International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

Cloud Data Auditing With a Focus on Privacy and Security

Anirudh Karthik[1], Aruna Reddy H[2]
Assistant Professor, Selection Grade
Department of Computer Science,
Vemana Institute of Technology,
Koramangala, Bangalore, Karnataka, India

Abstract: ***The storage of large amounts of data in a cloud poses risks such as loss of data integrity and privacy as data can be affected by movement of data from one place to another, by malicious users, or by dishonest Cloud Service Providers (CSPs). Third Party Auditors (TPAs) perform verification of remote data stored in cloud storages with the help of cryptography. TPAs are used for public auditing of clouds. Since most auditing schemes are not inclusive of protection of cloud data from malicious TPAs, this research's primary focus is on cryptographic algorithms for cloud data auditing and the integrity and privacy issues that these algorithms face.***

Keywords: Data Integrity, Verification, Public Auditing, Cryptographic Algorithms

I. INTRODUCTION

Major issues faced when a large amount of data is moved from one storage to another are losses of data integrity and confidentiality of private data, as the privacy of the data is compromised. Third Party Auditors (TPAs) perform public auditing to the data provided to them by the cloud owners. The verification is a major step in the data auditing process and is carried out by employing cryptographic techniques. The data in question is audited and verified after its transit from one cloud storage to another. Although TPAs promise a certain level of accuracy in data auditing and verification, the data in question is not properly scrutinized, which results in the data still being vulnerable to issues such as loss of integrity and confidentiality. This research provides an overall picture on the comprehensive methodologies that exist to overcome compromises on data integrity and focuses on preserving the data privacy, after it has been through a transit through storages.

II. DESIGN

Getting into the intricacies of the cloud data auditing process, this research lays emphasis mainly on the verification part of the entire process. Bearing that in mind, TPAs perform the auditing on cloud data only after the cloud owner has given full discretion. A set of cryptographic keys are exchanged between the TPA and cloud owner, following which the data to be audited is sent to the TPA, as a secure exchange between the TPA and cloud owner is established since the cryptographic keys are exchanged. Upon receiving the data to be audited from the cloud owner, the TPA makes use of system resources at its disposal to run the combination of various cryptographic algorithms, (to be discussed in later sections) to verify the data, during the auditing process.The TPAs verify the data given to them by the cloud owner, by expending the system resources available to them. The secure exchange of data between the could owner and TPA is facilitated primarily by the exchange of encryption keys, such as private and public keys. It must be noted that the length of the public and private keys is directly proportional to the complication in decryption of the keys in question, by any external or internal malicious entity. That is, longer the key, harder it is for external/internal malicious entities to decrypt. This ensures that the data's safety is not compromised.

III. ALGORITHMS USED FOR CRYPTOGRAPHIC VERIFICATION

1) MESSAGE AUTHENTICATION CODES
2) HOMOMORPHIC LINEAR AUTHENTICATORS
3) BONEH–LYNN–SHACHAM (BLS)-BASED HOMOMORPHISM METHODS

The cryptographic operations specific to auditing include

- *Key generators*
- *Tag generators*
- *Challenge generators*
- *Proof verifiers.*

A. ELABORATION OF THE ALGORITHMS USED FOR CRYPTOGRAPHIC VERIFICATION IS AS FOLLOWS:

1) Message Authentication Codes (MAC): In cryptography, a message authentication code (MAC) is a short piece of information used to authenticate a message or data, in other words, to confirm that the data came from the stated sender.

2) MAC codes are generated by hash functions, which contain a hash value and the message to be authenticated. The data is sent from the cloud owner to the TPA, along with the MAC codes. These codes are used to validate the sender's identity, and to provide assurance of the message's origin.MAC can be applied to cloud data auditing as well. MAC is mainly used when the end user wants to verify the data without much intervention from the TPA, which would otherwise perform public auditing of the data provided to it. This approach of the end user data verification can be carried out after the TPA has performed public auditing. This will result in a twostep verification process, improving the preservation of data integrity.

3) Homomorphic Authentication (HA): Homomorphic Authentication (HA) provides a unique feature that allows the chaining together of different services without exposing the data to each of those services. These services being the data verification services which are used to verify the data provided by the cloud owner. Homomorphic Authentication (HA) allows for blockless verification of data. In blockless verification, the data is remotely accessed from a server and verified. This method of data verification does not use much resources as the data need not be retrieved from the server in question and reuploaded thereby reducing overhead as well. Homomorphic Authentication allows the TPA to certify the result of the complex computation performed on the authenticated datasets with a data tag. For every block of data to be verified, corresponding tags are generated, uniquely numbered, and saved. The TPA can verify the data by simply adding a linear combination of tag values.

4) Boneh–Lynn–Shacham (BLS)-based homomorphic methods In cryptography, the Boneh–Lynn Shacham (BLS) signature scheme allows a user to verify that a signer is authentic. The scheme uses a bilinear pairing for verification, and signatures are elements of an elliptic curve group. The constituent blocks of data in a cloud storage can be encrypted before transit using the (BLS)-based homomorphic methods. BLS is further extended to support dynamic data, and public auditing of data, as performed by TPAs. Every block of data/ file has an index in the (BLS)-based homomorphic method, and the indices must be updated every time the data is dynamically updated.The support provided by the (BLS)-based homomorphic method to encrypt dynamic data is beneficial when being applied to schemes such as big data auditing, which is the need of the hour in today's exponentially increasing rate of data generation.

