INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 2, Issue 3 OCT 2014

# ENABLING AUDITABILITY FOR SECURE CLOUD STORAGE USING TPA

**[1] Chennuri. Kranthi kumar, [2] Vishakha Lokhande**

[1]M.Tech Student, Department of CSE, KG reddy College Of Engineering and Technology , Chilkur village, Moinabad Mandal, Rangareddy District, A.P, India.

[2] Assistant Professor, Department of CSE, KG reddy College Of Engineering and Technology, Chilkur village, Moinabad Mandal, Rangareddy District, A.P, India.

**ABSTRACT:**
Cloud computing is the arising technology to minimize the utilizer burden in the updation of data in business utilizing internet. Instead of local data storage and maintenance, the utilizer is availed with the cloud storage so that the utilizer can remotely store their data and relish the on-demand high quality application from a shared pool of resources. Cloud computing sanctions users to utilize applications without installation any application and access their personal files and application at any computer with internet access. Cloud Computing is technology for next generation Information and Software enabled work that is capable of transmuting the software working environment. The major quandary of cloud data storage is security. Many researchers have proposed their work or incipient algorithms to achieve security or to resolve this security quandary. In this paper, we propose an incipient innovative conception for Privacy Preserving Public Auditing with watermarking for data Storage security in cloud computing. It fortifies data dynamics where the utilizer can perform sundry operations on data like insert, update and expunge as well as batch auditing where multiple utilizer requests for storage correctness will be handled simultaneously which reduce communication and computing cost.

**1 INTRODUCTION**

Cloud accommodation providers manage an enterprise-class infrastructure that offers a scalable, secure and reliable environment for users, at a much lower marginal cost due to the sharing nature of resources. It is routine for users to utilize cloud storage accommodations to apportion data with others in a group, as data sharing becomes a standard feature in most cloud storage offerings, including Dropbox and Google Docs. Using cloud storage, usre can remotly store their data and relish the on-demand high quality applications and accommodations from a shared pool of configurable computing resources, without the encumbrance of local data storage and maintenance.

However, the fact the utilizer on longer have physical possession of the outsourced data makes the data integrity aegis in cloud computing a formidable task, especially for the users with constrained computing resource. Enabling public audit ability for cloud storage is of critical consequentiality so that utilizer can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an efficacious TPA, the auditing process should bring in no incipient susceptibilities towards utilizer data privacy, and introduce no adscititious online burden to utilizer. Here the a secure cloud storage system fortifying privacy preserving public auditing is proposed.

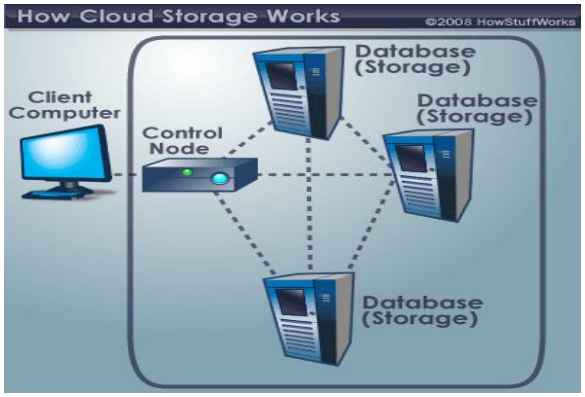


Fig. 1 Cloud Storage

## 2. PROBLEM DEFINITION

Cloud server, storage, cloud accommodation provider to provide the accommodation, and the utilizer is a substantial amount of data files stored in the cloud, which is carried through the cloud, it's paramount data: stored in cloud storage values for three different companies. Space and computational resources (we do not differentiate CS and CSP hereafter), a third-party auditor, expertise and capabilities that the cloud users, and to assess the reliability of a trusted cloud storage accommodation request on behalf of a utilizer. Based on the users of cloud storage and management, for the CS. Dynamic access to the stored data, and update the contact CS for sundry application purposes. Users will no longer be stored and maintained congruously to their data is a crucial part of users, to have their data locally. Outsourced cloud storage data for long-term immensely colossal-scale economic terms, but it is no assurance that the integrity of the data and is available immediately. This quandary, if not, may impede the prosperity of cloud structure. Periodic verification of the correctness of the calculation and storage, as well as the potential source of the cloud users may resort to TPA for ascertaining the integrity of outsourced data storage, online would preserve weight. Allows the utilizer to an external part, in additament to the correctness of remotely stored data, to verify the ability of a public audit. However, these schemes, external auditors should be considered against the aegis of the privacy of customer data.

