IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105252 |

Privacy-Preserving Public Auditing For Local Storage Based On Blockchain

Vaishnavi Shete[1], Bhushan Munjal[2], Amruta Daspute[3], Prof.Devray R. N.[4]

[1.2.3]Student, Department of Computer Engineering, Vishwabharati Academy's College of Engineering , Ahmednagar, India

[4]Professor, Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar, India

ABSTRACT*:* Auditing is the inspection of the processes and work done during a period of time whereas compliance is the process of complying to the rules. In Service management space various organizations provide and use various services in the form of transactions and are dependent on each other. Cloud storage services offer flexible, convenient solutions for business and personal users to store data. Traditionally, Third Party Auditors (TPAs) are introduced to ensure data integrity for public auditing. However, TPAs may also be untrusted for forging the auditing results or colluding with cloud storage servers to deceive users. An organization may not use only one service to provide its services to the client; it may use multiple services like database, storage, processing, etc. Due to this involvement of multiple parties in the business, it is very tedious to manage these licenses and also more difficult to audit this system. Each organization have stored information at their own data centres, hence it is very hard to guarantee the trust between these organizations. Our security analysis indicates that BPAO achieves soundness and robustness. The experimental results show that BPAO is computationally efficient for cloud storage users. To address this issue we propose a blockchain-based solution to ensure transparency and security in the transactions between these organizations.

KEYWORDS*:* Audit, Blockchain, Node, Angular, NPM, Firebase, Log, Auditor

I. INTRODUCTION

The security of most auditing schemes is based on the assumption that the TPA is honest and trustworthy however, in practice, the TPA does not always act as expected. What is worse, the TPA has total control to fabricate audit results without disincentive. Such undetected mistakes can be avoided by publishing all information related to auditing, although this is hard to realize in the TPA-based framework.In this Paper, we offer a promising solution to the above problems.

We propose a blockchain-based auditing framework in which the audit is performed by multiple auditors (who are selected randomly from local users) with the help of a smart contract. The proposed framework has the following dominance. a) Fault-tolerance: the audit is not affected even when a portion of auditors malfunction or are controlled by attackers. b) Transparency: both auditing rules and auditing processes are stored on the blockchain and so are publicly accessible.

Smart contracts have been used for many intentions, such as enhancing the security of public-key infrastructure and preserving data privacy during data usage. Audient uses smart contracts to implement audit-related procedures. Both local users and the local provider call the functions in the smart contract to take part in audits. Performing critical functions in a smart contract has many benefits. First, every system participant has access to the procedures related to the audit. Furthermore, functions are executed by numerous blockchain miners, which ensures reliable execution results. Finally, function inputs and outputs are recorded on the blockchain; when a dispute arises between the local user and the local provider, the audit records on the blockchain are evidence for arbitration.

PROBLEM DEFINITION AND OBJECTIVE

Current auditing schemes may encounter two kinds of problems. a) Single-point failures. The audit is suspended or erroneous once physical failures or human errors occur on the TPA's servers. Such singlepoint failures are inherent and unresolvable in the TPA-based framework; a suggested solution is to adopt a decentralized auditing framework. b) Undetected mistakes. Unnoticeable mistakes may happen because the audit is conducted privately by the TPA, and most information is not available to cloud users and the cloud provider.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105252 |

The aim of this research was to go deeper including the particularities of the Blockchain-based implementation for a general-purpose solution, as well as usability aspects. In this sense, a Blockchain monitoring tool is recommended that provides a graphical and web-based interface to access the information recorded in the Blockchain in a user-friendly way, with the Blockchain being fully transparent to users.

II. RELATED WORK

Remote Data Auditing

Remote Data Auditing (RDA) was first proposed in PDP and PoR, since researchers realized that cloud storage was not always reliable, and integrity verification was necessary on behalf of cloud users. The main idea of RDA is to upload data authenticators with data blocks to the cloud, so integrity verification can be performed without downloading the remote data. As a high-level summary, there are two auditing modes. In private verification, data owners are responsible for the audit. However, the computational cost is a serious problem for resource-limited data owners. Moreover, malicious data owners are able to pretend that audits do not succeed (and claim for compensation), which harms the cloud provider. Improving upon this, public verification allows cloud users to delegate audit tasks to the TPA

Blockchain and smart contract

The blockchain is a decentralized ledger originally proposed for Bitcoin, in which numerous ledger copies are kept consistent via a consensus mechanism. The blockchain is characterized by tamper-proofing and Byzantine fault tolerance; thus, it is suitable for scenarios where cooperators mistrust each other but need to share information. In recent years the blockchain has been applied to many fields, such as data integrity, data provenance, and data management.

