International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

DATA INTEGRITY AUDIT SCHEME BASED ON BLOCKCHAIN EXPANSION TECHNOLOGY

Arun kumar.V[1], K. Pravalika[2], B. Nishika[3], D. Joshitha Sree[4]

[1] Assistant Professor, Department of IT,Malla Reddy Engineering College For Women (UGC-Autonomous), Maisammaguda,Dhulapally,Secunderabad,Telangana-500100

[234]UG Scholar, School of CS,Malla Reddy Engineering College for Women, (UGC-Autonomous), Maisammaguda,Dhulapally,Secunderabad,Telangana-500100

ABSTRACT

As more users move their data to the cloud, ensuring data integrity has become a significant concern. Blockchain technology, with its decentralized and immutable nature, has emerged as a promising solution, replacing the need for third-party auditors. This paper introduces a data integrity system built on blockchain expansion technology, aiming to address the high costs associated with blockchain network maintenance and the creation of new blocks, which often arise as the size of the blockchain grows in data integrity audit schemes.The proposed system involves both users and cloud service providers (CSPs) deploying smart contracts on the main chain and sub-chains. By offloading intensive and frequent computing tasks to the sub-chain, the system reduces the load on the main chain. Results from the sub-chain are periodically submitted to the main chain, ensuring the integrity and finality of the data without compromising performance.To enhance the user experience, the concept of non-interactive auditing is introduced, eliminating the need for constant communication between the user and the CSP during the audit process. A reward pool mechanism is also incorporated to promote data security.Through comprehensive analysis in areas such as storage, batch auditing, and data consistency, the effectiveness of the scheme is demonstrated. Experiments conducted on the Ethereum blockchain platform show that the proposed system significantly reduces storage and computational overhead, proving its practical viability.

Keywords : Data Integrity, Cloud Computing, Blockchain Technology, Blockchain Expansion, Smart Contracts, Sub-chains, Main Chain, Non-Interactive Audit, Third-Party Auditors, Cloud Service Providers (CSP),Batch Auditing, Data Security, Ethereum Blockchain, Blockchain Network Maintenance, User Experience, Data Consistency

I.INTRODUCTION

Cloud computing allows users to take advantage of powerful computing and storage resources without the need to manage the underlying hardware. This has made it easier for businesses and individuals to store their data on cloud servers, reducing the burden on their own systems. However, while cloud storage has become widely used, it still faces challenges, particularly around security, reliability, and privacy. One major concern is that cloud service providers (CSPs) may accidentally or intentionally damage or delete user data, making data integrity a crucial issue.To address these concerns, remote data integrity auditing has emerged as a safe and convenient way for users to verify the integrity of their data stored in the cloud. The real challenge in ensuring cloud data security lies in building trust between users and CSPs. Risks like hardware failures, cyberattacks, or even the bribing of CSPs to access sensitive data all threaten user privacy. Furthermore, if data is damaged, users may struggle to hold CSPs accountable due to the lack of evidence and trust between the two parties. Current cybersecurity laws are also inadequate, leaving users with little recourse in these situations.

In traditional cloud storage models, third-party auditors (TPAs) are often used to perform data integrity checks. However, finding fully trustworthy auditors is difficult. TPAs may have hidden motives, such as colluding with CSPs or data owners to hide corruption or avoid penalties.Blockchain technology offers a potential solution. With its decentralized, tamper-proof, and transparent nature, blockchain can replace traditional auditors and provide a higher level of security for cloud data. However, the rapid growth of blockchain data can lead to high maintenance costs and slow down the process of adding new blocks.

To tackle these challenges, a new data integrity verification system based on blockchain expansion technology has been proposed. This system slows down the growth of the blockchain, reducing storage and computation costs. The main contributions of this approach are:

Data Integrity Audit Protocol: The introduction of plasma smart contracts allows for reduced storage pressure on the main blockchain by using both the main chain and sub-chains. This approach ensures that audits can be conducted with minimal computational and communication overhead.

Batch Auditing Scheme: This scheme allows multiple audits to be processed at once, making it more efficient. The use of non-interactive auditing ensures that users don't experience delays during the audit process. A reward pool mechanism motivates the verification nodes to perform audits correctly, ensuring data integrity.

Security Analysis: A thorough security analysis shows that the system meets its intended security goals. Experiments conducted on the Ethereum blockchain demonstrate that the solution is both efficient and effective

II.RELATED WORK

Outsourced Data Integrity Verification in Untrusted Environments

K. Hao, J. Xin, Z. Wang, and G. Wang (2020) propose a blockchain-based data integrity verification scheme for outsourced data in untrusted environments. This work focuses on ensuring the integrity of data stored in third-party environments, such as cloud storage, by leveraging the immutability and security features of blockchain. They explore the role of blockchain in providing transparent, auditable logs for data access and tampering verification.

