A STUDY ON DECENTRALIZED LIGHTWEIGHT SECURE AUDITING SCHEMES FOR DYNAMIC OUTSOURCING DATA INTEGRITY IN THE MULTI CLOUD STORAGE ENVIRONMENT

A.Shalini *

ABSTRACT

Multi cloud storage environment is an emerging paradigm which provides storage services to various categories of users to out source their data. Due to the multi-tenancy nature of data storage in the cloud, it leads to multiple security concerns like data breaches and unauthorized data access. It is of critical importance to the user of the cloud to outsource their data to cloud. In order to mitigate those challenges and enhance the data integrity in the multi-tenant cloud environment, many secure auditing schemes have been designed and implemented by various researchers. Hence, review of the decentralized lightweight secure auditing scheme defined by various researchers to ensure the data integrity on their outsourced data has been carried out in this article. Initially those models have been incorporated by third partyauditors (TPA) to accomplish the auditing task in the cloud with a list of secure policies for verifications and certification of the cloud storage. Next, decentralized cloud auditing scheme using block chain with group of verifiers has been incorporated which insists single designated third party auditors to verify the integrity of the data. Finally lattice based data auditing scheme with prior knowledge is implemented without delegating the auditing to the third party auditor for data integrity verification. On experimental analysis of those models using synthesis data in the cloudplatform, it leverages more challenges with respect to computation overhead (response time) and managing the data integrity verification among the streaming outsourcing data at runtime. Further those models are less capable to block based audit due to improper data auditing structures. To manage those challenges, decentralized lightweight data integrity verifying model for secure auditing of the streaming of outsourced data can be designed and implemented using Auto encoder based deep learning model as research methodology. It is efficient in verifying the data integrity and also it is capable in eliminating data duplication.

Keywords: Deep learning, Cloud Environment, Data Integrity, Data Outsourcing, Cloud Security, Data Duplication

I. INTRODUCTION

Multi Cloud Storage is a fast developing data paradigm which has large storage and processing capabilities with high scalability and reliability to various categories of users to outsource their big data from their local storages [1]. Despite convenience of cloud computing, outsourced data may lead to many security concerns like data breaches, unauthorized data access and multiple types of malicious attacks due to multi-tenancy models. As a result, itbecomes critical to the cloud user to outsource their data to cloud service providers. In order to ensure the data integrity to cloud user to their outsourced data, secure data auditing scheme has to be applied to prevent and isolate the security issues [2].

Traditionally many secure auditing schemes have been designed and implemented to ensure the data integrity in the cloud server, which has been analyzed in this article. Especially those auditing schemes were categorized as private auditing and public auditing. In private auditing, the user has to verify the integrity on employing the data auditor to check data consistency against various security policies while in public auditing scheme, public verifier with public key is enabled to verify the auditing process [3]. Initially Third Party Auditor (TPA) is employed for auditing task as they posses expertise and capability to execute the verification and certification [4] with list of secure policies [5].

Next, decentralized cloud auditing scheme using block chain with group of verifiers has been incorporated in spite of single designated third party auditors to verify the integrity of

Department of Computer Science and Engineering
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
shaliniasokan04@gmail.com
* Corresponding Author

the data as it works on provide trust based consensus and tamper proof and traceability[6] to eliminate the malicious auditors. Block chain is a decentralized protocol containing distributed database which adapts to decentralized consensus mechanism such as proof of work, proof of stake, fault tolerance and delegated proof of stake. It generates the challenge message to verify the originality of verifier [7].

Finally hash tree based data auditing scheme with prior knowledge is implemented without delegating the auditing to the third party auditor for data integrity verification. It performs verification on block level efficiently on establishing the dynamic index table [8]. It is highly efficient in handling the replay attack and considered as a lightweight mechanism [9]. On experimental analysis of those models using synthesis data in the cloud platform , it leverages more challenges with respect to computation overhead (response time) and managing the data integrity verification among the streaming outsourcing data at runtime.

