International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.5, pp : 601-603 1 May 2014

TPA For Privacy-Preserving Using Safe Cloud Storage

[1]Mr.Dhayalan.D, [2]M.Lavanya
Department of Computer Application, VeltechMultitechDr.RangarajanDr.Sakunthala Engineering College
Email ID:[1]dayalan.moorthy@rediffmail.com,[2]lavanya1073@gmail.com

Abstract:
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.Enabling public auditability for cloudstorage is important so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. Here we propose a secure cloud storage system supporting privacy-preserving publicauditing.

Keywords:
ThirdPartyAuditor,Integrity,Cloud Computing, Security.

1. INTRODUCTION

Cloud computing has been envisioned as the next generationinformation technology (IT) architecture forenterprises, suitable to its lengthyrecord of exceptional advantagesin the IT history: ubiquitous network access,rapid resource elasticity, location independent resource pooling usage-based pricing and transferenceof risk . As a disruptive technology, cloud computing is transforming the nature of how businesses use information technology. Onefundamental aspect of this pattern is shifting of data that arebeing centralized or outsourced to the cloud.While cloud computing makes these advantages moreimploring than ever, it also brings new challengingsecurity threats toward users 'outsourced data. Since cloudservice providers (CSP) are separate entities,data outsourcing is relinquishing user's ultimatecontrol over their data. To ensure the security of an effective TPA, the auditing process should bring no new vulnerabilities towards the user data privacy, and it should not be a burden to user.Accessing the data easily using local data storage and maintenance.

2. DIFFICULTY STATEMENT

2.1The Scheme and Threat Model

We consider a cloud data storage service involving threedifferent entities, the cloud user, whohas large amount of data files to be stored in the cloud; thecloud server, which is done by the cloud service provider toprovide data storage service and has significant storage

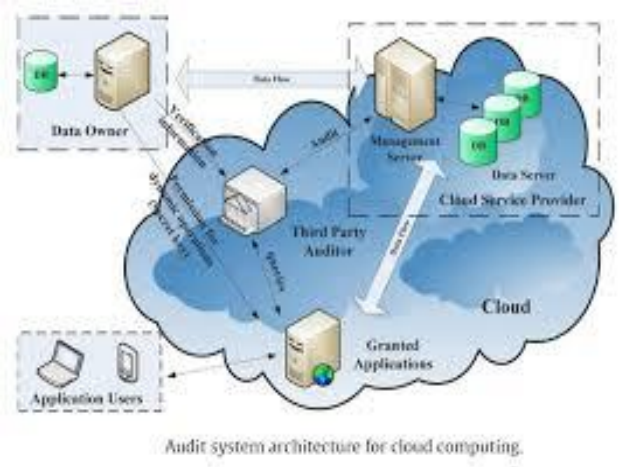


Figure: The architecture of cloud data storage service.

Space, computation resources; the third-party auditor, who has capabilities that cloud users is trusted to assess the cloud storage service reliability onbehalf of the user upon request.We assume the data integrity threats toward users' datacan comefrom both internal and external attacks at CS.These may include: software bugs, hardware failures, bugsin the network path, economically motivated hackers,malicious or accidental management errors, etc. Besides,CS can be self-interested.To authorize the CS to respond to the audit represented by the
TPA's, the user can issue a certificate on TPA's public key,and the TPA are authenticated against sucha certificate.

2.2 Design Goals

To enable privacy-preserving public auditing for cloud datastorage which is previously mentioned model, our obligation should achieve the following security and performanceguarantees:
1. **Public auditability**: To allow TPA to verify thecorrectness of the cloud data on demand withoutretrieving a copy of the whole data or introducingadditional online burden to the cloud users.
2. **Storage correctness**: to ensure that there exists nocheating cloud server that can pass the TPA's auditwithout indeed storing users' data intact.
3. **Privacy preserving**: to ensure that the TPA cannotderive users' data content from the informationcollected during the auditing process.
4. **Batch auditing**: to enable TPA with secure andefficient auditing capability to cope with multipleauditing delegations from possibly large number ofdifferent users simultaneously.
5. **Lightweight:** to allow TPA to perform auditingwith minimum communication and computationoverhead.

3. THE PROPOSED SYSTEM

Here we present our public auditing scheme whichprovides a complete outsourcing solution of data—not only the data itself, but also its unimpaired checking.

3.1 Notation and Preliminaries

F—the data file to be outsourced, denoted as asequence of n blocks $m_1,..,m_i...m_n \in Z_p$ forsome large prime p.
$MAC_{(.)}(.)$—message authentication code can be defined as: $K\times\{0,1\}^* \rightarrow \{0,1\}^l$ where Kdenotesthe key space..
H(.),h(.)—cryptographic hash functions.