Data Integrity Verification for Cloud Storage

Y. Fan et al. (2019) discuss a secure data integrity verification scheme for cloud storage systems. The authors propose a method that ensures data integrity while preserving privacy. The approach integrates blockchain technology to enhance verification processes and protect data from unauthorized access or modification.

Blockchain-Based Data Integrity Verification for Large-Scale IoT Data

H. Wang and J. Zhang (2019) present a blockchain-based solution for data integrity verification in IoT systems. The challenge in IoT environments lies in ensuring that large-scale, distributed data can be verified for authenticity without requiring centralized control. Their approach leverages blockchain's decentralized nature to verify data integrity and enhance system security.

Blockchain-Based Flexible Data Auditing for Cloud Services

F. Kefeng et al. (2021) propose a flexible data auditing scheme for cloud services based on blockchain. This work emphasizes flexibility, allowing users to modify or update their data while still ensuring integrity checks through blockchain technology. It aims to solve issues related to trust and auditing in multi-tenant cloud environments.

5. **Data Integrity Verification Using T-Merkle Tree for Cloud Storage**

K. He et al. (2020) combine blockchain with a T-Merkle tree structure for cloud storage data integrity verification. The T-Merkle tree improves efficiency in verifying the integrity of large datasets. The approach ensures that data verification can be performed quickly, even with large volumes of data being stored in cloud environments.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

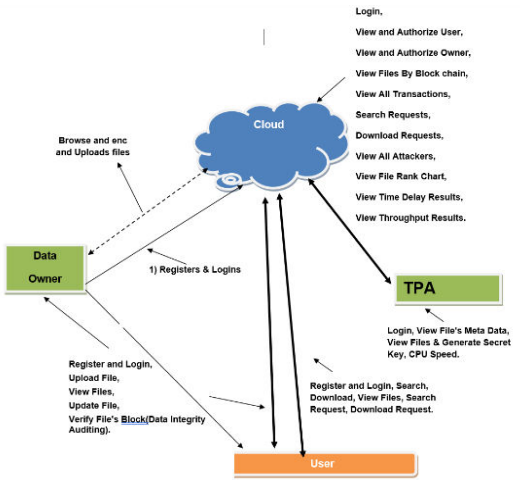

Fig:1.Architecture

III.IMPLEMENTATION

1. Setting Up the Blockchain

Choosing the Blockchain Platform: The first step is to select a blockchain platform like Ethereum, which is known for supporting smart contracts. This is where all the data and audit processes will take place.

Main and Sub-Chains: The blockchain system will have a main chain and additional sub-chains. The main chain handles the important data and overall validation, while the sub-chains handle more frequent tasks like checking data integrity. This setup helps keep things running smoothly as the system grows.

2. Smart Contracts

On the Main Chain: The main chain will have smart contracts that manage important tasks like storing data, verifying its integrity, and making sure everything is running according to the rules.

On the Sub-Chains: The sub-chains will handle the smaller tasks, like performing checks on the data and calculating hash values. These smart contracts help reduce the workload on the main chain and keep things efficient.

3. Data Integrity Auditing

Hashing the Data: Every piece of data stored in the cloud gets a unique "fingerprint" called a hash. This hash is stored in the blockchain so that if the data is altered, the change can be easily detected.

Auditing the Data: The system will check data periodically to make sure it's still intact by comparing its current hash to the one saved in the blockchain.

Non-Interactive Auditing: To avoid disrupting the user experience, the audit process doesn't require users to constantly interact with the cloud provider. The system can perform audits automatically, making it seamless for users.

4. Blockchain Expansion Techniques

On-Chain Expansion: As the blockchain grows, we can increase the block sizes or adjust how data is processed to keep things running smoothly. This helps the system handle more transactions without slowing down.

Off-Chain Expansion: Some tasks can be done off the blockchain itself to reduce the load. For example, we might use side chains or state channels to perform certain calculations, and only the results are recorded on the main blockchain. This keeps the system fast and efficient.

5. Batch Auditing and Rewards

Batch Auditing: Instead of checking data one by one, we group multiple audits together. This speeds up the process and reduces the number of transactions that need to be processed.

Reward System: To encourage participants to help verify the data, a reward pool is set up. Validators who correctly audit the data are rewarded with tokens or other incentives.

6. Security Measures

Preventing Replay Attacks: The system includes measures to prevent bad actors from reusing old data to cheat the system. Each audit request is unique, which makes it difficult for anyone to manipulate the data.

Arbitration: If a dispute arises (like if a user claims their data was tampered with), the system includes a way for third parties to step in and resolve the issue, ensuring fairness and transparency.

