Hindawi
Security and Communication Networks
Volume 2023, Article ID 9876716, 1 page
https://doi.org/10.1155/2023/9876716

Retraction

Retracted: Blockchain-Based Data Audit Mechanism for Integrity over Big Data Environments

Security and Communication Networks

Received 10 October 2023; Accepted 10 October 2023; Published 11 October 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Wu, S. A. Haider, M. Bhardwaj, A. Sharma, and P. Singhal, "Blockchain-Based Data Audit Mechanism for Integrity over Big Data Environments," *Security and Communication Networks*, vol. 2022, Article ID 8165653, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 8165653, 9 pages
https://doi.org/10.1155/2022/8165653

WILEY | Hindawi

Research Article

Blockchain-Based Data Audit Mechanism for Integrity over Big Data Environments

Jianbin Wu,[1] **Sami Ahmed Haider**,[2] **Manish Bhardwaj**,[3] **Aditi Sharma**,[4] **and Piyush Singhal**[5]

[1]*Department of Computer Science and Engineering Zhejiang Normal University, Jinhua, China*
[2]*Deparment of Computing University of Worcester, Worcester, UK*
[3]*KIET Group of Institutions, Assistant Professor Research Computer Science and Engineering, Ghaziabad, Uttar Pradesh, India*
[4]*Department of Computer Science Engineering & Information Technology,*
Institute of Engineering & Technology (an Autonomous Constituent Institute of Dr. A.P.J. Abdul Kalam Technical University, U.P Lucknow), Lucknow, India
[5]*Professor Department of Mechanical Engineering, GLA University, Mathura, India*

Correspondence should be addressed to Sami Ahmed Haider; s.ahmedhaider@worc.ac.uk

Received 5 February 2022; Accepted 19 April 2022; Published 16 May 2022

Academic Editor: Mukesh Soni

Recently, data integrity for multiagent-based big data environments has been challenging. This paper presents a blockchain-based Merkle DAG structure (M-DAG) for audit data integrity. M-DAG resolves the problem that arises due to the multicopy of a large data volume in a big data environment. It employed Boneh–Lynn–Shacham's (BSL) signature to verify the integrity of identical multicopy on big data environments. The proposed M-DAG audit mechanism uses a consortium chain algorithm for decentralized traceability and audit to archive reliable data. The evaluation has been carried out for the efficiency of the data integrity audit.

1. Introduction

The rapid development of big data technology has penetrated deeply into people's lives. Big data technologies such as government affairs big data [1], big judicial data [2], and extensive medical data [3] are gradually providing robust data technical support for the progress of the society. However, big data has characteristics different from traditional data and needs to be processed using technologies suitable for big data.

The most significant feature of big data is the large amount of data. Statista's global data volume will reach 175 ZB in 2025. The surge in data volume has prompted the development of related storage technologies. Storage technologies such as local storage, distributed storage, and cloud storage provide technical support for ample data storage. To ensure the security of big data storage, it is necessary to perform data integrity verification [4] to determine whether the data has been tampered with or damaged.

Data integrity verification technology generally realizes the judgment of data integrity through the challenge-response mechanism. The data owner stores the data in the data storage system and uses technologies such as BLS signature to realize the significance of the stored data before the data is stored and generates a certificate.

The data owner selects the corresponding data from the proof metadata to generate a challenge and sends the challenge to the data storage system. The data storage system uses the stored data to generate corresponding evidence of data integrity according to the challenge received. The data integrity audit institution judges the evidence generated by the data storage system and determines whether the data is consistent with the original data.

The data integrity audit of big data needs to fully consider the characteristics of big data:

(a) The large data volume of big data requires that data integrity verification technology meet the efficiency requirements of auditing and realize efficient judgment of data integrity.

(b) Due to the wide range of significant data sources, the data types have become diverse and data can be divided into three types: structured, semistructured, and unstructured [5]. For example, the significant data types in government affairs can be divided into four categories: business data, public opinion and social situation data, environmental data, and decentralized public data [6]. The data in the big data environment is mainly unstructured. According to IDC statistics, unstructured data accounts for 80% of big data. Therefore, unstructured data integrity verification has become the key to ample data integrity verification.

(c) At the same time, data has become an increasingly important resource in the information age. Therefore, breaking down data silos by sharing big data has become an important challenge for information companies. Data sharing requires the realization of data exchange and the authenticity of the data. For example, data authenticity is highly prominent for more sensitive data such as big government data, judicial big data, and medical big data.

The integrity verification of big data needs to prove that the data has not been tampered with or destroyed and needs to confirm with the users who share the data.