Cryptographic Sortition

Cryptographic sortition is proposed in Algorand, the proof-of-stake cryptocurrency, to select a random subset of users with wealthier individuals having a higher probability of being chosen. Sortition is executed by each user privately and without any interaction. Theoretically, there is a fixed number of users being selected in each sortition round. Also, sortition results are tough to predict and control. The auditor election in Audinet is based on cryptographic sortition. In the auditor election, we define the user's wealth as the number of files uploaded to the cloud.

III. PROPOSED METHODOLOGY

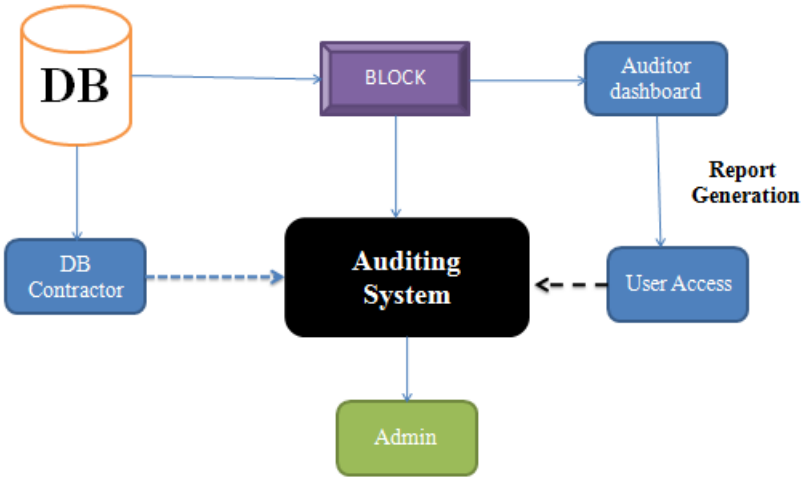

Fig 1. Proposed System Architecture

Figure 1 shows the Proposed System Architecture diagram of our decentralized and privacy-preserving public auditing scheme based on blockchain. In the scheme, there are four different entities, i.e., key generation center (KGC), cloud server (CS), data user (U) and a third-party auditor (TPA).

- Key generation center is an authority, whose task is to generate system parameters and partial private key for users according to their identity.
- Cloud server provides cloud storage services. It not only has enough storage space, but also possesses amount of computing power.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105252 |

- Data user is the data owner, who outsources data to the cloud and delegates the TPA to check the data integrity. He checks the auditor's behavior via the blockchain.
- *Third-party auditor* detects the data integrity periodically and checks if there is any data corruption. TPA uploads the verification results to the blockchain after verifying the proof information from the CS.

Blockchain

A blockchain-based digital auditing can protect data, streamline processes, and reduce fraud, waste, and abuse while simultaneously increasing trust and accountability. On a blockchain-based government model, individuals, businesses, and governments share resources over a distributed ledger secured using cryptography. This structure eliminates a single point of failure and inherently protects sensitive citizen and government data.
A blockchain-based Auditing has the potential to solve legacy pain points and enable the following advantages:

- Secure storage of government, citizen, and business data
- Reduction of labor-intensive processes
- Reduction of excessive costs associated with managing accountability
- Reduced potential for corruption and abuse
- Increased trust in government and online civil systems

The distributed ledger format can be leveraged to support an array of government and public sector applications, including digital currency/payments, land registration, identity management, supply chain traceability, health care, corporate registration, taxation, voting (elections and proxy), and legal entities management.

MD5 Hash Key Generation

An MD5 hash is created by taking a string of an any length and encoding it into a 128-bit fingerprint. Encoding the same string using the MD5 algorithm will always result in the same 128-bit hash output. MD5 hashes are commonly used with smaller strings when storing passwords, credit card numbers or other sensitive data in databases such as the popular MySQL. This tool provides a quick and easy way to encode an MD5 hash from a simple string of up to 256 characters in length.
Proposed System Flow

- User should login to our system
- User perform the file operation upload/download/delete
- Every file upload block is created
- On every file operation system create a log
- Auditor uses that log file for check and validate it