7. Testing and Improvement

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Testing the System: Before going live, the system is tested to make sure it can handle large amounts of data and transactions without breaking down. The goal is to ensure everything works smoothly even as the number of users grows.
Audit Accuracy Testing: The system is also tested to ensure that it can detect data corruption and inaccuracies reliably, without requiring users to do anything.

8. Deployment and Monitoring
Going Live: Once everything is set up and tested, the system is deployed. This means that the blockchain, smart contracts, and reward pools are all live, and users can start using the service.
Continuous Monitoring: After deployment, the system is continuously monitored to make sure everything is running smoothly. This includes checking for security issues or performance problems and fixing them as needed.

IV.ALGORITHM USED

1. Hashing Algorithms :

SHA-256 (Secure Hash Algorithm 256-bit) The SHA-256 algorithm produces a 256-bit (32-byte) hash value from input data. It is based on the Merkle–Damgård structure and involves multiple rounds of bitwise operations, including modular addition, bitwise shifts, and logical operations (XOR, AND, OR).The formula for SHA-256 can be represented as:

$$H(m) = \text{SHA-256}(m)$$

2. Smart Contract Algorithms :
Plasma Protocol:
This helps with scalability by using sub-chains to handle most transactions off the main blockchain, reducing congestion and improving efficiency.
Merkle Tree: Merkle Trees are used to efficiently and securely verify the integrity of large datasets. A Merkle tree is a binary tree where each leaf node is a hash of a data block, and each non-leaf node is the hash of its children.

$$R = H(H(D_1)||H(D_2)||H(D_3)||...||H(D_n))$$

Where:

- H is the cryptographic hash function (e.g., SHA-256).
- $D_1, D_2, ..., D_n$ are the data blocks being verified.
- $||$ denotes concatenation of the hash values.

4. Consensus Algorithms
Proof of Work (PoW)
Proof of Work requires participants (miners) to solve a computationally difficult problem to add a block to the blockchain. The objective is to find a nonce NNN such that the hash of the block's header satisfies the target difficulty:

$$\text{SHA-256}(H_{\text{block}}||N) < \text{Target}$$

Where:

- H_{block} is the hash of the block header.
- N is the nonce.
- Target is a predefined threshold (difficulty target).

V.RESULTS

Fig 1 : Home Page

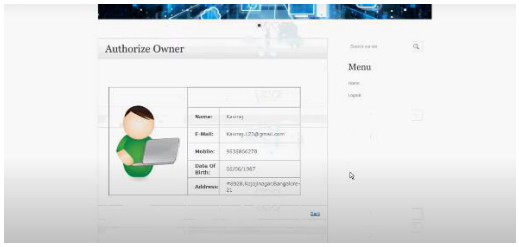

Fig 2 : Authorize Owner

Fig 3 : Data Received Time Delay

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

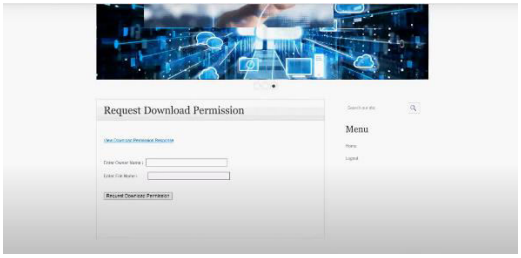

Fig 4 : Request Download Permission

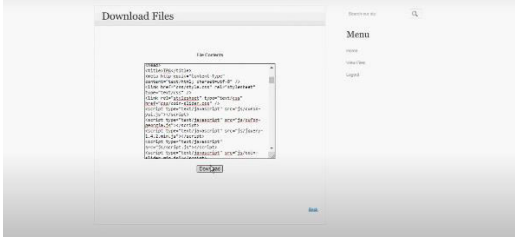

Fig 5 : Download Files

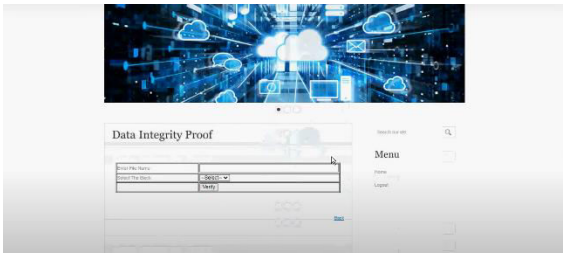

Fig 6 : Data Integrity Proof

VI CONCLUSION

As cloud computing and storage technologies continue to evolve rapidly, the volume of data stored in the cloud is increasing at an unprecedented pace. Ensuring the integrity of this extensive data repository has emerged as a significant concern. This article introduces a data integrity solution that utilizes blockchain expansion technology. By harnessing the capabilities of the blockchain network, our method overcomes several limitations associated with conventional auditing techniques, thereby enhancing both efficiency and security. We propose the use of plasma sub-chains and implement smart contracts on both the primary and sub-chains. This configuration alleviates the storage demands on the main chain, mitigates its growth rate, reduces storage and computational expenses, and improves overall system performance. Furthermore, we integrate a reward pool system along with the concept of non-interactive audits to guarantee the precision of the auditing process while minimizing