Satoshi Nakamoto published the article Bitcoin, a peer-to-peer electronic cash system [7], marking the birth of blockchain technology. Since then, blockchain technology has attracted many scholars to study its sound characteristics, such as decentralization and not being easy to tamper with. The data integrity verification technology verifies multiparty credits such as data storage. The combination of blockchain technology and data integrity verification technology can play a significant role in the data integrity verification system.

Based on this, this paper proposes a blockchain-based multiparty efficient audit mechanism for data integrity (MBE-ADI) to solve the audit problem of data integrity in the big data environment. The main contributions are as follows:

(a) Propose the concept of data domain in the big data environment and construct a hybrid Merkle DAG structure based on the data domain to realize the management of unstructured data. With this structure, the generation of proof metadata can be learned to solve a large number of unstructured data in the big data environment.

(b) Design a multicopy deterministic verification method based on BLS signature to realize multicopy simultaneous deterministic verification of data integrity and meet the needs of efficient data integrity verification in the big data environment.

(c) Design a dual-verification audit structure based on the alliance chain, the corresponding smart contract, and the metadata upload method of the verification process, realize the decentralized automatic audit of data integrity and the trusted traceability of audit history, and provide data for data owners and data users at the same time. The integrity verification service ensures the historical consistency of data before sharing and improves the credibility of the data.

(d) Deploy the MBE-ADI system based on the Alibaba Cloud server, and conduct related tests to verify the feasibility of the system and the efficiency of data integrity auditing.

2. Related Work

Indumathi et al. [8] proposed an integrity verification mechanism based on the MAC code, which uses the MAC value as authentication metadata to achieve data integrity verification. Still, there are problems of high communication overhead and easy privacy leakage. Rahalkar et al. [9] proposed a data possession proof, a PDP (provable data possession) mechanism, which divides the data into blocks and uses the RSA signature mechanism to sample the integrity of the data blocks, which improves the detection efficiency and reduces the communication overhead. Khan et al. [10] proposed a PDP mechanism that supports fully homomorphic operations, which uses the Merkle tree to verify the correctness of the location of the data block and uses the BLS signature to verify the integrity of the data block. Adekunle et al. [11] proposed a mechanism for integrity verification using multibranch path tree (MBT), which increases the out-degree of nodes. Compared with the integrity verification mechanism based on the Merkle tree, it can verify larger-scale data and use MBT. The structure can better realize data block replacement and other dynamic operations.

The multicopy mechanism can improve the antirisk capability of data and use multiple copies to repair damaged data in real time. For essential data, the multicopy tool is more important. Aloulou et al. [12] proposed a multicopy verification mechanism that supports dynamic operations. This mechanism transforms the Merkle tree structure and offers a level-based Merkle tree to help dynamic verification. This mechanism realizes the synchronous update of multiple copies by associating numerous documents. Agca et al. [13] discovered the generation of multicopy data through random mask technology using a constant amount of metadata for any number of replicas; new replicas can be dynamically created without preprocessing the data again, and the time and cost of multicopy integrity verification and for single-copy data are close. However, the multicopy mechanism generates too much metadata, such as random numbers, and the metadata management burden is too heavy when processing files with a large amount of data. Therefore, it is unsuitable for a big data environment with extensive and unstructured data.

The audit of the above data integrity verification mainly uses trusted third-party organizations. Still, it is difficult to find trusted third-party organizations and is prone to third-party attacks. Therefore, the application of blockchain technology for data integrity verification has become a new choice [14–21].

Pawar et al. [18] adopted blockchain smart contracts to replace third-party auditors and believed that data users should verify data integrity before sharing data. To achieve a fair integrity audit, Sahi et al. [19] considered blockchain technology for data integrity verification. The data owner uploads the signature of the data block to the blockchain ledger, uploads the encrypted data to the cloud, downloads the data during validation, and uses the digital signature recorded in the blockchain ledger to verify the integrity of the data. The study in [20] realized data integrity based on the blockchain through virtual agent mechanism.

Authentication, combined with role-based access control technology, is to manage and control stored data. Yang et al. [21] proposed a data integrity verification mechanism based on Ethereum [22], which holds data hash values, data signatures, and other information in smart contracts.

However, the current blockchain-based data integrity verification mechanism does not consider the needs of data users to obtain the authenticity of shared data and only provides services to data owners.

At present, some scholars have noticed the problem of integrity verification for big data. Prathiwi et al. [23] summarized the integrity verification technology of big outsourced data. Still, it is consistent with the technology proposed by Shen et al. [4] and does not reflect the characteristics of ample data integrity verification. Tyagi et al. [24] implemented a fine-grained update of data blocks, using a balanced update tree.

