IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

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 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203114 |

Data Integrity Audit Scheme Based on Blockchain Expansion Technology

Dr. P. Ravinder Rao, Gundlapally Sairam, Jannapala Dayamani, Vootkur Likitha

Assistant Professor, Department of CSE, Anurag Group of Institutions, Hyderabad, Telangana, India

Department of CSE, Anurag Group of Institutions, Hyderabad, Telangana, India

ABSTRACT: A growing number of users are entrusting their data to the cloud, but ensuring data integrity poses a significant challenge. Blockchain, known for its decentralization and immutability, is increasingly being explored by researchers as a substitute for third-party auditors. This research introduces a data integrity system leveraging blockchain expansion technology, targeting the high costs associated with maintaining blockchain networks and the creation of new blocks. The rapid expansion of blocks in existing blockchain data integrity audits prompted this approach. In this system, users and cloud service providers (CSP) deploy smart contracts on both the main chain and sub-chains. To mitigate costs, resource-intensive computing tasks are offloaded to the sub-chain, and results are periodically submitted to the main chain for confirmation. The concept of non-interactive audits is introduced to maintain a smooth user experience by avoiding constant communication with CSP during audits. For enhanced data security, a reward pool mechanism is implemented. Rigorous analysis encompassing storage, batch auditing, and data consistency validates the scheme's correctness. Experiments conducted on the Ethereum blockchain platform illustrate the scheme's effectiveness in significantly reducing storage and computational overhead.

KEYWORDS: Blockchain, cloud storage, data auditing, blockchain expansion, TPA.

I. INTRODUCTION

Cloud computing is a distributed computing model based on a large shared virtualized computing resource pool, it helps users use powerful computing and storage resources. And it can greatly reduce the burden of data storage on hardware and software for users, which encourages many enterprises and individuals to store their data on cloud servers.

Despite the great success of cloud storage, it also faces various challenges, and its security, reliability and privacy have always been a serious issue. After the user stores the data on the cloud server, the server provider may damage or delete the user data due to various factors, verifying the integrity of outsourced data becomes a crucial issue in cloud storage. Remote data integrity audit technology is very convenient and safe to help users check the integrity of data stored in outsourced. Therefore, the essence of cloud data security is how cloud storage providers (CSP) can establish trust with users. Cloud device failures, illegal attacks, and CSPs may be bribed to view user data, all of which can lead to illegal infringement of user data. Furthermore, even if the user data is damaged, the user may not be able to hold the CSP accountable effectively, since the CSP may evade responsibility and deny it. This is due to the lack of trust between the two parties, resulting in the party being questioned being unable to come up with evidence that would convince the other party. In addition, the current law on cyber security is not sound, which makes it difficult for users to obtain due compensation.

In traditional cloud auditing schemes, there is an entity called auditors (often referred to as third-party auditors, or TPA) which implement public audits. The TPA accept audit mandates from data owners and perform as instructed. In each of these methods, a trusted Third Party Auditor (TPA) must be found to assist the user in auditing, but in reality it is difficult to find fully trusted third-party auditors. For example, TPA will also partner with CSP for some ulterior purpose to hide data corruption, or with data owners to avoid penalties.

The emergence of block chain can solve this problem very well. Block chain has the properties of decentralization, tamper resistance, consistency and traceability. Therefore, information stored on the block chain is open and transparent. In recent years, more and more researchers use block chain to replace third-party auditors. Although the use of block chain as a trusted third-party auditor can well address users' concerns in cloud computing

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203114 |

environments, but the rapid growth of blocks will lead to high cost for block chain network maintenance and for user creation of new blocks.

II. RELATED WORK

The Although the emergence of blockchain has many advantages in data integrity auditing, with the increase of the number of users, the transaction throughput of the blockchain system will be seriously insufficient, and the storage burden on the blockchain is bound to increase. The basic idea is to increase the block size (either directly or indirectly) or reduce the block verification propagation time and consensus formation time. The off-chain expansion scheme mainly includes four methods: state channel, side chain, cross-chain and offchain computation. The idea is to transfer some on-chain transactions to off-chain for execution, in order to reduce the processing pressure on the chain and improve the overall efficiency. While improving the performance of the blockchain, the off-chain scaling technology takes into account decentralization and security, and has various excellent properties.

