is transforming the very nature as a disruptive technology with profound implications. One fundamental aspect of this paradigm shifting is that data are being centralized or outsourced to the cloud. From users' perspective including both individuals and IT enterprises the cloud in a flexible on-demand manner brings appealing benefits:

- Relief of the burden for storage management
- Universal data access with location independence
- Avoidance of capital expenditure on hardware
- Software
- Personnel maintenances
- So on

Cloud service providers (CSP) are separate administrative entities; data outsourcing is actually relinquishing user's ultimate control over the fate of their data. The correctness of the data in the cloud is being put at risk due to the following reasons. Initially, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices. Next, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status. Although outsourcing data to the cloud is economically attractive for long-term large-scale storage and does not immediately, offer any guarantee on data integrity and availability. Simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network.

Considering the large size of the outsourced data and the user's constrained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for the cloud users. In particular, users may not want to go through the complexity in verifying the data integrity. It is of critical importance to enable public auditing service for cloud data storage to fully ensure the data integrity and save the cloud users' computation resources as well as online burden. Therefore, that

user may resort to an independent third-party auditor (TPA) to audit the outsourced data when needed. The audit result from TPA would also be beneficial for the cloud service providers to improve their cloud-based service platform and even serve for independent arbitration purpose.

Enabling public auditing services will play an important role for this nascent cloud economy to become fully established. The notion of public auditability has been proposed in the context of ensuring remotely stored data integrity under different system and security models. Public auditability allows an external party to verify the correctness of remotely stored data in addition to the user himself. The perspective of protecting data privacy that own the data and rely on TPA just for the storage security of their data. Encryption does not completely solve the problem of protecting data privacy against third party auditing but just reduces it to the complex key management domain. Our work is among the first few ones to support privacy-preserving public auditing in cloud computing with the prevalence of cloud computing a foreseeable increase of auditing tasks from different users may be delegated to TPA.

II. PROBLEM STATEMENT

THREAT & SYSTEM MODEL

We consider a cloud data storage service involving three different entities that has large amount of data files to be stored in the cloud. As shown in the fig.1 the cloud server that is managed by the cloud service provider to provide data storage service and has significant storage space and computation resources. The third-party auditor has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request. They may also dynamically interact with the CS to access and update their stored data for various application purposes. It is of critical importance for users to ensure that their data are being correctly stored and maintained, as users no longer possess their data locally. To save the computation resource as well as the online burden potentially brought by the periodic storage correctness verification. Cloud users may resort to TPA for ensuring the storage integrity of their outsourced data while hoping to keep their data private from TPA. We assume the data integrity threats toward users' data can come from both internal and external attacks may include:

- Software bugs
- Hardware failures
- Bugs in the network path
- Economically motivated hackers
- So on

Using third-party auditing service provides a cost-effective method for users to gain trust in cloud. We also assume that cloud servers have no incentives to reveal their hosted data to external parties. We assume that neither CS nor TPA is motivated to collude with each other during the auditing process. To authorize the CS to respond to the audit delegated to TPA's and all audits from the TPA are authenticated against such a certificate.

Design Goals

Our protocol design should achieve the following security and performance guarantees:

- *Public auditability*: To allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users
- Storage correctness: to ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact
- Privacy preserving: to ensure that the TPA cannot derive users' data content from the information collected during the auditing process
- Batch auditing: to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously
- Lightweight: To allow TPA to perform auditing with minimum communication and computation overhead

III. PROPOSED SCHEMES

Our public auditing scheme, which provides a complete outsourcing solution of data not only the data itself. We start from an overview of our public auditing system and discuss two straightforward schemes and their demerits after introducing notations and brief preliminaries. We present our main scheme and show how to extent our main scheme to support batch auditing for the TPA upon delegations from multiple users. We discuss how to generalize our privacy-preserving public auditing scheme and its support of data dynamics.

Definitions and Framework:

The context of remote data integrity checking and adapt the framework for our privacy preserving public auditing system. There are four algorithms present in the public auditing scheme:

a. *KeyGen*
   The user to setup the scheme runs a key generation algorithm
b. *SigGen*
   The user to generate verification metadata that may consist of digital signatures uses it
c. *GenProof*
   The cloud server to generate a proof of data storage correctness runs it
d. *VerifyProof*
   The TPA to audit the proof runs it.

Running a public auditing system consists of two phases:

Setup: The user initializes the public and secret parameters of the system by executing KeyGen and preprocesses the data file F by using SigGen to generate the verification metadata.

Audit: The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of the audit.

TPA does not need to maintain and update state between audits that is a desirable property especially in the public auditing system. It is easy to extend the framework above to capture a stateful auditing system that is essentially by splitting the verification metadata into two parts, which are stored by the TPA and the cloud server.

Basic Schemes

We study two classes of schemes as a warm up:

- It is a MAC-based solution which suffers from undesirable systematic demerits bounded usage and stateful verification in a public auditing setting. The auditing problem is still not easy to solve even if we have introduced a TPA.
- A system based on homomorphic linear authenticators that covers many recent proofs of storage systems. We will pinpoint the reason why all existing HLA-based systems are not privacy preserving.