IV. WORKING SCREENSHOT

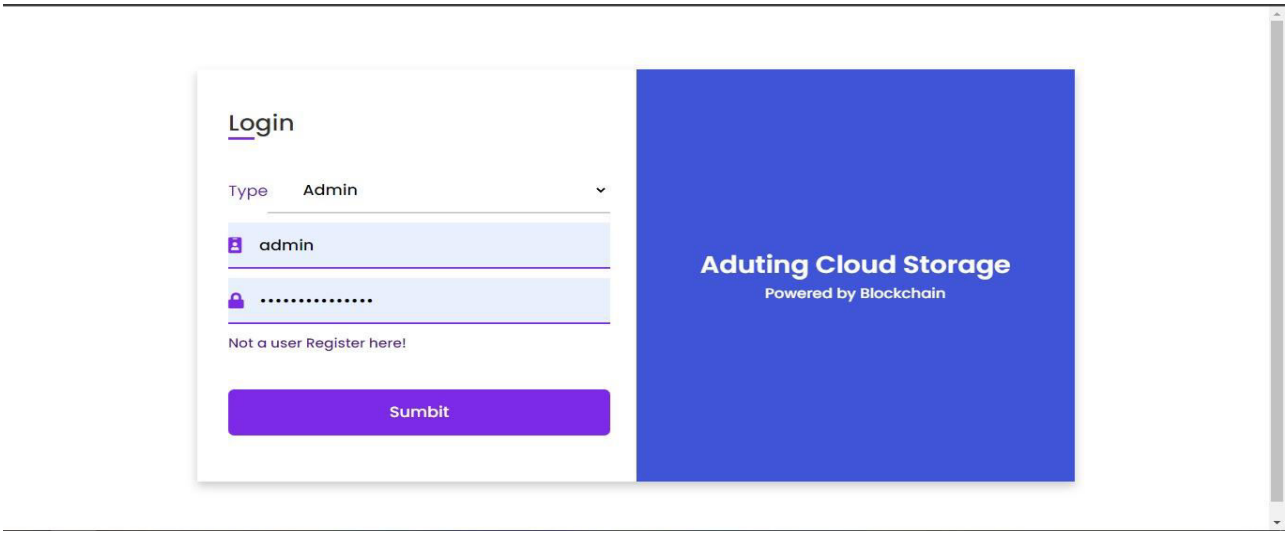

Fig 2. Login Form

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105252 |

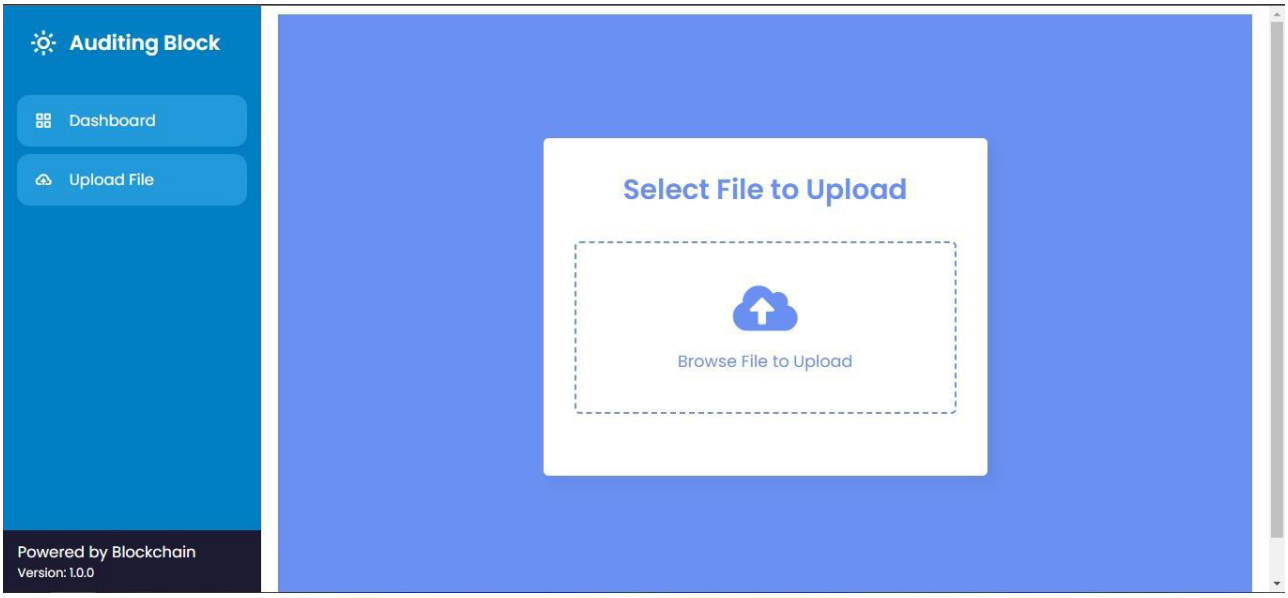

Fig 3. Dashboard

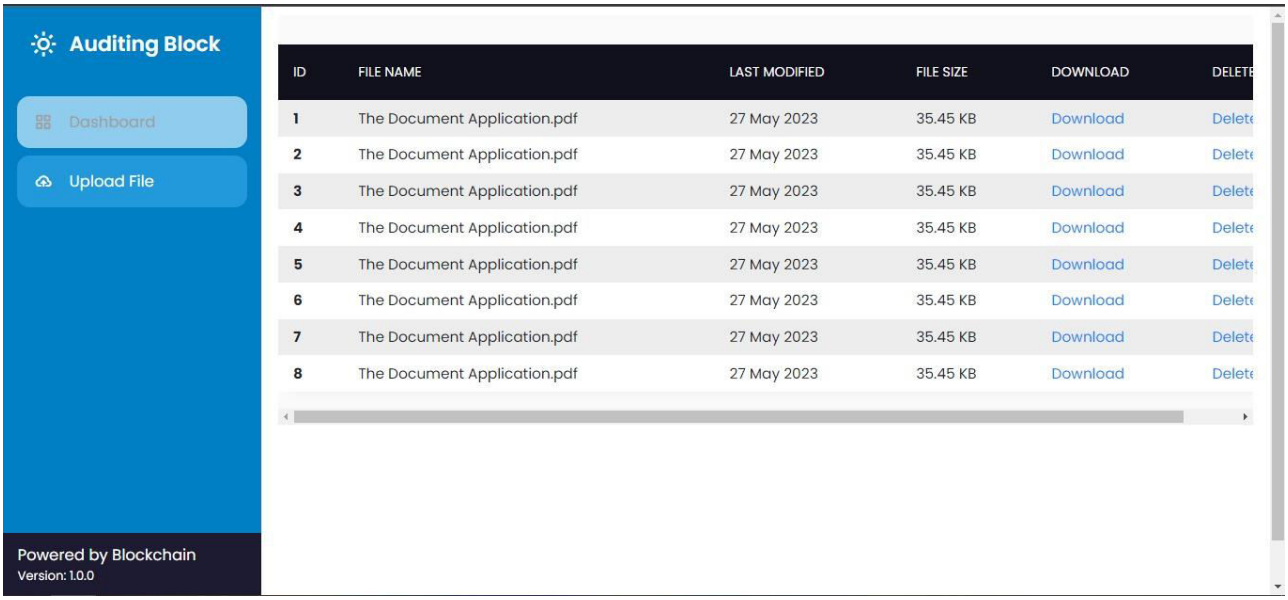

Fig 4. Uploaded File

V. CONCLUSION

In this Paper, we proposed or we design a decentralized and privacy preserving public auditing scheme, which is secure against the procrastinating third-party auditor and malicious cloud server. Our scheme utilizes two components to generate unpredicted challenge messages. One is generated by the auditor, and the other is a series of decentralized block hashes. Our scheme could resist against the procrastinating auditor, and a malicious cloud server could not retrieve or guess the challenge message ahead of the audit time. Furthermore, our scheme provides better protection of user privacy during the process of verification of the audit response from the cloud server. We analyzed our scheme to show that it is secure, and conducted a comprehensive performance analysis, showing that our scheme has low communication overhead and is efficient in terms of computation overhead.

REFERENCES

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105252 |