III. EXISTING METHOD

Fan *et al.* zhe'ge replaced the TPA with a smart contract, and the user signed an agreement with the CSP to prevent one party from denying it. The data owner obtains the hash of the remote data through the block identifier and compares it with the hash value previously stored in the blockchain ledger. Obviously, this scheme cannot resist the replay attack carried out by the CSP. Yu *et al* decentralize the data without any TPA in their scheme. Their solution is effective against replay attacks due to the random challenge set generated in each audit request. To defend against dishonest provers and verifiers, Xu *et al.* proposed an arbitrable data audit protocol that supports exchange hashing. Existing cloud storage service providers (CSP) may not have a fair compensation for users even if they damage data, and CSP may store redundant and duplicate data. Yuan *et al.* proposed a deduplication scheme with public audit and fair arbitration.

Zhou *et al.* proposed a solution for blockchain scalability. The existing expansion schemes are designed to improve different layers, and are divided into layer-0 expansion, on-chain expansion, and off-chain expansion. Among them, on-chain expansion improves the efficiency of the blockchain by changing the basic protocol. Off-chain expansion does not change the basic protocol, and changes are made at the application layer to improve scalability. Layer-0 expansion improves blockchain scalability by changing the underlying data transmission protocol of the blockchain. The on-chain expansion scheme includes data layer improvement scheme, consensus layer improvement scheme and network layer improvement scheme. The basic idea is to increase the block size (either directly or indirectly) or reduce the block verification propagation time and consensus formation time. The off-chain expansion scheme mainly includes four methods: state channel, side chain, cross-chain and off- chain computation. The idea is to transfer some on-chain transactions to off-chain for execution, in order to reduce the processing pressure on the chain and improve the overall efficiency. While improving the performance of the blockchain, the off-chain scaling technology takes into account decentralization and security, and has various excellent properties.

The disadvantages of existing systems in data integrity audit scheme based on blockchain, as highlighted by the research, include:

- The system is not implemented Data auditing technique for data integrity proof.
- The system is not implemented Data Hashing Techniques.

IV. PROPOSED METHOD

The advantages of the data integrity audit scheme based on blockchain expansion technology are as follows:

- **Batch auditing**: including multi-user single-task auditing and multi-user multi-task auditing. This is to ensure the efficiency of auditing.
- **Public auditing:** Ensure that any user including the data owner can challenge the CSP to verify the integrity of the data based on the certificate generated by the CSP.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203114 |