3.2 Definitions and Framework

We follow a similar definition of previously proposedschemes in the context of remote data integrity checking and adapt the framework for our privacy preservingpublic auditing scheme. A public auditing system contains four algorithms(KeyGen, SigGen, GenProof, VerifyProof).

3.3 The Basic System

Before producing our main result, we study two classes ofschemes as a warmup.

MAC-based solution.There are two possible ways tomake use of MAC to attest the data. A common way is just uploading the data blocks with their MACs to the server, and sens the corresponding secret key *sk* to theTPA. Afterwards, the TPA can indiscriminatelyrecover blocks with theirMACs and check the correctness via sk. Apart from thehigh (linear in the sampled data size) communication andcalculation complexities, the TPA requires the informationof the data blocks for confirmation.

HLA-based solution

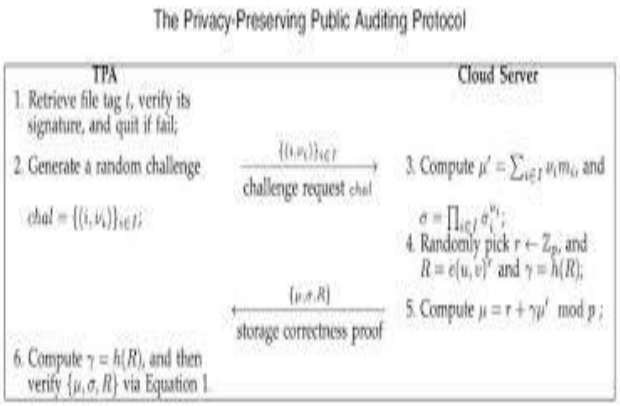
. To effectively support publicauditability without having to retrieve the data blocksthemselves, the HLA technique can be used.HLAs, like MACs, are also some unforgeable verificationmetadata that authenticate the integrity of a data block.
Though allowing efficient data auditing and consumingonly constant bandwidth, the direct adoption of these HLAbasedtechniques is still not suitable for our purposes. Thisis because the linear uniting of blocks,may reveal user data in sequence to TPA, andviolates the privacy-preserving assurance. Specifically, bychallenging the same set of c blocks $m_1,m_2,...,m_c$ using different sets of random coefficients $\{v_i\}$ TPA canaccumulate c different linear combinations WithTPA can derive the user's data $m_1,m_2,..,m_c$by simply solving a system of linear equations.

3.4Privacy preserving public auditing system

To achieve privacy-preserving public auditing,we come up to uniquely integrate the homomorphic linearauthenticator with random masking method. In our protocol, the linear arrangement of sampled blocks in theserver's response is masked with randomness generated bythe server.

Properties of our protocol.

There is no secret keying material or states for the TPA to maintain between audits, and thus auditing protocol does not pose any potential online trouble on users.



This approachensures the retreat of user data satisfied during the auditingprocess by employing a random masking, alinear combination of the data blocks..

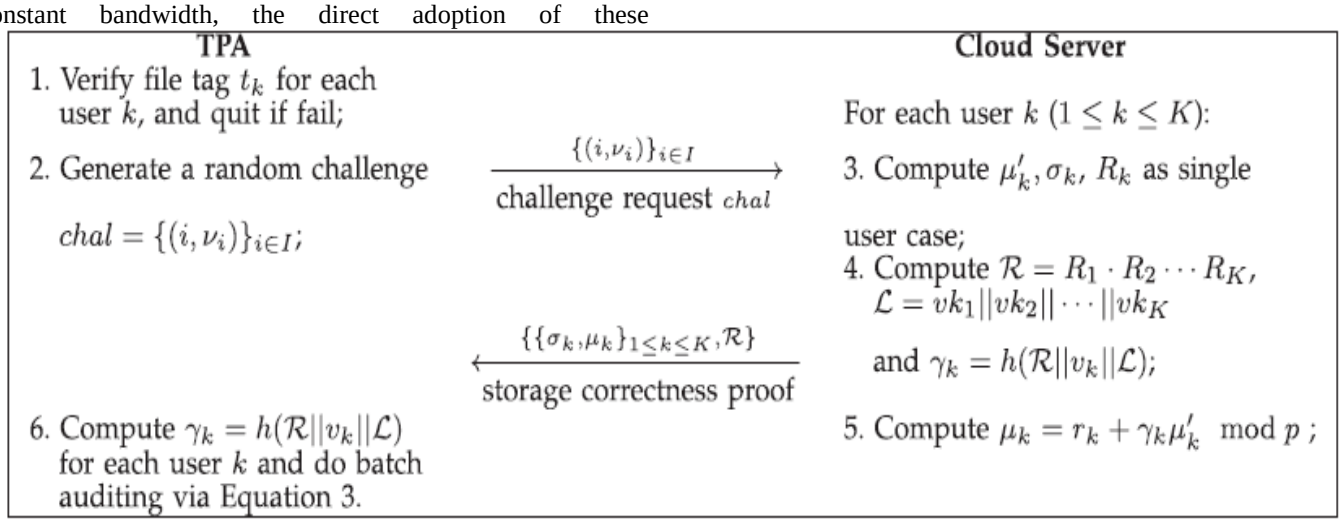


Figure 1the Batch Auditing Protocol

3.5Support for Batch Auditing

With the establishment of privacy-preserving publicauditing, the TPA may along withholdseveralauditing upon different users' delegation.