### 2.1 Design Goals

To enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantees.

1) 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.

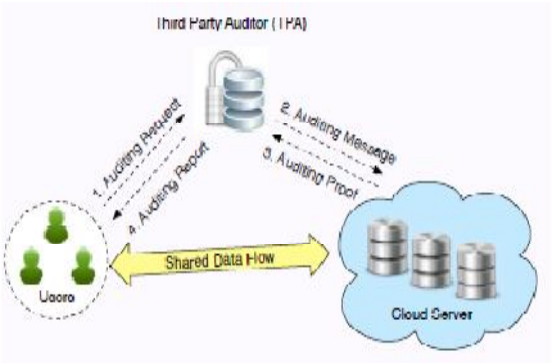


Fig. 2: The architecture of cloud data storage service

2) Storage correctness: to ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact.

3) Privacy-preserving: to ensure that the TPA cannot derive users' data content from the information collected during the auditing process.

4) 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.

5) Lightweight: to allow TPA to perform auditing with minimum communication and computation overhead.

## 3. Privacy-Preserving Public Auditing

The privacy-preserving public auditing, we propose to uniquely integrate the homomorphic non-linear authenticator with arbitrary masking technique. In our protocol, the non-

linear blocks in the server's replication is masked with desultoriness engendered the server. With desultory masking, the TPA no longer has all the compulsory information to build up a correct group of non-linear equations and therefore cannot derive the user's data content, no matter how many linear cumulations of the same set of file blocks can be amassed. On the other hand, the correctness validation of the block authenticator dyads can still be carried out in an incipient way even with the presence of the arbitrariness. Our design makes utilization of a public key predicated HLA, to equip the auditing protocol with public auditability. Specifically, which is predicated on the short signature scheme.

**Periodic Sample Audit :** In the Cloud Server environment arbitrary "sampling" checking greatly reduces the workload of audit accommodations, while still achieve an efficacious detection of misconduct. Thus, the probabilistic audit on sampling checking is preferable to realize the abnormality detection in a timely manner, as well as rationally allocate resources. The fragment structure can provide the fortification of probabilistic audit as well: given an arbitrary culled challenge (or query) Q = {(i, vi)}iεI , where I is a subset of the block indices and vi is a desultory coefficient, an efficient algorithm is utilized to engender a constant-size replication(μ1, μ2, … , μs, _′), where μi emanates from all {mk,i, vk}kεI and all {_k, vk}kεI . Generally, this algorithm relies on homomorphic properties to aggregate data and tags into a constant size replication, which minimizes network communication. Since the single sampling checking may overlook a diminutively minuscule number of data abnormality, we propose a periodic sampling approach to audit outsourcing data, which is called as Periodic Sampling Audit. In this way, the audit activities are efficiently scheduled in an audit period, and a TPA needs merely access diminutive portions of file to perform audit in each activity. Therefore, this method can detect the exceptions in time, and reduce the sampling numbers in each audit.

**Security Consistency for Batch Auditing:** The way to describe the result to a multi-utilizer setting will not affect the aforementioned security indemnification, as shown in the Theorem.

**Theorem:** The batch auditing protocol achieves the same storage correctness and privacy preserving guarantee as in the single-utilizer case.

## 4. THE PROPOSED SOLUTION

My work focus on data storage, cloud computing is in some parts of the first in the privacy -preserving public auditing Support. Besides, the prevalence of cloud computing, with the auditing tasks from different users may be delegated to The predictable increase in the tpa. Without demanding the local copy of the data in our work allows tpa to perform Auditing and so completely straightforward to define the data and computational overhead compared to the auditing Procedures reduces the use of public-key based homomorphic linear authenticator or hla process . Tpa our protocol Effectively masking random auditing process by integrating with the hla cloud server (cs) is not a promise to learn The knowledge of the content stored in the data. Authenticator and the algebraic properties of the aggregation of our Design for the purpose of auditing more batch

TABLE I

COMPARISON WITH EXISTING MECHANISMS

| | PDP [2] | WWRL [3] | Oruta |
|---|---|---|---|
| Public auditing | Yes | Yes | Yes |
| Data privacy | No | Yes | Yes |
| Identity privacy | No | No | Yes |

A high-level comparison between Existing mechanisms in the literature is shown in table 1. To Our best knowledge, this paper represents the first attempt Towards designing an effective privacy-preserving public auditing mechanism for shared data in the cloud.

