© 2017 IJSRST | Volume 3 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

# Implementation of Data Privacy Framework for Public Cloud Storage

**Apeksha A. Dhone[1], Prof. Avinash P. Wadhe[2]**

[1]Department of Computer Science & Engineering, G.H. Raisoni College of Engineering & Management, Amravati, Maharashtra, India
[2]Department of Computer Science & Engineering, G.H. Raisoni College of Engineering & Management, Amravati, Maharashtra, India

## ABSTRACT

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality services and applications from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, to protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage together with data integrity checking and failure reparation becomes critical. Recently, regenerating codes have gained popularity due to their lower repair bandwidth while providing fault tolerance. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Many mechanisms dealing with the integrity of outsourced data without a local copy have been proposed under different system and security models up to now 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. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. Many mechanisms dealing with the integrity of outsourced data without a local copy have been proposed under different system and security models up to now. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

**Keywords:** Cloud Storage, Regenerating Codes, Public Audit, Privacy Preserving, Authenticator Regeneration, Proxy, Privileged, And Third Party Auditor

## I. INTRODUCTION

Cloud computing is innovation that uses advanced computational power and improved storage capabilities. Cloud computing is a long dreamed vision of computing utility, which enable the sharing of services over the internet. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing resources, on-demand network access and provisioned by the service provider. The advantage of cloud is cost savings. The prime disadvantage is security. Cloud computing is used by many software industries. Since the security is not provided in cloud, many companies adopt their unique security structure. The data placed in the cloud is accessible to everyone, security is not guaranteed. To ensure security, cryptographic techniques cannot be directly adopted. Sometimes the cloud service provider may hide the data corruptions to maintain the reputation. To avoid this problem, we introduce an effective third party auditor to audit the user's outsourced data when needed. The security is achieved by RC5 Encryption Algorithm. We utilized public key based homomorphic authenticator with random masking to achieve privacy preserving auditing protocol.TPA performs the auditing task for each user.

Third Party Auditor is kind of inspector. There are two categories: private auditability and public auditability. Although private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would help owners to evaluate the risk of their subscribed cloud data services, and it will also be beneficial to the cloud service provider to improve their cloud based service platform [3]. Hence TPA will help data owner to make sure that his data are safe in the cloud and management of data will be easy and less burdening to data owner. Cloud consumers save data in cloud server so that security as well as data storage correctness is primary concern. A novel and homogeneous structure is introduced [4] to provide security to different cloud types. It allows TPA to perform multiple auditing tasks for different users at the same.

## II. LITERATURE SURVEY

In this paper, we focus on the integrity verification problem in regenerating-code-based cloud storage, especially with the functional repair strategy. Considering the large size of the outsourced data and the user's constrained resource capability, the tasks of auditing and reparation in the cloud can be dangerous and expensive for the users.

It is the technique to analyze storage architectures that combine any form of coding and replication, as well as presenting two new schemes for maintaining redundancy using erasure codes. It minimizes the amount of bandwidth used to maintain that redundancy. Storing a file using an erasure code, in fragments spread across nodes, promises to require less redundancy and hence less maintenance bandwidth than simple replication to provide the same level of reliability [1].

In this paper, focuses on combination the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system. It supports efficient handling of multiple auditing tasks. They further explore the technique of bilinear aggregate signature to extend result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously [2].

In this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphism token and distributed erasure-coded data. proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. It proposed scheme is highly efficient and resilient against malicious data modification attack, and even server colluding attacks [3].

In this paper, we propose a new privacy preserving public auditing mechanism for shared data in an un trusted cloud. Here, we utilize ring signature so that the third party auditor is able to verify the integrity of shared data for a group of users without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the TPA. This paper provides a privacy preserving public auditing scheme that supports public auditing and identity privacy on shared data stored in the cloud storage service for enhancing its security and efficiency. This paper has mainly concentrated on improving the security mechanism of own Cloud storage service [4].

They design and implement a practical data integrity protection (DIP) scheme for a specific regenerating code, while preserving its properties of fault tolerance and repair traffic saving. DIP scheme is designed under a mobile and enables a client to feasibly verify the integrity of random subsets of outsourced data against general or malicious corruptions. It works under the simple assumption of thin-cloud storage and allows different parameters to be fine-tuned for a performance-security trade-off [5].

In this paper we proposed two schemes. First for auditing scheme and second for privacy preserving. Although previous paper introduced private remote data checking schemes for regenerating-code-based cloud storage. They proposed public auditing scheme which

allows the public verifier to audit the correctness of data even if the data owner is offline. First, this scheme constructs a BLS-based authenticator, which consists of two parts for each segment of coded blocks. The data owner is able to generate those authenticators in a new method, which is more efficient compared to the straightforward approach. This is the main paper of this research, this paper totally focus on the public auditing using proxy server and TPA (Third Party Auditor) for persevering data integrity even if the user is offline to lose the burden of data owner to be online [6].