Remaining part of the article is organized into following sections: section 2 is a review of literature in establishing secure auditing scheme to the multi cloud storage system on highlighting its security analysis and performance analysis in the tabular form. In section 3, problem statement of the analysis of the literature is mentioned along with the objective to eliminate it effectively and efficiently. Section 4 outlines the research methodology to handle the secure auditing scheme on streaming of the outsourcing data to the cloud storage and deduplication approach to eliminate the duplicate in the storage. Finally section 5 concludes the article.

II. REVIEW OF LITERATURES

In this section, traditional secure public data auditing scheme is analyzed to verify and ensure the data integrity to outsourced data in the cloud server. They can also be considered as provable data possession which verifies the data and its structure without retrieving it. Security analysis and performance analysis of those schemes are categorized into three segments as centralized secure data auditing, decentralized secure data auditing and automatic secure data auditing scheme is as follows

2.1. Analysis of centralized secure data auditing scheme

In this part, central authority considered as Third Party Auditor (TPA) were employed for auditing task as they possess expertise and capability to execute the verification and certification with list of secure policies. It provides accountability and transparency of the cloud service provider to build trust among the user in the multitenant cloud environment. Further analysis is carried out to ensure error localization with data correctness. This is done as follows:

Design architecture to ensure the integrity of data stored in the cloud, using a private key for secure auditing of outsourced data through a third-party auditor. This architecture employs a new signature scheme that supports block-less verifiability and is compatible with linear coding and error correction processes [4].

The architecture eliminates uncontrolled malicious modifications by establishing identity traceability for data through a secure data auditing process. Additionally, it preserves the privacy of the data user. This functionality is achieved through the generation of authenticators using a blind signature technique. [3].

The architecture is considered an economical storage auditing solution. It uses an authenticator called Homomorphism Invisible Authenticator (HIA), which protects the privacy of the authenticator and supports block-less verification. Neither the cloud service provider nor the public verifier has access to the real authenticators (signatures) for the cloud data. [6].

The system enables data owners and public verifiers to efficiently audit the integrity of cloud data without needing to retrieve the entire dataset from the cloud server, using ring signatures. Ring signatures are employed to compute the verification metadata required to audit the correctness of shared data. The identity of the signer for each block of shared data is kept private from public verifiers, and the system is capable of performing multiple auditing tasks simultaneously. [7].

2.2. Analysis of Decentralized Secure Data Auditing Scheme

In this part, decentralized secure data auditing scheme using block chain along with the group of verifiers has been incorporated in spite of single designated third party auditors to verify the integrity of the data as it works on providing trust based consensus to eliminate the malicious auditor .Block chain is a decentralized protocol containing distributed database which adapts to decentralized consensus mechanism such as proof of work, proof of stake, fault tolerance and delegated proof of stake. Further analysis is carried out to ensure tamper proof, traceability with data correctness as follows

The system provides a decentralized self-auditing scheme to verify the integrity of outsourced data through interactions with cloud servers. It effectively identifies misbehaving auditors with low computational costs and resists denial-of-service attacks initiated by malicious auditors. These attacks attempt to undermine the audit process performed by genuine auditors [8].

The system offers an efficient data integrity verification scheme for multi-cloud storage services by utilizing blockchain technology. Local verification can trace the source of any damage to a specific cloud service provider (CSP), enhancing security and reliability. The data verification process is executed directly on the blockchain for public verification, providing data integrity services without relying on any third-party auditors [9].

The system offers a stateless cloud auditing scheme for dynamic group data with privacy preservation for users, utilizing a random masking technique. Additionally, it employs Shamir's Secret Sharing to split the re-signing process into multiple components, which helps resist collusion attacks during user revocation. The system generates a challenge message to verify the authenticity of the verifier [10].

2.3. Analysis of Automatic Secure Data Auditing Scheme

In this part, automatic secure data auditing scheme using hash tree based data auditing scheme with prior knowledge is implemented without delegating the auditing to the third party auditor for data integrity verification and utilizing the block chain for third party auditor verification. It provides verification on block level efficiently in establishing the dynamic index table. It is highly efficient in handling the replay attack and considered as lightweight mechanism.

The architecture employs a Ternary Hash Tree for block ordering and storage verification to ensure data integrity and availability in the cloud based on prior knowledge. It also supports error localization, helping to verify data correctness. [11].