**SOLUTION:** the privacy-preserving guarantee in the

multiuser setting. The storage correctness guarantee, we are Going to reduce it to the single- user case. We use the forking Technique for the verification equation for the batch audits Involves k challenges from the random block. This time we Need to ensure that all the other k − 1 challenges are Determined before the forking of the concerned random Oracle response. This can be done using the idea in [4]. As Soon as the adversary issues the very first random oracle Query for i = h(r||vi||l) for any i ε [1,k], the simulator Immediately determines the values j = h(r||vj ||l) for all j ε [1,k]. This is possible since they are all using the same r And l. Now, all but one of the k's are equal, so a valid Response can be extracted similar to the single-user case.

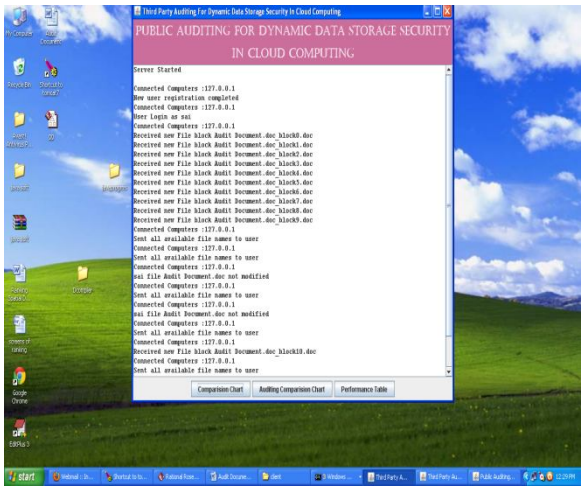


Fig. 3 TPA operations

## 5. CONCLUSION AND FUTURE WORK

This paper will proposed a privacy-preserving public auditing system for data storage security in cloud computing. We Develop the homomorphic linear authenticator and desultory masking to ensure that the tpa would not learn any Knowledge about the data content stored on the cloud server during the efficient auditing process, which not only Disregards the encumbrance of cloud utilizer from the tedious and possibly expensive appraising task, but withal alleviates the Users' trepidation of their outsourced data leakage.we leave the full-fledged implementation of the mechanism on commercial Public cloud as a consequential future allowance, which is expected to vigorously cope with profoundly and immensely colossal scale data and thus Encourage users to adopt cloud storage accommodations more confidently. Considering tpa may concurrently handle multiple Audit sessions from different users for their outsourced data files, as a future work, we further elongate our privacy preserving public auditing protocol into a multiuser setting, where the tpa can execute multiple auditing tasks in a Batch manner for more preponderant efficiency.

## REFERENCES

[1]. M.A. Shah, M. Baker, J.C. Mogul, and R.Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.

[2].R. Curtmola, O. Khan, and R. Burns, "Robust Remote Data Checking," Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (StorageSS '08), pp. 63-68, 2008

[3] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4,pp. 19-24, July/Aug. 2010.

[4] K. Yang and X. Jia, "Data Storage Auditing Service in CloudComputing: Challenges, Methods and Opportunities," World Wide Web, vol. 15, no. 4, pp. 409-428, 2012.

[5]Shrinivas, "Privacy-Preserving Public Auditing in Cloud Storage security", International Journal of computer science nad Information Technologies, vol 2, no. 6, pp. 2691-2693, ISSN: 0975-9646, 2011

[6]XU Chun-xiang, HE Xiao-hu, Daniel Abraha,"Cryptanalysis of Auditing protocol proposed by Wang et al. for data storage security in cloud computing", http://eprint.iacr.org/2012/115.pdf,and cryptologyeprintarchieve: Listing for 2012

[7]Abhishek Mohta, Lalit Kumar Awasti, "Cloud Data Security while using Third Party Auditor", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, ISSN 2229-8 June 2012.

[8] C. Hota, S. Sanka, M. Rajarajan, S. Nair, "Capabilitybased Cryptographic Data Access Control in Cloud Computing", in International Journal of Advanced Networking and Applications, Volume 01, Issue 01, 2011.

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

[11] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song. Provable data possession at untrusted stores. In Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, pages 598–609, 2007.

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