ADS (authenticated data structure) reduces update verification after the dynamic update, reducing computing and communication resources. Morrison et al. [25] proposed a distributed big data platform based on the blockchain to achieve data transaction integrity, focusing on designing an integrity manager module to ensure the authenticity and consistency of data. Mingming et al. [26] considered the characteristics of a wide range of significant data sources and a large amount of big data, proposed a data input verification model to verify the data source, and proposed a continuous integrity monitoring model to verify the integrity of the data during use but only the framework of the model.

Based on the above analysis, it is still necessary to study the data integrity verification mechanism suitable for the big data environment and fully consider the characteristics of the large data volume, a large amount of unstructured data, and the tendency to share in the big data environment.

3. Hybrid Merkle DAG Structure

Due to the wide range of data sources in the big data environment, most of them are unstructured data with different structures (for example, a set of data obtained by the data owner may include images, videos, documents, etc.). Efficient organization of data is a prerequisite for efficient validation. In this section, aiming at the characteristics of big data environment data, to realize the effective management of data and generate the proof metadata of data integrity audit on this basis, a hybrid Merkle DAG structure based on data domain is proposed. At the data domain level, the Merkle DAG structure is used to construct the organizational relationship between unstructured data. At the data block level, a multibranch balanced Merkle tree is built for the data blocks of a single data.

This section proposes the concept of the data domain, which is used to organize unstructured data. The domain here refers to a class of associated data or subdata domains. For a batch of data that needs to be stored, the data owner divides the data according to the internal relationship of the data (such as data source, acquisition date, and category) and classifies the data into one domain. This results in a maximum field containing all data and subdata fields.

A Merkle DAG structure in this storage structure is used. The Merkle DAG structure is constructed based on the Merkle tree, which breaks the limit of the number of subnodes of the Merkle tree, does not need to perform data balancing operations, and can build a more flexible data structure according to actual needs. Merkle DAG retains the Merkle tree loop computing node hash to obtain a Merkle root, the hash value of the parent node is determined by the hash value of the child node, and the parent node contains the information pointing to the child node. In IPFS [27], Merkle DAG is used as the data storage structure to realize the distributed file storage network.

The process of building a data domain-based hybrid Merkle DAG structure is as follows:

(a) According to the inclusion and parallel relationship of unstructured data, construct a Merkle DAG file structure containing all data

(b) Build a multibranch balanced Merkle tree structure for each data in the domain, and obtain the id node in the Merkle DAG node information.

4. Construction of the Merkle DAG File Structure

A data domain is constructed for unstructured data. The associated data is placed in one domain, and the data domain contains subdata domains. Data domains at all levels represent different degrees of association of data. Multiple pieces of associated data are stored in the domain simultaneously. The domain contains at least two data files. As shown in Figure 1, the data field is {A, A_1, A_2}. The A field contains {A_1, A_2, d_7, d_8, d_9}, the A_1 field contains {d_1, d_2}, and the A_2 field contains {d_3, d_4, d_5, d_6}.

The hybrid Merkle DAG structure based on the data domain contains domain and data nodes. A domain node is constructed for each part to identify the field. The domain node is shown in Figure 2. The node_{id} is the unique identification information of the domain node, and the id node can be used to distinguish the node; Lr is the write pointer, pointing to other nodes in the same level domain; $\{\text{ID}_1, \text{ID}_2, \ldots, \text{ID}_i\}$ is a child pointer, pointing to a data node or a child data domain node.

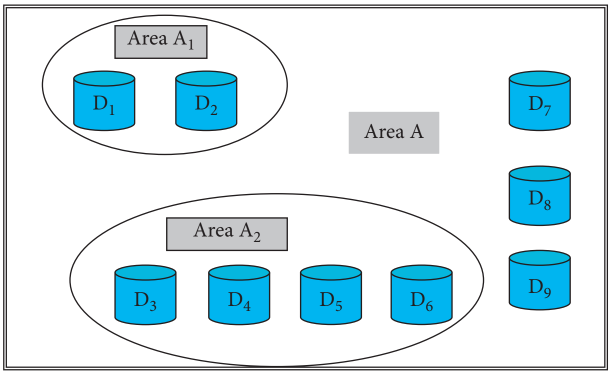

Figure 1: Data domain structure.

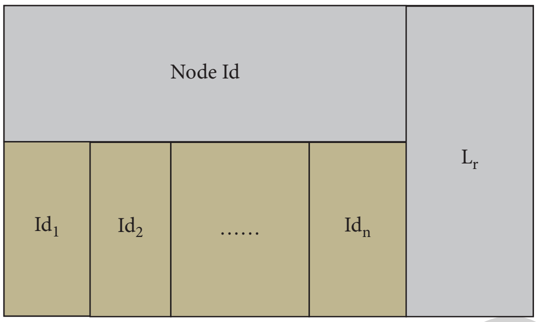

Figure 2: Merkle DAG structure domain node information based on the data domain.