The system is a public auditing scheme for secure cloud storage based on a dynamic hash table (DHT), a novel two-dimensional data structure. It supports privacy preservation by integrating automated authenticators. Additionally, it performs batch auditing using the aggregate BLS (Boneh-Lynn-Shacham) signature technique [12].

The architecture utilizes a quad Merkle hash tree for auditing data. Automated verification of auditing activities through a deployed smart learning model eliminates the costs associated with data integrity verification. It is designed for lightweight operation with a data structure suitable for batch auditing. The system is secure against multiple types of attacks. [13].

2.4. Tabular view of the secure auditing scheme

In this part, security analysis of the various secure auditing schemes is carried out in the tabular form. It provides analysis of the work with advantages and disadvantages of the work on various performance factors.

Table 1: Secure Analysis of Secure Auditing Scheme

Audit Scheme Type	Technique	Advantage	Disadvantage
Centralized with Third Part Auditor	Enabling public auditing for shared data using Blind signature technique	It increases identity traceability and privacy preserving of data and user information	Authenticator generation to auditor is challenging on basis of computation cost and leads to duplication attack

Audit Scheme Type	Technique	Advantage	Disadvantage
Centralized with Third Part Auditor	Oruta: Privacy preserving public auditing Ring signatures	It performs multiple auditing tasks simultaneously	It leads to malicious intruding with fake certificate through third party auditors
De centralized without Third Part Auditor	A Block chain-Based Efficient Data Integrity Verification Scheme using POS consensus	It is efficient in local verification	It consumer more commu nication cost and Consensus generation time
De centralized without Third Part Auditor	Stateless Cloud Auditing Scheme Shamir Secret Sharing	It provides random masking to data and resist collusion attacks	It increase the computation time and Consensus generation time
Automated without Third Part Auditor	Data Integrity Audit Scheme Based on Quad Merkle Hash Tree	Smart learning model for auditing activities and considered as light weight	It utilizes the more knowledge and identify associations

III. PROBLEM STATEMENT

The implementation of the secure audit schemes with security policies and strategies in cloud storage system leads to several challenges due to its dynamics in data storage and processing it. Further it is exposed to multiple kinds of new data attacks [14]. Primary consideration to be incorporate on the automated security policies is listed below

- Configuration and log of the cloud has to be verified as it leads to propagation of the denial of service attack.
- It is mandatory to determine data duplication to ensure the data integrity of the outsourced data
- It is mandatory to employ the bidirectional verification to support dynamic data operation of the user in the cloud.

IV. RESEARCH OBJECTIVE

Objective of the work is defined to manage those challenges mentioned in the problem statement as follows

- Decentralized lightweight data integrity verifying model for secure auditing of the streaming of outsourced data using deep learning model
- Automated deduplication technique to eliminate the data duplication in the cloud.
- Dynamic operation on the cloud data has to be managed effectively.

V. OUTLINE OF THE PROPOSED METHODOLOGY

Decentralized lightweight data integrity verifying model for secure auditing of the streaming of outsourced data is designed and modeled using deep belief network which is capable of securing the data on various layers of the neural network and construct the feature map to compute the duplicate of the data to enhance the data integrity and identity traceability of the attacker to attain the user revocation. The proposed model contains the hidden layer for processing the dynamic cloud data [15] on the operation of insert, delete and update operation with less computation cost and time. Architecture plan of the proposed model is mentioned in the figure 1.

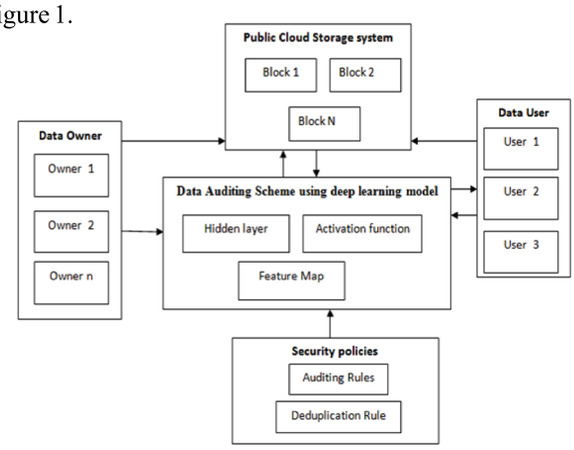

Figure 1: Architecture Plan of the proposed model

VI. CONCLUSION

In this article, detailed study of the various secure auditing schemes utilizing the third party auditor, block chain and automated auditing method with prior knowledge have been analyzed on the basis of security and performance. In the model evaluation in the cloudplatform, it leverages many challenges on data integrity verification among the outsourcing data at runtime. In order to manage those challenges, a new decentralized lightweight data integrity verifying model using deep belief network is projected as research methodology to increase the traceability and eliminate the duplication of the outsourced data.

