iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure third-party auditing for user data in cloud using HLA with random masking algorithm

Nisha R S[1], Poovaraghan R J[2]
[1] Final Year, M.Tech CSE, [2]Assistant Professor (OG), Department of CSE,
[1,2] SRM University, Chennai

Abstract — Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. The cloud facilitates on-demand self service, integrated availability of resources and high flexibility. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct resource management. Although cloud computing offers several advantages, it also brings in several threats and challenges; the integrity of data stored in the cloud being the major one. Thus permitting the public auditability of cloud data by an independent third party auditing (TPA) authority is essential to ensure the authenticity of the cloud data. Also, the use of TPA should not introduce new data management and privacy issues like revealing the data contents to the TPA. In this paper, the Homomorphic Linear Authenticator with random masking algorithm is used for ensuring data privacy during third party auditing process of cloud data.

Keywords — public auditing, Cloud server, Batch auditing, random masking, Verification

I. INTRODUCTION

Cloud services are extensively used because they can reduce the cost and complexity of owning and operating computers and networks. Since cloud users do not have to spend in setting up the hardware and software infrastructure, it paves the way for less initial investments, quick return on investment, provision for high customization, reduced operational expenses and a scalable infrastructure [1]. In addition, cloud providers who are specialized in a particular domain can provide advanced services that a single company might not be able to offer or build. Some other benefits to users include on demand scalability and efficiency. Even though cloud computing provides numerous advantages, its data also has its own share of vulnerabilities and threats. Since The Cloud Service Providers (CSP) are independent organizational entities, outsourcing of user data actually leads to loss of control over the data. Therefore the integrity and correctness of the user data suffers a major blow. Since the cloud providers often serve multiple customers simultaneously, some may have the tendency to behave disloyally towards their customers. They may behave like this for monetary benefits or to maintain their reputation. Hence, the user data stored in the cloud suffers from integrity and privacy issues [2].

Hence, a mechanism to maintain and ensure the consistent integrity of data in the cloud is necessary. Standard methods like downloading the cloud data into the user's machine are simply impractical due to the high communication costs, huge number of memory accesses and high storage requirements of the user. Moreover due to the large volume of data content in the cloud the complexity and associated overhead are extremely high in the above method. The cloud users also do not like to burden themselves with the authentication process of their data. Therefore, outsourcing the cloud data auditing process to an independent authority is an optimal solution for the users.

II. PROBLEM STATEMENT

The cloud data storage service comprises of three distinct entities, the cloud user (U), who has large amount of data files to be stored in the cloud; the cloud service provider (CSP) who provides data storage service and has considerable storage space and computation resources and the third party auditor (TPA) who has the technical skills that cloud users do not have and is trusted to verify the cloud service security on behalf of the user upon request.

This public auditability helps the users to verify their data in cloud storage. But, there arises a new issue of leakage of user data to the TPA during the auditing process which is unwarranted. Hence it is of utmost importance to protect the secrecy of user data from TPA during data audit [3]. The data in encrypted format also fails to solve this vulnerability due to the possible disclosure of encryption keys [4]. Therefore enabling third party auditing of user data independent of data encryption is the possible and optimal

©IJRASET 2015: All Rights are Reserved

solution to this problem.

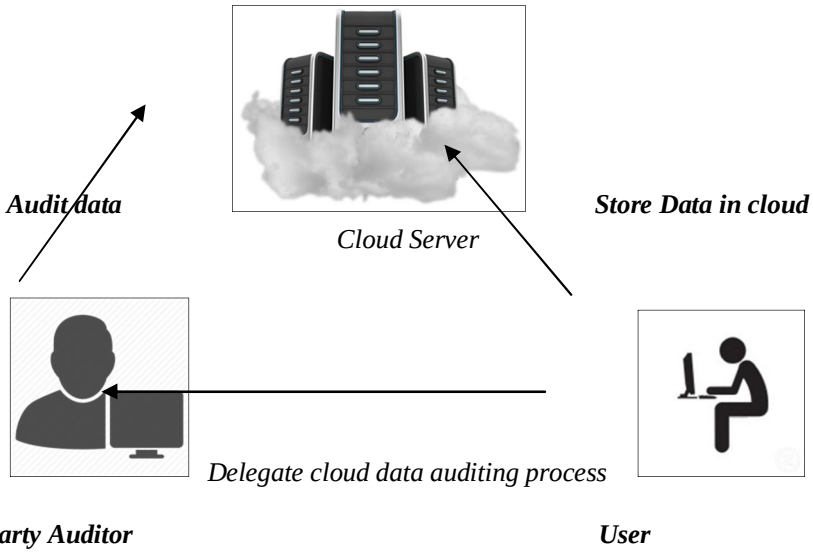


Fig. 1 Architecture of cloud storage and data auditing proces

To deal with this issue, this paper utilizes the technique of public key based Homomorphic linear authenticator with random masking. Using this approach the TPA can perform auditing of user data in cloud, without asking for a physical copy of the data. This ensures total protection for user data against leakage and also eliminates the unnecessary communication and computation costs associated with data transfers. This method also has inbuilt capabilities for processing auditing requests from multiple users concurrently. The above scheme can be summarized as follows:

A. Delegate the task of auditing user data in cloud to independent third party auditors.
B. Facilitate a third party auditor to audit user data without gaining knowledge about the data content.
C. Handle batch auditing requests simultaneously.
D. Improved performance in auditing process and high security for user data.

III. THE PROPOSED SCHEME

To achieve privacy preservation for user data during TPA audit the Homomorphic Linear Authenticator (HLA) with random masking technique is applied [5] [6]. To ensure privacy, all data in cloud are stored only in encrypted format and computations are performed only on the encrypted data. The Homomorphic encryption is a scheme that allows meaningful computations on encrypted data. The HLA scheme splits the original data into linear blocks before encrypting it and then creates one verification metadata for a group of encrypted data blocks. Since the encrypted data is ordered in linear format, the TPA can derive the user data if required. This violates the privacy and secrecy of user data. To overcome this, the linear blocks of data are masked with random data generated by the cloud server. With random masking, the TPA now does not possess sufficient information to reconstruct the original data.

Phases**:** The HLA with random masking includes two phases:

A. Compose phase

The cloud user generates the private and secret key pairs (p_k, s_k). The user then encrypts the data file D and generates a random authenticator for file D as (μ,t). Then the user uploads the file D and the verification data to the cloud server and removes the local.copy.

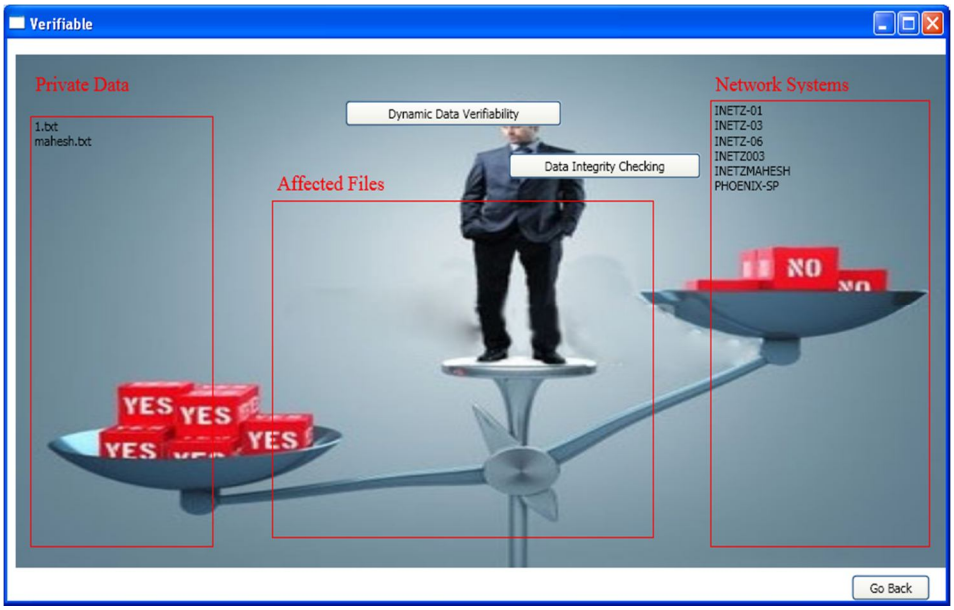
©IJRASET 2015: All Rights are Reserved

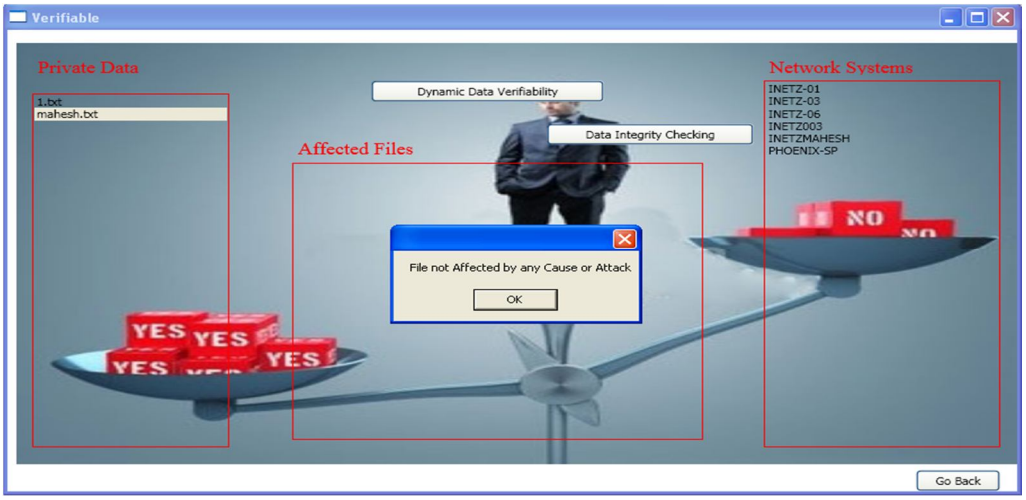
B. Inspect phase

The TPA first obtains the file tag *t* for the user file D from the cloud server and verifies its signature through the secret key s_k generated by the user during the compose phase. If the signature has changed, the TPA immediately issues a failure message and then quits. If the signature matches, then it issues a challenge message to the cloud server that specifies the block positions that are to be verified. The server in turn generates a response message of data storage accuracy and sents it to the TPA. For this the server chooses a random block of file D and recomputes the verification data which was sent by the owner of file D. The TPA then verifies the message from cloud server and generates the audit report.

The above process can be modified a little to accommodate the need for batch auditing, which arises when several users delegate the auditing task to the TPA simultaneously. If there are *n* verification requests from *n* users then naturally *n* auditing tasks need to be carried out by TPA. But using batch auditing technique the *n* auditing task requests can be aggregated into one which greatly simplifies the job of the TPA. It also reduces the computation cost and time of TPA.

