Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

*IJCSMC, Vol. 2, Issue. 11, November 2013, pg.113 – 116*

RESEARCH ARTICLE

# Scalable and Efficient Provable Automatic Blocker in Cloud

**D. Arjun Reddy[1], P.S. Murthy[2], D. Baswaraj[3]**
[1,2,3]CMR Institute of Technology, Kandlakoya, Hyderabad, India

[1] *dendiarjun@gmail.com*, [2] *moorthypsm@gmail.com*, [3] *braj5555@yahoo.co.in*

***Abstract— Cloud computing plays a vital role in day to day life digital world. In every day the digital data is going to increase. To store this data we should require a large amount of databases to avoid all these conflicts we are moving to cloud storage concept. But the security is the issue. 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, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. 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. We propose, we propose a new innovative idea for Privacy Preserving Public Auditing with watermarking for data Storage security in cloud computing. It supports data dynamics where the user can perform various operations on data like insert.***

***Keywords: - Privacy Preserving; Public Auditing; Watermarking; TPA; Security***

## I. INTRODUCTION

Cloud Computing is using hardware and software as computing resources to provide service through internet. Cloud computing provides various service models as platform as a service (PaaS), software as a service (SaaS), Infrastructure as a service (Iaas), storage as a service (STaaS), security as a service (SECaaS), Data as a service (DaaS) & many more. Out of this Paas, SaaS and IaaS are most popular. Cloud computing has four models as Public cloud: though which the service is available to all public use. Private cloud:Through which service is available to private enterprise or organization. Community Cloud: It allows us to share infrastructure among various organizations through which we can achieve security, compliance and jurisdiction. This can be managed internally or by a third-party and hosted internally or externally. Hybrid cloud: it is a combination of public and private cloud. Cloud computing has many advantages as: we can easily upload and download the data stored in the cloud without worrying about security. We can access the data from anywhere, any time on demand. Cost is low or pay per usage.

Hardware and software resources are easily available without location independent. The major disadvantages of cloud computing is security.

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 [11]. In particular, 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. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those unaccessed data and might be too late to recover the data

 

loss or damage. 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 Moreover, the overhead of using cloud storage should be minimized as much as possible, such that a user does not need to perform too many operations to use the data (in additional to retrieving the data). In particular, users may not want to go through the complexity in verifying the data integrity. Besides, there may be more than one user accesses the same cloud storage, say in an enterprise setting. For easier management, it is desirable that cloud only entertains verification request from a single designated party.

To address these problems, our work utilizes the technique of public key based homomorphic linear authenticator (or HLA for short) [9], [13], [8], which enables TPA to perform the auditing without demanding the local copy of data and thus drastically reduces the communication and computation overhead as compared to the straightforward data auditing approaches. By integrating the HLA with random masking, our protocol guarantees that the TPA could not learn any knowledge about the data content stored in the cloud server during the efficient auditing process. The aggregation and algebraic properties of the authenticator further benefit our design for the batch auditing. Specifically, our contribution can be summarized as the following three aspects:

1) We motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol. Our scheme enables an external auditor to audit user 's cloud data without learning the data content.

2) To the best of our knowledge, our scheme is the first to support scalable and efficient privacy-preserving public storage auditing in Cloud. Specifically, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner.

3) We prove the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art.

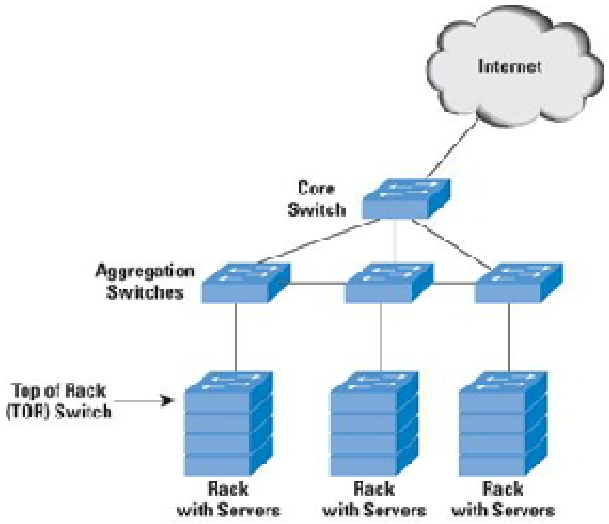


Fig: Cloud Data Storage Format

## II. EXISTING SYSTEM

The cloud data storage service contains 3 different entities as cloud user, Third party auditor & cloud server / cloud service provider. Cloud user is a person who stores large amount of data or files on a cloud server. Cloud server is a place where we are storing cloud data and that data will be managed by the cloud service provider. Third party auditors will do the auditing on users request for storage correctness and integrity of data. The proposed system specifies that user can access the data on a cloud as if the local one without worrying about the integrity of the data. Hence, TPA is used to check the integrity of data. It supports privacy preserving public auditing. It checks the integrity of the data, storage correctness. It also supports data dynamics & batch auditing. The major benefits of storing data on a cloud is the relief of burden for storage

 

management, universal data access with location independent & avoidance of capital expenditure on hardware, software & personal maintenance.