## III. PROPOSED WORK

Our proposed system contains the cluster of cloud storages. It may call as "Cloud of clouds" or "multi clouds". These individual clouds are interconnected to each other. Here, the user uploaded file is replicated on more than one cloud storage that is two to three different interconnected but individual clouds. User host machine implements Shamir's secret sharing algorithm and it is responsible to generate the set of secret keys. To access a particular file, user must input a set of secret keys with minimum threshold value. Therefore, using these secret keys, machine can easily authenticate the user.

To manage the users' activity, the system administrator is introduced. System administrator has rights to authenticate the user and to update the user information. In this we focus on the integrity verification problem in regenerating-code-based cloud storage, especially with the functional repair strategy. To fully ensure the data integrity and save the users' computation resources as well as online burden, we propose a public auditing scheme for the regenerating-code-based cloud storage, in which the integrity checking and regeneration (of failed data blocks and authenticators) are implemented by a third-party auditor and a semi-trusted proxy separately on behalf of the data owner. Instead of directly adapting the existing public auditing scheme to the multi-server setting, we design a novel authenticator, which is more appropriate for regenerating codes. Besides, we "encrypt" the coefficients to protect data privacy against the auditor, which is more lightweight than applying the proof blind technique and data blind method. We will design a novel homomorphic authenticator based on BLS signature, which can be generated by a couple of secret keys and verified publicly.

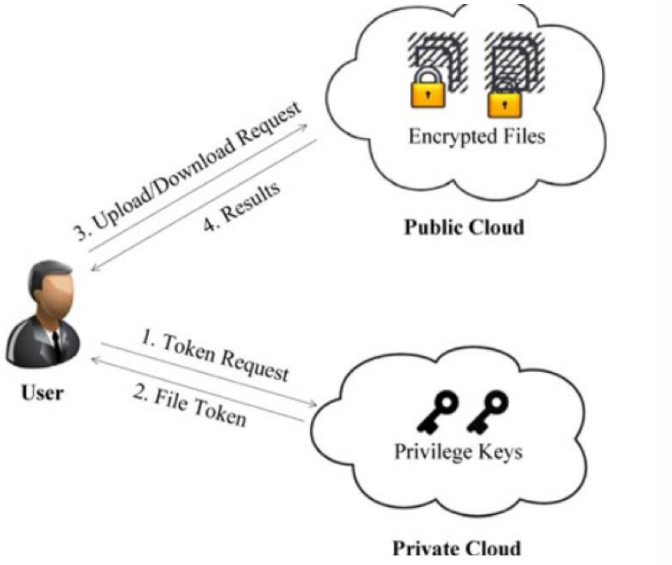


**Figure 1.** Diagram for Privacy Framework

In terms of security, it can be achieved by verifying the information each time it is queried and fail the request if it failed the verification. The advantages are, utilizing the linear subspace of the regenerating codes, the authenticators can be computed efficiently. Besides, it can be adapted for data owners equipped with low end computation devices (e.g. Tablet PC etc.) in which they only need to sign the native blocks. To the best of our knowledge, our scheme is the first to allow privacy-preserving public auditing for regenerating code- based cloud storage. The coefficients are masked by a PRF (Pseudorandom Function) during the Setup phase to avoid leakage of the original data.

This method is lightweight and does not introduce any computational overhead to the cloud servers or Third Party Auditor. Our scheme completely releases data owners from online burden for the regeneration of blocks and authenticators at faulty servers and it provides the privilege to a proxy for the reparation. Optimization measures are taken to improve the flexibility and efficiency of our auditing scheme; thus, the storage overhead of servers, the computational overhead of the data owner and communication overhead during the audit phase can be effectively reduced. Our scheme is provable secure under random oracle model against adversaries.

## IV.CONCLUSION

In this paper, we propose a privacy-preserving public auditing system for data storage security in Cloud Computing. In this paper, use the Third Party Auditor(TPA)to maintain to overkill this issue here, we are giving public auditing process for cloud storage that users can make use of a third-party auditor (TPA) to check the integrity of data. Not only verification of data integrity, the proposed system also supports data. Considering TPA may concurrently handle multiple audit sessions from different users for their data files which are outsourced, we further extend our privacy preserving public auditing agreement into a multi-user setting, where the TPA can perform the multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

## V. REFERENCES


[1] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag,2001.

[2] Farzad Sabahi Student Member, IEEE, "Cloud Computing Security Threats and Responses", Mar 2006.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards secure and dependable storage services in cloud computing," IEEE Transactions on Service Computing, 2007.

[4] A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007.

[5] J. Stanek, A. Sorniotti, E. Androulaki, and L. Kencl, "A secure data regeneration scheme for cloud storage," in *Technical Report*, 2013.

[6] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer, "Reclaiming space from regenerate files in a server less distributed file system." in *ICDCS*, 2002, pp. 617–624.

[7] P. Anderson and L. Zhang, "Fast and secure laptop backups with encrypted de-regeneration," in *Proc. of USENIX LISA*, 2010.

[8] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Dupless: Server aided encryption for deregenerated storage," in *USENIX Security Symposium*, 2013.

[9] Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian: Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage,2015.

[10] H. C. H. Chen and P. P. C. Lee, "Enabling data integrity protection in regenerating-coding-based cloud storage: Theory and implementation," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 407–416, Feb. 2014.

[11] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 9, pp. 1717–1726, Sep. 2013