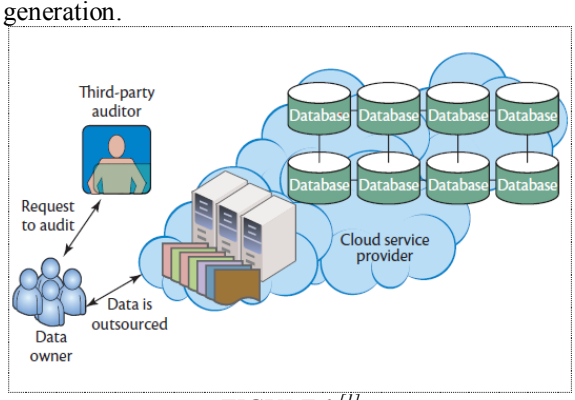

FIGURE 1 [1]

INTERACTION BETWEEN TPA AND DATA OWNER [1]

1.THE FIGURE ABOVE SHOWS THE INTERACTION THAT TAKES BETWEEN A TPA AND THE DATA OWNER.[1]

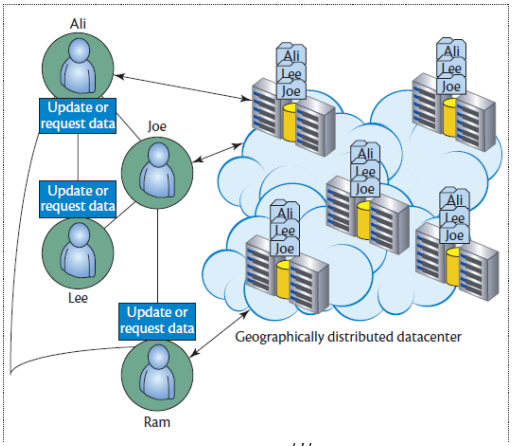

Figure 2[1]

STORING USER'S DATA ACROSS MULTIPLE DATACENTERS [1]

2. The figure (Figure 2)above depictsthe storage ofusers' data across multiple datacenters. These datacenters provide high availability of data storage services and an improved cloud user capability across broader geographical areas.[1]

B. SCHEMES USED IN CLOUD DATA AUDITING:

- *Schemes such as Proof Of Retrievability (POR) and Provable Data Possession (PDP) are used to enable the cloud storage system or the cloud owner to produce proof of a client's data without retrieving data from the system.*

- *We must note that the schemes, namely POR and PDP can be used by the cloud owner to verify the data after it has been publicly audited, thereby resulting in a two-phase verification of the data, improving the data's integrity, and reducing the privacy and security risks.*
- *The TPA receives an authentication tag from the*
- *The main purpose of these schemes, namely POR and PDP are to facilitate End User Authentication, apart from the verification performed by the concerned TPA. These schemes prove to be useful if the TPA in question is malicious, thereby enabling the cloud owner to maintain the data integrity and privacy of the data it owns.*

C. DRAWBACKS OF SCHEMES USED IN CLOUD DATA AUDITING:

- *POR methods are not entirely suitable for third-party auditing schemes if the data in question to be verified is dynamic data.*
- *Significant amount of overhead is generated with the use of end user verifiable schemes, as every block of data has to be encrypted.*

D. RESULTS

The results obtained after analyzing the transaction between cloud server and auditor are presented graphically, below:

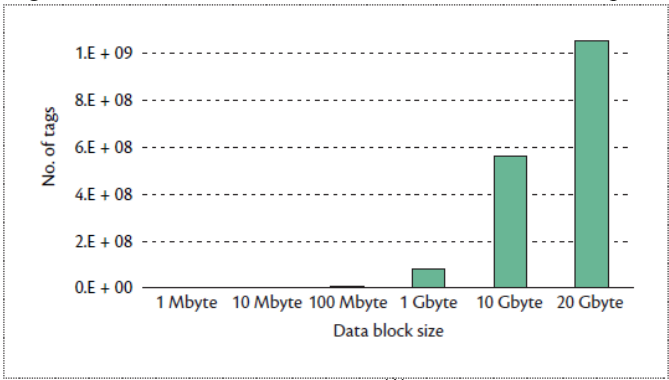

FIGURE 3 [1]

TRANSACTION BETWEEN CLOUD SERVER AND AUDITOR [1]

The graph (Figure 3) above depicts the transaction between cloud server and auditor: generation of security tags between TPA and cloud storage during auditing. [1] It has to be noted that the number of tags increase proportionally, but exponentially with the increase in the data block size.

E. CONCLUSION:

In this research, auditing schemes such as MAC-based data verification, Homomorphic Authentication, and BLS-based homomorphic methods have been proposed. We can therefore conclude that the auditing process consists of an exchange of cryptographic keys between the cloud owner and a TPA, following which the TPA will verify the data given to it, as a part of the auditing process. However, end user authentication is facilitated as well, with schemes such as PDP (Provable Data Possession) and POR (Proof Of Retrievability).

ACKNOWLEDGMENT

This research was supported by Vemana Institute of Technology. We thank our colleagues from Vemana Institute of Technology who provided insight and expertise that greatly assisted this research.

REFERENCES

[1]. .ManjurKolhar, Mosleh M. Abu-Alhaj, Mosleh M. Abu-Alhaj Cloud Data Auditing Techniques With A Focus on Privacy and Security
[2]. NahilaZaibaRuksar, K. Rajasekhar Reddy ORUTA: Privacy-Preserving Public Auditing For Shared Data in the Cloud
[3]. Sultan Aldossary, William Allen Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions
[4]. Vitthal Sadashiv Gutte, Prof.Priya Deshpande A Survey on Privacy Preserving Technique to Secure Cloud
[5]. TejashreePaigude , Prof. T. A. Chavan A survey on Privacy Preserving Public Auditing for Data Storage Security
[6]. Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring,Lea Kissner, Zachary Peterson, Dawn Song Provable Data Possession at Untrusted Stores