TPA checks the integrity of the data stored on a cloud but if the TPA itself leaks the user's data. Hence the new concept comes as auditing with zero knowledge privacy where TPA will audit the users' data without seeing the contents. It uses public key based homomorphic linear authentication (HLA) [1], [2] which allows TPA to perform auditing without requesting for user data. It reduces communication & computation overhead. In this, HLA with random masking protocol is used which does not allow TPA to learn data content.

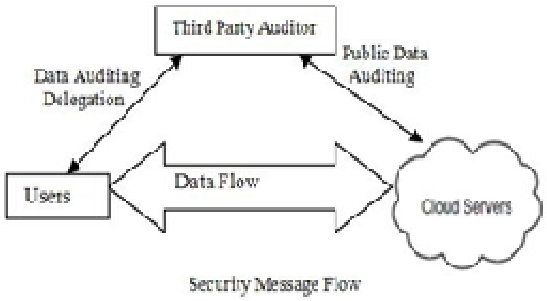


Fig 2: Architecture of Cloud Data storage service

In cloud, data is stored in a centralized form and managing this data and providing security is a difficult task. TPA can read the contents of data owner hence can modify. The reliability is increased as data is handled by TPA but data integrity is not achieved. It uses encryption technique to encrypt the contents of the file.

Design Goals

1) Public audit ability: Allows third party auditor to check data correctness without accessing local data.
2) Storage Correctness: The data stored on a cloud is as it. No data modification is done.
3) Privacy preserving: TPA can't read the users' data during the auditing phase.
4) Batch Auditing: Multiple users auditing request is handled simultaneously.
5) Light Weight: Less communication and computation.

## III. PROPOSED SCHEME

The data on the cloud has a minimum concern about sensitive information such as social security number, medical records, bank transaction and shipping manifests for hazardous material. We provide additional security such as watermark technique at specific time interval. These techniques enable single sign-on in the cloud and access control for sensitive data in both public and private clouds.

MAC-based Solution. There are two possible ways to make use of MAC to authenticate the data. A trivial way is just uploading the data blocks with their MACs to the server, and sends the corresponding secret key sk to the TPA. Later, the TPA can randomly retrieve blocks with their MACs and check the correctness via sk. Apart from the high (linear in the sampled data size) communication and computation complexities, the TPA requires the knowledge of the data blocks for verification.

## IV. PRIVACY-PRESERVING PUBLIC AUDITING SCHEME

Overview. To achieve privacy-preserving public auditing, we propose to uniquely integrate the homomorphic linear authenticator with random masking technique. In our protocol, the linear combination of sampled blocks in the server 's response is masked with randomness generated by the server. With random masking, the TPA no longer has all the necessary information to build up a correct group of linear equations and therefore cannot derive the user 's data content, no matter how many linear combinations of the same set of file blocks can be collected. On the other hand, the correctness validation of the block-

 

authenticator pairs can still be carried out in a new way which will be shown shortly, even with the presence of the randomness. Our design makes use of a public key based HLA, to equip the auditing protocol with public auditability. Specifically, we use the HLA proposed in [13], which is based on the short signature scheme proposed by Boneh, Lynn and Shacham (hereinafter referred as BLS signature).

## V. RELATED WORK

Ateniese et al. [9] are the first to consider public auditability in their "provable data possession" (PDP) model for ensuring possession of data files on untrusted storages. They utilize the RSA-based homomorphic lin- ear 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. Juels et al. [11] describe a "proof of retrievability" (PoR) model, where spot-checking and error-correcting codes are used to ensure both "possession" and "retrievability" of data files on remote archive service systems.

## VI. CONCLUSIONS

In this paper, we proposed watermarking technique for Privacy Preserving Public Auditing for cloud data storage security. Cloud computing security is a major issue that needs to be considered. Using TPA, We can verify the correctness and integrity of data stored on a cloud. It uses public key based homomorphic linear authentication (HLA) protocol with random masking to achieve privacy preserving data security. We achieved zero knowledge privacy through random masking technique. It supports batch auditing where TPA will handle multiple users request at the same time which reduces communication and computation overhead. It uses bilinear signature to achieve batch auditing. It also supports data dynamics. It uses Merkle Hash Tree (MHT) for it. We are introducing Privacy Preserving Public Auditing with watermark process for secure cloud Storage.

## REFERENCES

[1] C wang, Sherman S. M. Chow, Q. Wang, K Ren and W.Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage",IEEE Trasaction on Computers I, vol. 62, no. 2, pp.362-375 , February 2013.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public auditing for storage security in cloud computing," in Proc.of IEEE INFOCOM'10, March 2010.

[3] Wang Shao-hu, Chen Dan-we, Wang Zhi-weiP, Chang Su-qin, "Public auditing for ensuring cloud data storage security with zero knowledge Privacy" College of Computer, Nanjing University of Posts and Telecommunications, China, 2009

[4] KunalSuthar, Parmalik Kumar, Hitesh Gupta, "SMDS: secure Model for Cloud Data Storage", International Journal of Computer applications, vol56, No.3, October 2012

[5] AbhishekMohta, 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.

[6] Q. Wang, C. Wang,K.Ren, W. Lou and Jin Li "Enabling Public Audatability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transaction on Parallel and Distributed System, vol. 22, no. 5, pp. 847 –859,2011.

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

 