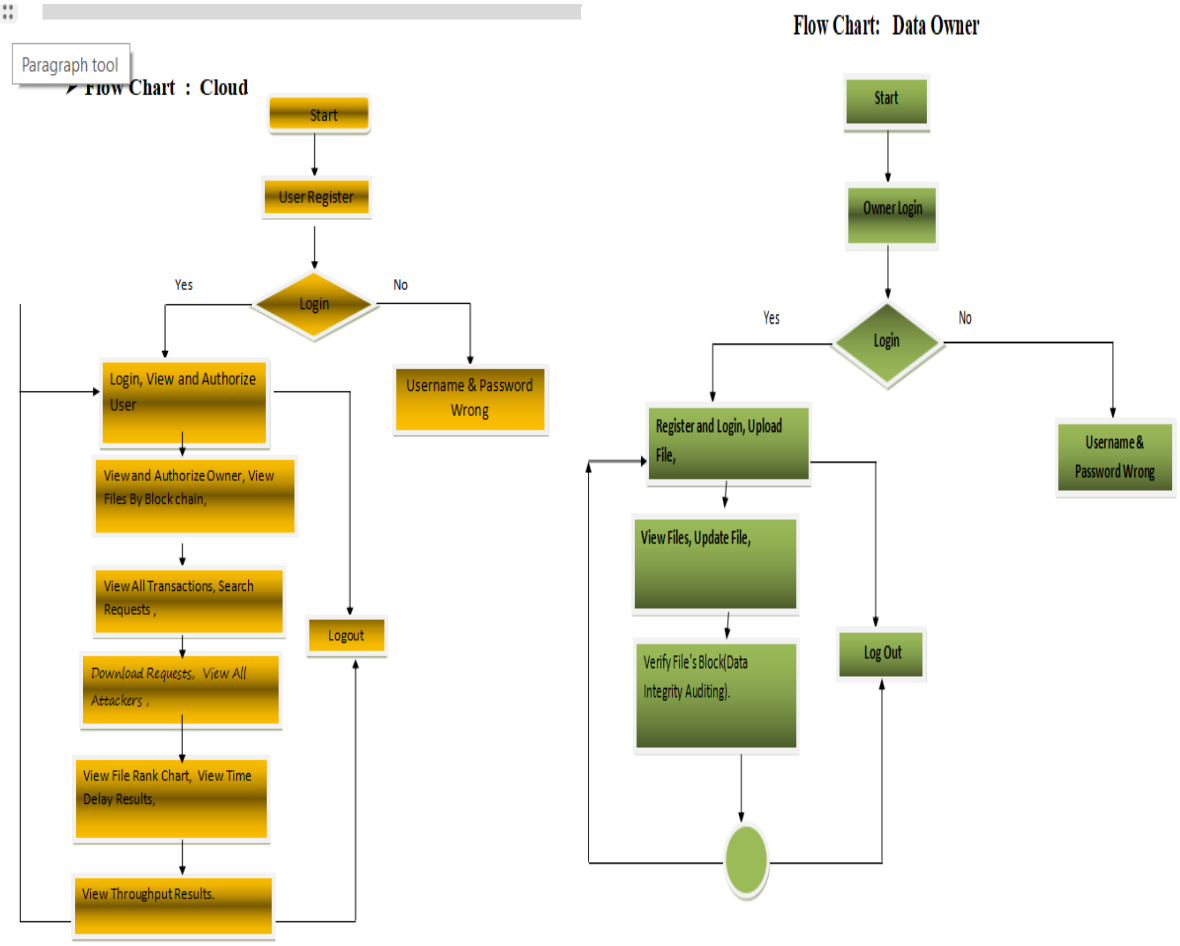

Fig 1: Flow Chart

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203114 |

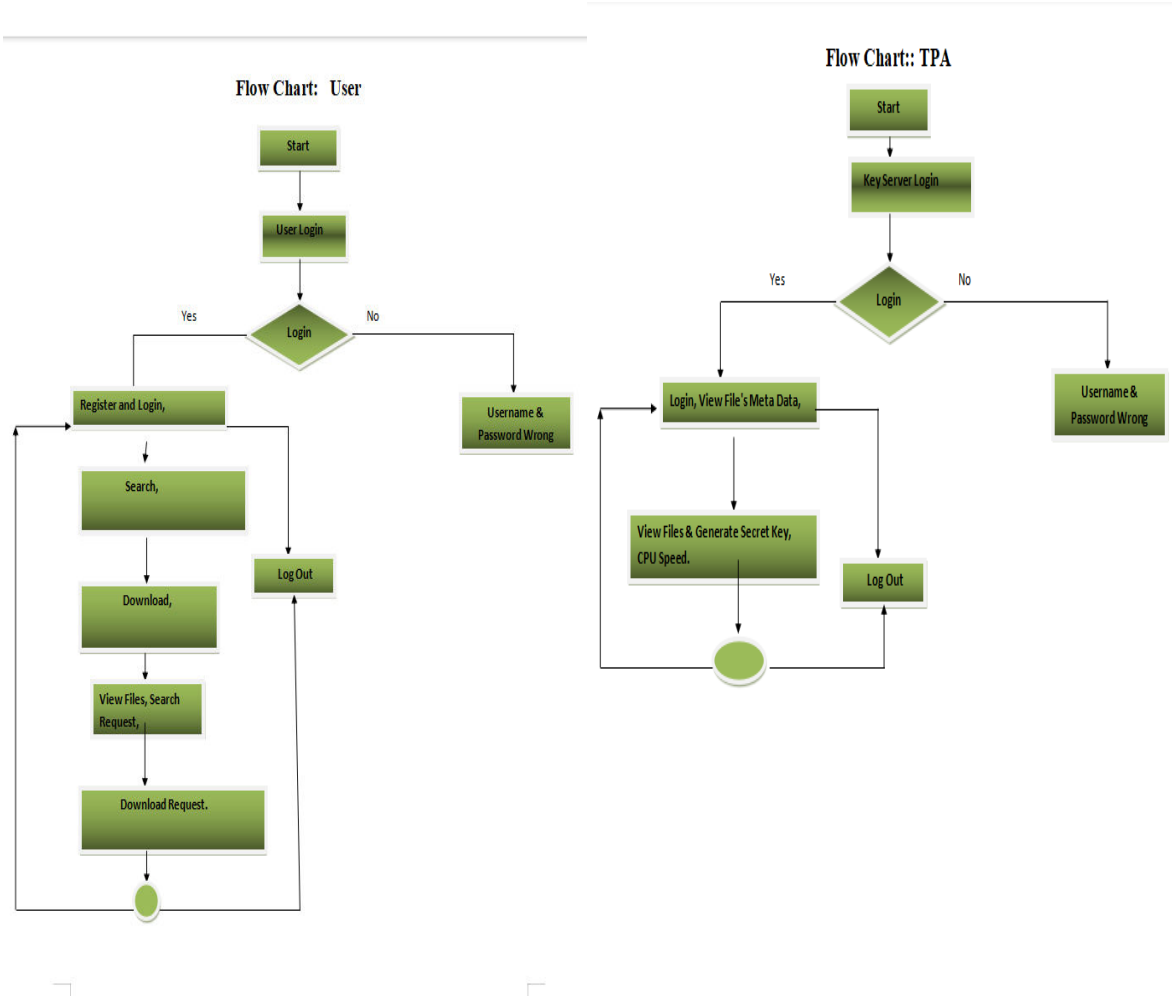

Fig 2: Flow Chart

V. SIMULATION RESULTS

The project you are inquiring about focuses on a trustworthy data sharing framework utilizing blockchain technology. Several research papers have explored this topic, highlighting the significance of blockchain in enhancing data trust and sharing. The framework aims to address challenges related to data accuracy, provenance, privacy implications, and fair incentives for data providers. Blockchain's properties like transparency, immutability, non-repudiation, and decentralization make it suitable for improving trust in data-sharing platforms. However, challenges such as performance limitations, scalability issues, and high costs hinder its effectiveness in handling big data.

Key points from the search results include:

- The proposed framework emphasizes enhancing data trust through blockchain technology
- Blockchain is recognized for its potential in ensuring trustworthy data sharing and addressing various challenges in data accuracy and privacy
- Research has highlighted the importance of blockchain in providing transparency, immutability, and decentralization to enhance trust in data-sharing platforms

These findings underscore the growing interest and importance of blockchain technology in establishing secure and reliable data-sharing frameworks.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203114 |