MAC-based solution: There are two possible ways to make use of MAC to authenticate the data. Trivial way is just uploading the data blocks with their MACs to the server and sends the corresponding secret key s_k to the TPA. To circumvent the requirement of the data in TPA verification, one may restrict the verification to just consist of equality checking. The TPA can reveal a secret key sk_T to the cloud server and ask for a fresh-keyed MAC for comparison in each audit. It is privacy preserving as long as it is impossible to recover F in full given MAC_{skT} (F) and sk_T.

HLA-based solution: To effectively support public auditability without having to retrieve the data blocks themselves can be used. HLAs are also some unforgeable verification metadata that authenticate the integrity of a data block. It is possible to compute an aggregated HLA, which authenticates a linear combination of the individual data blocks. Though allowing efficient data auditing and consuming only constant bandwidth and the direct adoption of these HLA based techniques is still not suitable for our purposes.

IV. EVALUTION

SECURITY ANALYSIS:

The security of the proposed scheme by analyzing its fulfillment of the security guarantee, the storage

correctness and privacy preserving property. We show the security guarantee of batch auditing for the TPA in multiuser setting.

Storage Correctness Guarantee

We need to prove that the cloud server cannot generate valid response for the TPA without faithfully storing the data. The extractor controls the random oracle h(.) and answers the hash query issued by the cloud server. Suppose that our extractor can rewind a cloud server in the execution of the protocol to the point just before the challenge h(R) is given.

Security Guarantee for Batch Auditing

We show that our way of extending our result to a multiuser setting will not affect the aforementioned security insurance. The privacy-preserving guarantee in the multiuser setting is very similar and thus omitted here. The verification equation for the batch audits involves K challenges from the random oracle. we need time, to ensure that all the other K-1 challenges are determined before the forking of the concerned random oracle response.

PERFORMANCE ANALYSIS

We consider our auditing mechanism to users data outsources happens between a dedicated TPA and some cloud storage node. The cloud server side process is implemented on Amazon Elastic Computing Cloud (EC2) with a large instance type. when using the cloud storage auditing users have to pay both the storage cost and the bandwidth cost because the cloud is a pay-per-use model. we conduct the experiment with two different sets of storage/communication tradeoff parameter 's'.

If s=1 the mechanism incurs extra storage cost as large as the data itself. However, it takes very small auditing bandwidth cost. we also choose a properly larger s = 10 that reduces the extra storage cost to only 10 percent of the original data but increases the auditing bandwidth cost roughly 10 times larger than the choice of s = 1.

Cost of Privacy-Preserving Protocol

We begin by estimating the cost in terms of basic cryptographic operations. Suppose there are c random blocks specified in the challenge message chal during the Audit phase. we quantify the cost introduced by the privacy preserving auditing in terms of server computation. In the following privacy-preserving cost analysis we only give the atomic operation analysis for the case s = 1 for simplicity.

Batch Auditing Efficiency

Considering only the total number of pairing operations gives an asymptotic efficiency analysis on the batch auditing. There are additional less expensive operations required for batching like modular exponentiations and multiplications. whether the benefits of removing pairings significantly outweighs these additional operations remains to be verified. The performance of the corresponding non-batched, auditing is provided as a baseline for the measurement. Consider the settings c = 300 and c = 460 that is computed by dividing total auditing time by the number of tasks as shown in the fig.1.

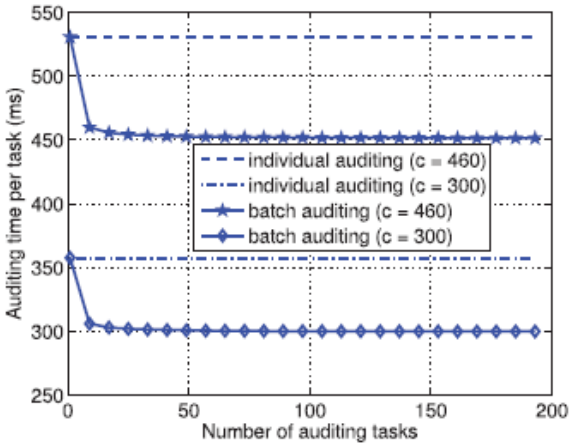

Fig. 2. Comparison on auditing time between batch and individual auditing: Per task auditing time denotes the total auditing time divided by the number of tasks.

It can be shown that compared to individual auditing, batch auditing indeed helps reducing the TPA's computation cost.

V. CONCLUSION

We propose a privacy-preserving public auditing system for data storage security in cloud computing.

The utilization of the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files. Our privacy-preserving public auditing protocol into a multiuser setting can perform multiple auditing tasks in a batch manner for better efficiency. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of our design on both the cloud and the auditor side.

VI. REFERENCE

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html, June 2009.

[2] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof-mass-email-deletions/, 2006.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.

[4] 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, "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

[5] Amazon.com, "Amazon s3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, July 2008.

[6] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors," http:// www.techcrunch.com/2008/07/10/mediamaxthelinkup-closesits- doors/, July 2008.

[7] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.

[9] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof-mass-email-deletions/, 2006.

[10] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," http://www.cloudsecurityalliance.org, 2009.