REFERENCES

[1] K. Hao, J. Xin, Z. Wang, and G. Wang, ‘‘Outsourced data integrity,verification based on blockchain in untrusted environment,’’Jul. 2020.
[2] Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong, and J. Lei, ‘‘One secure data integrity verification scheme for cloud storage,’’ Jul. 2019.
[3] H. Wang and J. Zhang, ‘‘Blockchain based data integrity verification for
large-scale IoT data,’’ 2019.
[4] Z. Miao, C. Ye, P. Yang, R. Liu, B. Liu, and Y. Chen, ‘‘A scheme for electronic evidence sharing based on blockchain and proxy re-encryption,’’Dec. 2021
[5] F. Kefeng, L. Fei, Y. Haiyang, and Y. Zhen, ‘‘A blockchain-based flexible
data auditing scheme for the cloud service,’’ Nov. 2021.
[6] K. He, J. Shi, C. Huang, and X. Hu, ‘‘Blockchain based data integrity verification for cloud storage with T-Merkle tree,’’ Oct. 2020
[7] Y. Lei, Z. Jia, Y. Yang, Y. Cheng, and J. Fu, ‘‘A cloud data access authorization update scheme based on blockchain,’’Oct. 2020
[8] Y. Yuan, J. Zhang, W. Xu, and Z. Li, ‘‘Identity-based public data integrity verification scheme in cloud storage system via blockchain,’’Jan. 2022.
[9] S. Wang, D. Zhang, and Y. Zhang, ‘‘Blockchain-based personal health records sharing scheme with data integrity verifiable,’’2019.
[10] A. Liu, Y. Wang, and X. Wang, ‘‘Blockchain-based data-driven smart customization,’’ in Data-Driven Engineering Design. Cham, Switzerland:Springer, 2022.
[11] K. Dhyani, J. Mishra, S. Paladhi, and I. S. Thaseen, ‘‘A blockchain-based

document verification system for employers,''2022.
[12] K. Xu, W. Chen, and Y. Zhang, ''Blockchain-based integrity verification of data migration in multi-cloud storage,''Dec. 2021.
[13] G. Xu, S. Han, Y. Bai, X. Feng, and Y. Gan, ''Data tag replacement algorithm for data integrity verification in cloud storage,''Apr. 2021.
[14] G. Xie, Y. Liu, G. Xin, and Q. Yang, ''Blockchain-based cloud data integrity verification scheme with high efficiency,''Apr. 2021.
[15] U. Arjun and S. Vinay, ''Outsourced auditing with data integrity verification scheme (OA-DIV) and dynamic operations for cloud data with multi-copies,'' EAI Endorsed Trans. Cloud Syst., Jul. 2018.
[16] A. V. Ezhil, G. K. Indra, and K. Kulothungan, ''Auditable attribute-based data access control using blockchain in cloud storage,''Jan. 2022.
[17] R. Mishra, D. Ramesh, D. R. Edla, and M. C. Trivedi, ''Blockchain assisted privacy-preserving public auditable model for cloud environment with efficient user revocation,'' Jan. 2022.
[18] X. Tao, Y. Liu, P. K.-Y. Wong, K. Chen, M. Das, and J. C. P. Cheng, ''Confidentiality-minded framework for blockchain-based , Apr. 2022
[19] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, ''Blockchain databased cloud data integrity protection mechanism,'' Jan. 2020.
[20] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, ''Blockchain empowered arbitrable data auditing scheme for network storage as a service,'' Mar. 2020.
[21] H. Yu, Z. Yang, and R. O. Sinnott, ''Decentralized big data auditing for smart city environments leveraging blockchain technology,'' 2019.
[22] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ''Privacypreserving public auditing for secure cloud storage,'' Feb. 2013.
[23] L. Chen, Q. Fu, Y. Mu, L. Zeng, F. Rezaeibagha, and M.-S. Hwang, ''Blockchain-based random auditor committee for integrity verification,''Jun. 2022.
[24] H. Yuan, X. Chen, J. Wang, J. Yuan, H. Yan, and W. Susilo, ''Blockchainbased public auditing and secure deduplication with fair arbitration,'' Dec. 2020.
[25] C. Yang, Y. Liu, F. Zhao, and S. Zhang, ''Provable data deletion from efficient data integrity auditing and insertion in cloud storage,'' Aug. 2022.
[26] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, ''Solutions to scalability of blockchain: A survey,''2020.
[27] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K.-K.-R. Choo, ''Fuzzy identitybased data integrity auditing for reliable cloud storage systems,''Jan. 2019.