Fig 2.1: Home Page

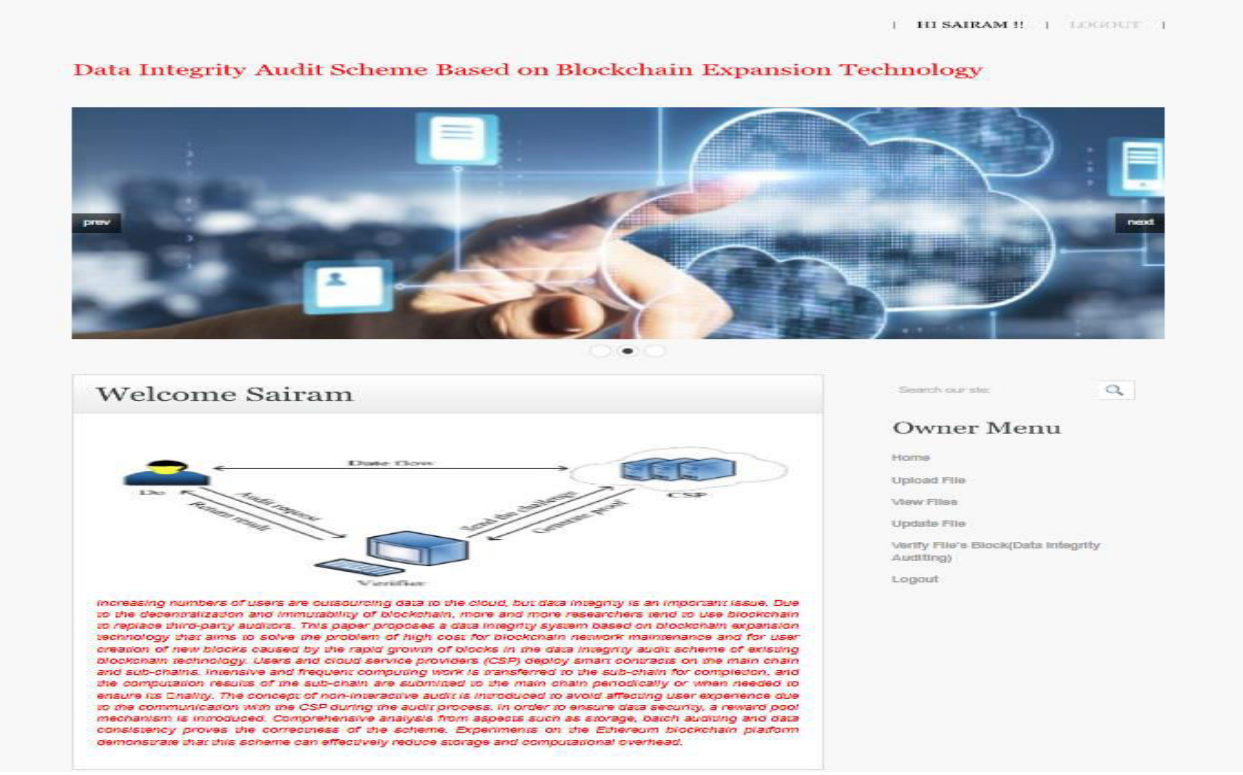

Fig :2.2 :Home Page of Owner

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 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203114 |