REFERENCES

[1] S. Majumdar, T. Madi, Y. Wang, Y. Jarraya, M. Pourzandi, L. Wang, and M. Debbabi, “Security compliance auditing of identity and access management in the cloud: Application to OpenStack,” in IEEE CloudCom, 2015.

[2] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 767–778, Apr. 2017.

[3] G.Yang, Wenting Shen, Qianqian Su, Zhang fu"Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability" Journal of Systems and Software, Elsevier, Vol.113, pp: 130-139, 2016

[4] Wenting Shen, Jing Qnr , jia Yu, Rong Hao,JiankunHu,JixinMa"Data Integrity Auditing without Private Key Storage for Secure Cloud Storage"IEEE transaction on Cloud Computing, Vol.9, Issue .4, pp:1408-1421, 2019

[5] W. Shen, G. Yang, J. Yu, H. Zhang, F. Kong, and R. Hao, “Remote data possession checking with privacypreserving authenticators for cloud storage,” Future Generation Computer Systems, vol. 76, no. Supplement C, pp. 136 – 145, 2017.

[6] B. Wang, B. Li, and H. Li, “Oruta: Privacy-preserving public auditing for shared data in the cloud,” in 2012 IEEE Fifth International Conference on Cloud Computing, June 2012, pp. 295–302.

[7] Yuan Su, Yanping Li, Bo Yang, Yong Ding "Decentralized Self-Auditing Scheme With Errors Localization for Multi-Cloud Storage" IEEE transaction on dependable and secure computing , Vol.19, Issue .4, 2022

[8] Xiaodong yang, Meiding Wang, Xiuxiu Wang, Guila Chen, Caifen Wang" Stateless Cloud Auditing Scheme for Non-Manager Dynamic Group Data With Privacy Preservation " IEEE access , 2020

[9] Yushu Zhang, Jiajia Jiang, Xuewen Dong, Liangmin Wang, Yong Xiang "BeDCV: Blockchain-Enabled Decentralized Consistency Verification for Cross-Chain Calculation" IEEE transaction on cloud computing , Vol.11, 2023

[10] Yiran Zhang,Huizheng Geng, Li Su, Li Lu "A Blockchain-Based Efficient Data Integrity Verification Scheme in Multi-Cloud Storage" IEEE access, Vol. 10, 2022

[11] M. Thangavel; P. Varalakshmi, Enabling Ternary Hash Tree Based Integrity Verification for Secure Cloud Data Storage" IEEE transaction on Knowledge and Data Engineering , vol.32, 2020

[12] Hui Tian; Yuxiang Chen; Chin-Chen Chang; Hong Jiang; Yongfeng Huang; Yonghong Chen; Jin Liu" Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage" IEEE Transactions on Services Computing (Volume: 10, Issue: 5,2017

[13] Zhenpeng Liu; Lele Ren; Yongjiang Feng; Shuo Wang; Jianhang Wei" Data Integrity Audit Scheme Based on Quad Merkle Tree" IEEE access, vol.11, 2023

[14] Q. Zhou, C. Tian, H. Zhang, J. Yu, and F. Li, "How to securely outsource the extended uclidean algorithm for large-scale polynomials over finite fields," Inf. Sci., vol. 512, pp. 641–660, Feb. 2020,

[15] Guohua Tian; Yunhan Hu; Jianghong Wei; Zheli Liu; Xinyi Huang; Xiaofeng Chen; Willy usilo" Blockchain-Based Secure Deduplication and Shared Auditing in Decentralized Storage" IEEE transaction on dependable computing , vol.19, 2022