*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 5, Ver. I (Sep.- Oct. 2017), PP 27-30*
*www.iosrjournals.org*

# Privacy Preserving Public-Auditing for secure cloud Storage

*Naveena M , Bharath S Chetty, G hemantha Kumar
*Department of Studies in Computer Science, University of Mysore Manasagangotri-570006, Mysore, INDIA.*
*Corresponding Author: Naveena M*

***Abstract:*** *This privacy preserving public auditing for secure cloud storage will be carried out to design and develop Cloud computing technology which makes long dreamed vision of computing as a utility, where users can remotely store their data into the cloud. 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. For that purpose we securely introduce an effective third party auditor, 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. our contribution in this work can be summarized as, we motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol, achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA. And finally we prove the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state of the art.*

***Indexterms:*** *Data integrity, Storage auditing, dynamic auditing, privacy-preserving auditing, cloud computing, zero knowledge.*

---

Date of Submission: 24-08-2017 Date of acceptance: 08-09-2017

---

## I. Introduction

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 auditability 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.

Cloud Computing has been envisioned as the next-generation architecture of IT enterprise, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricking and transference of risk. As a Cloud Computing technology is transforming the very nature of how businesses use information technology and also data is being centralized or outsourced into the Cloud.

The advantages of using clouds are unarguable, as separate administrative entities, the internal operation details of cloud service providers may not be known by cloud users. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First, 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. Secondly, for the benefits of their own, there does exist various motivations for cloud service providers to behave unfaithfully. 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.

As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. Thus, how to efficiently verify the correctness of outsourced cloud data without the local copy of data files becomes a big challenge for data storage security in Cloud Computing.

Considering the large size of the outsourced data and the user's constrained resource capability, the ability to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users. Data storage so that the users may resort to a third party auditor, who has expertise and capabilities that the users do not, to audit the outsourced data when needed. Based on the audit result, TPA could release an audit report, which would not only help users to evaluate the risk of their subscribed cloud data services, but also be beneficial for the cloud service provider to improve their cloud based service platform . In a word, enabling public risk auditing protocols will play an important role for this nascent cloud.

## II. Literature Survey

We can find some of the works carried out in this cloud computing security, it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then next step is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

Ateniese et al. are the first to consider public audit ability in their "provable data possession" model for ensuring possession of data files on untrusted storages. They utilize the RSA-based homomorphic linear authenticators for auditing outsourced data and suggest randomly sampling a few blocks of the file. However, among their two proposed schemes, the one with public auditability exposes the linear combination of sampled blocks to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the external auditor.

Shah et al., propose introducing a TPA to keep online storage honest by first encrypting the data then sending a number of pre computed symmetric-keyed hashes over the encrypted data to the auditor. The auditor verifies the integrity of the data file and the server's possession of a previously committed decryption key. This scheme only works for encrypted files, requires the auditor to maintain state, and suffers from bounded usage, which potentially brings in online burden to users when the keyed hashes are used up. Dynamic data have also attracted attentions in the recent literature on efficiently providing the integrity guarantee of remotely stored data.

Concurrently, elway et al. Develop a skip list based scheme to also enable provable data possession with full dynamics support. However, the verification in both protocols requires the linear combination of sampled blocks as an input, like the designs in, and thus does not support privacy-preserving auditing.

In other related work, Sebe et al. thoroughly study a set of requirements which ought to be satisfied for a remote data possession checking protocol to be of practical use. Their proposed protocol supports unlimited times of file integrity verifications and allows preset tradeoff between the protocol running time and the local storage burden at the user.

Schwarz and Miller propose the first study of checking the integrity of the remotely stored data across multiple distributed servers. Their approach is based on erasure-correcting code and efficient algebraic signatures, which also have the similar aggregation property as the homomorphic authenticator utilized in our approach.

We have revised the paper a lot and improved many technical details as compared as, First, we provide a new privacy-preserving public auditing protocol with enhanced security strength in For completeness, we also include an additional protocol design for provably secure zero-knowledge leakage public auditing scheme in Second, based on the enhanced main auditing scheme, we provide a new provably secure batch auditing protocol. All the experiments in our performance evaluation for the newly designed protocol are completely redone. Third, we extend our main scheme to support data dynamics in, and provide discussions on how to generalize our privacy-preserving public auditing scheme, which are lacking in . Finally, we provide formal analysis of privacy-preserving guarantee and storage correctness, while only heuristic arguments are sketched.