Fig:2.3:Home Page of User

Fig:2.4: Home page of Cloud Service Provider

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203114 |

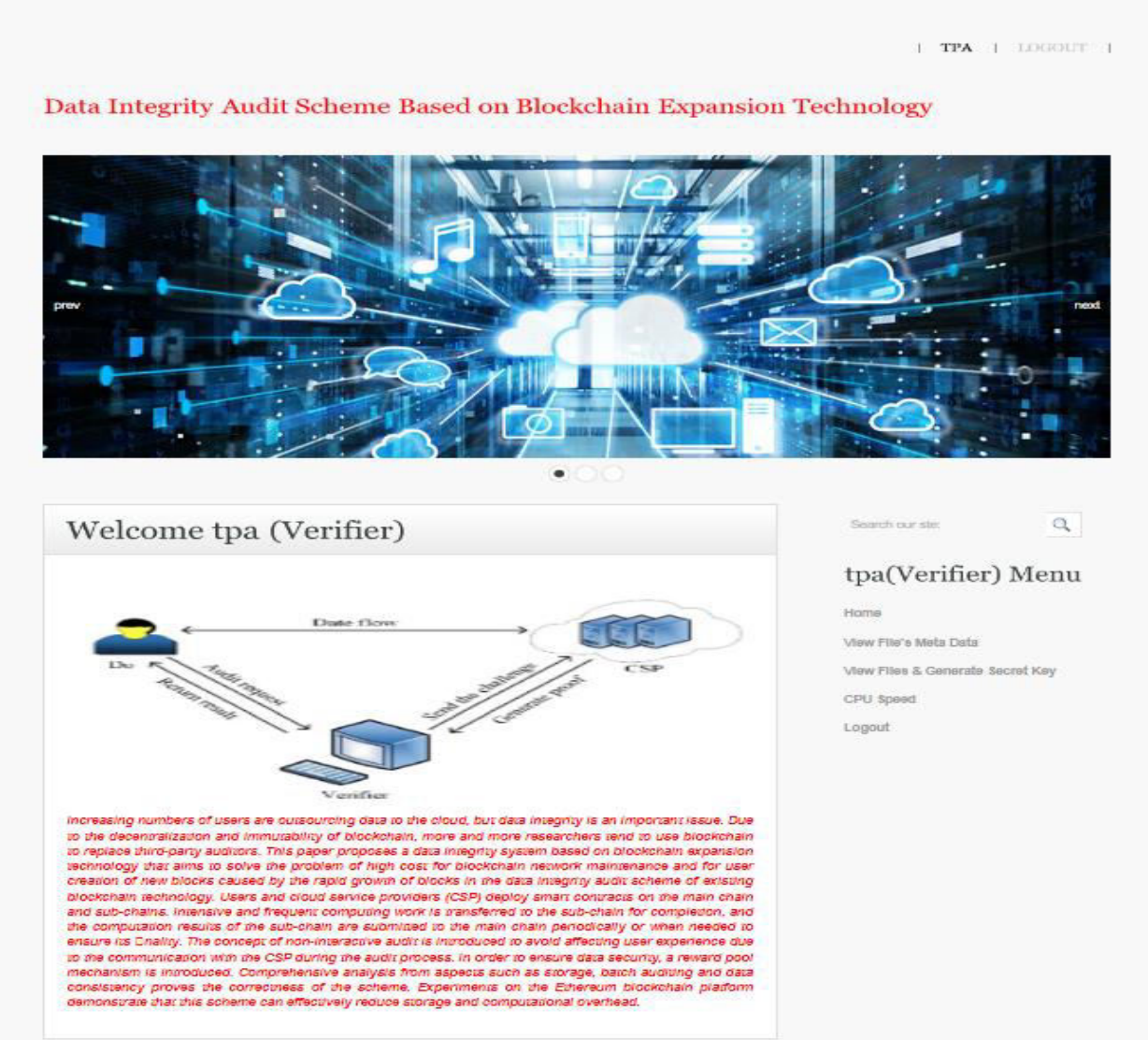

Fig:2.5 : Home Page of TPA

VI. CONCLUSION AND FUTURE WORK

As cloud computing and cloud storage technologies evolve faster and faster, the amount of data in cloud storage grows explosively, how can we ensure that the full information stored by users on cloud servers becomes an important topic for discussion. This article proposes a data integrity scheme based on block chain expansion technology. In our scheme, we use the block chain network to overcome some of the shortcomings of traditional auditing, improving the efficiency and security of the scheme. In addition, we introduce plasma sub-chain and deploy smart contracts on the main chain and sub-chain respectively. Through this protocol, the storage pressure of the main chain can be greatly reduced, the growth rate can be slowed down, the storage and computational overhead can be reduced, and the system performance can be improved. At the same time, the reward pool mechanism and the concept of non-interactive audit are introduced to ensure the correctness of the audit and avoid the interaction between the smart contract platform and the CSP during the contract execution process, and the solution can achieve the expected security goals.

REFERENCES

[1] Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong and J. Lei, "One secure data integrity verification scheme for cloud storage", Future Gener. Comput. Syst., vol. 96, pp. 376-385, Jul. 2019.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203114 |

[2] Zhou, H. Huang, Z. Zheng and J. Bian, "Solutions to scalability of blockchain: A survey", IEEE Access, vol. 8, pp. 16440-16455, 2020.
[3] Xu, W. Chen and Y. Zhang, "Blockchain-based integrity verification of data migration in multi-cloud storage", J. Phys. Conf. Ser., vol. 2132, no. 1, Dec. 2021.
[4] Xie, Y. Liu, G. Xin and Q. Yang, "Blockchain-based cloud data integrity verification scheme with high efficiency", Secur. Commun. Netw., vol. 2021, pp. 1-15, Apr. 2021.
[5]Lei, Z. Jia, Y. Yang, Y. Cheng, and J. Fu, ``A cloud data access authorization update scheme based on blockchain," in *Proc. 3rd Int. Conf. Smart BlockChain (SmartBlock)*, Oct. 2020, pp. 33_38.
[6] Y. Yuan, J. Zhang, W. Xu, and Z. Li, ``Identity-based public data integrity veri_cation scheme in cloud storage system via blockchain," *J. Supercomput.*, vol. 78, pp. 8509_8530, Jan. 2022.

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