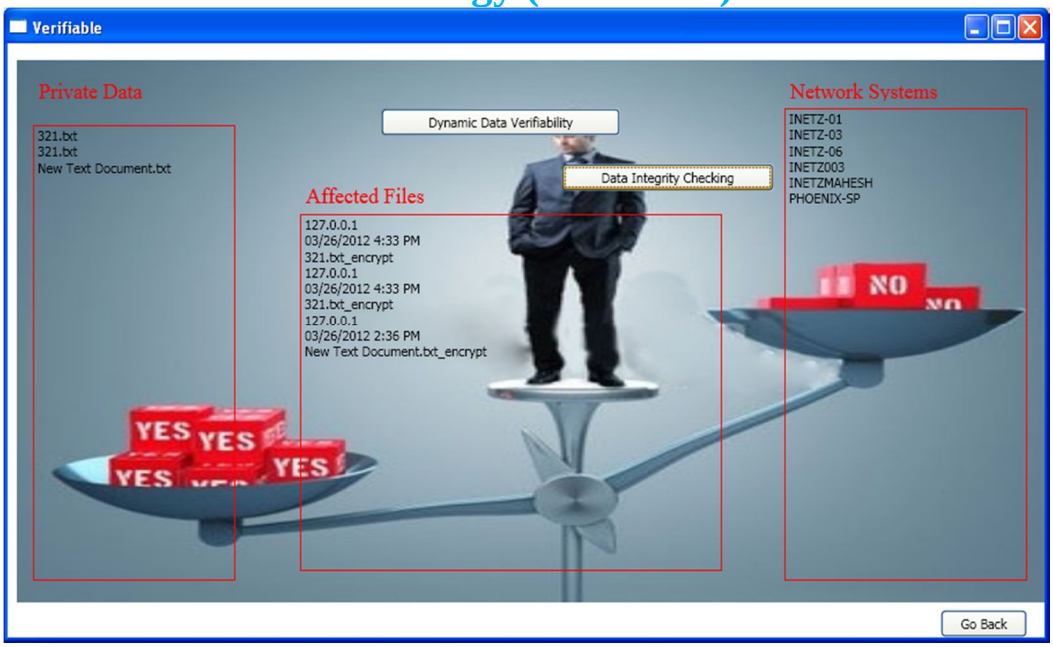
IV. IMPLEMENTATION





©IJRASET 2015: All Rights are Reserved

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



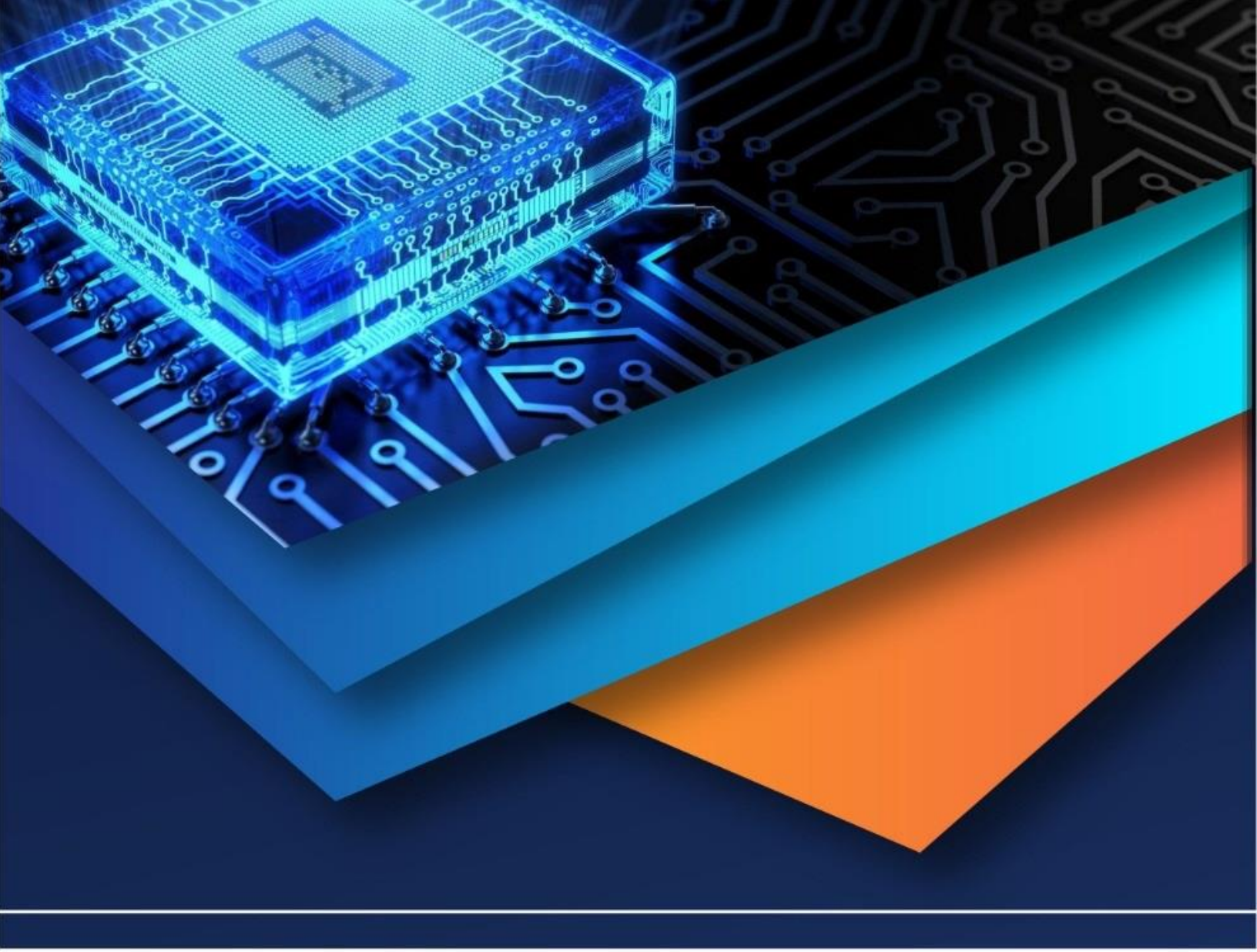
V. CONCLUSION

In this paper, a method for ensuring privacy for user data in cloud throughout the data auditing process is described. This method guarantees total security and privacy for user data thereby eliminating the fear of data leakage from the minds of cloud users. This can be expanded further to support batch auditing tasks when multiple users simultaneously request for public auditing by the TPA. The initial experiments were conducted in the private cloud, Eucalyptus to verify the performance of TPA and cloud servers. Analysis of the results shows high performance and security.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloudcomputing/ index.html, June 2009.
[2] 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 Distributed Systems, vol. 22, no. 5,pp. 847-859, May 2011.
[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEEINFOCOM, pp. 525-533, 2010.
[4] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.
[5] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. International Conf. on Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107,
Dec. 2008.
[6] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," J. Cryptology, vol. 17, no. 4, pp. 297-319, 2004.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)