Setup phase: Basically, the users just perform Setupindependently. If suppose there are K users in the system, each user k has a data to beoutsourced to the cloud server.

Audit phase: TPA first retrieves and verifies file tag tkfor each user k for auditing. If the checking fails,

TPA quits by emitting FALSE. Otherwise, TPA recovers $name_k$ and sends the audit challenge chal={(i,v_i)} tothe server for auditing data files of all K users.

Efficiency improvement.

Batch auditingnot only allows TPA to perform the multiple auditingtasks simultaneously, it also reduces the computationcost on the TPA side. This is for the reason that aggregatingK confirmation equations into one helps reduce the numberof relatively expensive pairing operations from 2K, isrequired in the individual auditing, for K þ 1, which saves aconsiderable amount of auditing time.

Identification of invalid responses.

The verificationequation holds when all the responses are valid, fails with high probability when there is even onesingle invalid response in the batch auditing.

4. EVALUATION

4.1 Security Analysis

We criticize the security of the proposed system byanalyzing its fulfillment of the security guarantee

4.1.2 Privacy-Preserving Guarantee

The theorem shows that the TPA cannot derive users'data from the information collected at the time of auditing.

Theorem 1. From the server's response {σ,μ,R}, TPA cannotrecover μ'.

Proof. We show the existence of a simulator that canproduce a valid response even without the knowledge of μ', in the random oracle model. Finally, We remark that this backpatchingtechnique in the random oracle model is also used inthe proof of the underlying scheme.

4.1.3 Security Guarantee for Batch Auditing

Now, the way of extending our result is amultiuser setting will not affect the aforementioned securityinsurance.

4.2 Performance Analysis

The TPA/user side process is implemented on a workstationwith an Intel Core 2 processor runs at 1.86 GHz,2,048 MB of RAM, and a 7,200 RPM Western Digital250 GB Serial drive. The cloud server side process isimplemented on Amazon Elastic Computing Cloud (EC2)with a large instance type, which has 4 EC2 ComputeUnits, 7.5 GB memory, and 850 GB instance storage. Theactual generated test data is of 1 GB size.Because the cloud is a pay-per-use model, users have topay both the storage cost and the bandwidth cost (for datatransfer) when using the cloud storage auditing.

5. CONCLUSION

The data content stored on the cloudserver during the efficient auditing process, it not onlyeliminates the burden of cloud user andpossibly expensive auditing task. ConsideringTPA may concurrently handle multiple audit sessions fromdifferent users for their outsourced data files areextend our privacy-preserving public auditing protocol intoa multiuser location, somewhere the TPA can executeseveralauditing tasks in a batch manner for better efficiency.An importantupcomingexpansion, which is predictable to stronglymanagebyvery large scale data and thus encourage users to adopt cloudstorage services more confidently.

6. ACKNOWLEDGMENTS

This work was supported in part by the US National Science Foundation (NSF) under grants CNS-1054317, CNS-1116939, CNS-1156318, and CNS-1117111, and by Amazonweb service research grant. A preliminary version [1] of this paper was presented at the 29th IEEE Conference on Computer Communications (INFOCOM '10).

7. REFERENCES

i. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-PreservingPublic Auditing for Storage Security in Cloud Computing," Proc.IEEE INFOCOM '10, Mar. 2010.

ii.Cloud Data Storage Services Using Third Party Auditor

iii.Cloud Security Alliance, "Top Threats toCloud Computing,

"http://www.cloudsecurityalliance.org, 2010.

iv.Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling PublicAuditability and Data Dynamics for Storage Security in CloudComputing," IEEE Trans. Parallel and Distributed Systems, vol. 22,no. 5, pp. 847-859, May 2011.

v.Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud

Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22,

no. 5, pp. 847-859, May 2011.

vi. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable Data Possession at UntrustedStores," Proc. 14th ACM Conf. Computer and Comm. Security

(CCS '07), pp. 598-609, 2007.

vii. M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-PreservingAudit and Extraction of Digital Contents," Cryptology ePrintArchive, Report 2008/186, 2008.

viii.A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievabilityfor Large Files," Proc. ACM Conf. Computer and Comm. Security

(CCS '07), pp. 584-597, Oct. 2007.

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

x. H. Shacham and B. Waters, "Compact Proofs of Retrievability,"

Proc. Int'l Conf. Theory and Application of Cryptology and Information

Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107,