## III. Existing System

In the Existing systems, 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, in addition to the user himself, to verify the correctness of remotely stored data. However, most of these schemes do not consider the privacy protection of users' data against external auditors. Indeed, they may potentially reveal user's data to auditors. This severe 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 toward their data security.

In the Existing System, Cloud Computing brings new and challenging security threats towards users' outsourced data. Cloud Service Providers are separate administrative entities; data outsourcing is actually 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. 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.

To securely introduce an effective third party auditor, the following two fundamental requirements have to be met first, 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; second, The third party auditing process should bring in no new vulnerabilities towards user data privacy.

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.

## IV. Proposed Model

In this project we utilize the public key based homomorphic authenticator and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. 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. We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users.

## V. System Archetecture

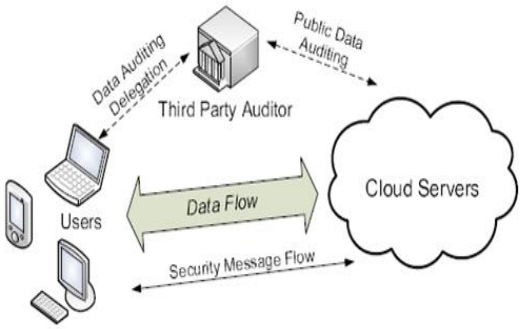


**Fig. 1.** The architecture of cloud data storage service.

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

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 on-line burden to the cloud users.

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

3) Privacy-preserving: to ensure that there exists no way for TPA to 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.

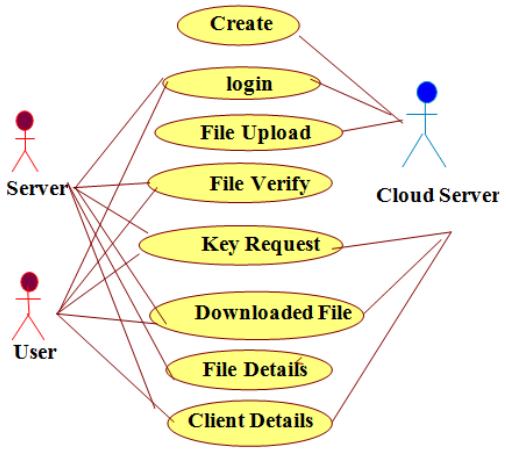


**Fig. 2.** Use case Diagram of Secure audit service by using TPA for data integrity in cloud system.

## VI. Conclusion

We propose a privacy-preserving public auditing system for data storage security in Cloud Computing, where TPA can perform the storage auditing without demanding the local copy of data. We utilize the homomorphic authenticator and random mask technique to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the user's fear of their outsourced data leakage. Here we Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner or simultaneously. Extensive security and performance analysis shows that the proposed schemes are provably secure and highly efficient. We believe all these advantages of the proposed schemes will shed light on economies of scale for Cloud Computing.

## References

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in computing,"Proc. IEEE INFOCOM '10,Mar. 2010.
[2] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling PublicAuditability and Data Dynamics for Storage Security in Cloud Computing,"IEEE Trans. Parallel and Distributed Systems, vol. 22,no. 5, pp. 847-859, May 2011.
[3] Cloud Security Alliance, "Top Threats to Cloud Computing,"http://www.cloudsecurityalliance.org, 2010.
[4] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-PreservingAudit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.
[5] G. Ateniese, S. Kamara, and J. Katz, "Proofs of Storage fromHomomorphic Identification Protocols,"Proc. 15th Int'l Conf.Theory and Application of Cryptology and Information Security:
[6] Advances in Cryptology (ASIACRYPT),pp. 319-333, 2009.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Naveena M. "Privacy Preserving Public-Auditing for secure cloud Storage ." IOSR Journal of Computer Engineering (IOSR-JCE) , vol. 19, no. 5, 2017, pp. 27–30.