1. E. Azhir, N. J. Navimipour, M. Hosseinzadeh, A. Sharifi, and A. Darwesh, ''Query optimization mechanisms in the cloud environments: A systematic study,'' Int. J. Commun. Syst., vol. 32, no. 8, May 2019, Art. no. e3940.
2. A. Singh and K. Chatterjee, ''Cloud security issues and challenges: A survey,'' J. Netw. Comput. Appl., vol. 79, pp. 88–115, Feb. 2017.
3. Y. Shin, D. Koo, and J. Hur, ''A survey of secure data deduplication schemes for cloud storage systems,'' ACM Comput. Surveys, vol. 49, no. 4, pp. 1–38, Feb. 2017.
4. M. Du, Q. Wang, M. He, and J. Weng, ''Privacy-preserving indexing and query processing for secure dynamic cloud storage,'' IEEE Trans. Inf. Forensics Security, vol. 13, no. 9, pp. 2320–2332, Sep. 2018.
5. N. Kaaniche and M. Laurent, ''Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms,'' Comput. Commun., vol. 111, pp. 120–141, Oct. 2017.
6. Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, ''Intelligent cryptography approach for secure distributed big data storage in cloud computing,'' Inf. Sci., vol. 387, pp. 103–115, May 2017.
7. N. A. Kofahi and A. R. Al-Rabadi, ''Identifying the top threats in cloud computing and its suggested solutions: A survey,'' Adv. Netw., vol. 6, no. 1, pp. 1–13, 2018.
8. A. Juels and B. S. Kaliski, ''Pors: Proofs of retrievability for large files,'' in Proc. 14th ACM Conf. Comput. Commun. Secur. CCS, 2007, pp. 584–597.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details