In the hybrid Merkle DAG structure based on the data domain, each unstructured data is identified by a data node; the data node is shown in Figure 3. The $node_{id}$ is the unique identification information of the data node, and the $node_{id}$ can be used to distinguish the data nodes; Lr is the right pointer, pointing to the data node in the same-level domain. The Merkle DAG file structure shown in Figure 4 can be constructed for the data domain of Figure 1.

5. Result Analysis

5.1. Verifying Process Security. The integrity verification process is summarized into four stages: data copy generation, proof metadata generation, evidence generation, and evidence auditing [28, 29]. The unstructured data is organized by the Merkle DAG file structure based on the data domain. The $node_{DF}$ in the node information ensures the uniqueness of the node, the pointer information in the node information confirms that the structure of the Merkle DAG file is determined, and the data is determined in the data storage system. The replica generation mechanism ensures that data corruption can be repaired instantly. In the data copy generation stage, data encryption is implemented by setting μ at different AES keys $\{K_1, K_2, \ldots, K_\mu\}$. Copies are generated to prevent the storage system from pseudo-storing multiple copies of data. The copy generation mechanism can reduce the storage of copy parameters and avoid the loss and damage of massive parameters. In the proof metadata generation stage, the composite data domain $node_{DF}$ is

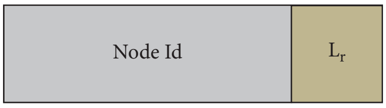

Figure 3: Merkle DAG unstructured data node information based on the data domain.

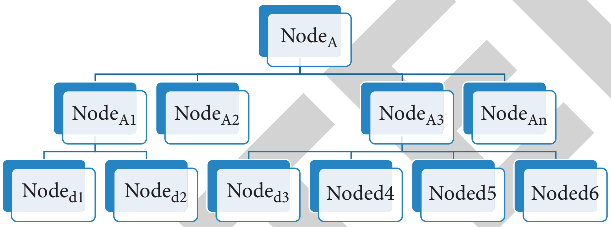

Figure 4: Merkle DAG file structure based on the data domain.

obtained by combining the random sequence splicing method and the $node_{DF}$ is signed to receive the proof metadata $\{node_{df}, l_i, s_i, \sigma_i, y\}$. In the evidence generation stage, the storage system also uses random sequence splicing to obtain the composite data domain $node_{DF}$. This method can ensure that the metadata generation must use complete copy data blocks to ensure the feasibility of integrity auditing. In the evidence verification stage, by checking whether (g, K_i, y, σ_i) is a DH quadruple, it is judged whether the data is damaged or not. The reliability of the verification result is guaranteed.

5.2. The Reliability of Block Chain Ledger Records. The integrity verification process in this paper is implemented through smart contracts, and the relevant data verified is recorded on the blockchain ledger. Intelligent contracts replace the auditing of evidence by trusted third parties, which can prevent third-party attacks on the verification process. The blockchain ledger can realize the secure and reliable multiparty storage of ledger data. The verification process data is recorded on the blockchain ledger to prevent all parties from tampering with the verification process and ensure the authenticity of the data integrity verification history. The unique identifier Node_block of the data on the blockchain ledger on the blockchain ledger is recorded. The determination of the unique identifier can ensure the data.

The consistency of storage and integrity verification enables retrieval of a particular data integrity verification history. By returning the data integrity verification history, the historical character of the data before sharing can be guaranteed and the reliability of the data can also be guaranteed.

5.3. Scheme Comparison. Table 1 shows the comparison between the proposed scheme and the existing scheme. The solution in this paper includes multiple data owners and data users and various data storage systems, which can realize multiparty auditing of data in the same field or data among alliance members. The scheme in this paper selects intelligent contracts as the system audit institution, which can

Table 1: Scheme comparison.

Plan	Participants	Auditor	Multiple copies	Deterministic verification	Public verification	Heterogeneous multiple data	Data dynamic modification	Verification of history retrieval	Multiparty verification
Literature [10]	SP	TPA	NO	NO	YES	NO	YES	NO	NO
Literature [11]	SP	TPA	NO	NO	YES	NO	YES	NO	NO
Literature [12]	SP	DO	YES	NO	NO	NO	YES	NO	NO
Literature [14]	SP	Dynamic TPA	NO	NO	YES	NO	NO	YES	YES
Literature [18]	DU	Smart contract	NO	YES	NO	NO	NO	NO	YES
Literature [19]	SP	DO/SP/ TPA	NO	NO	NO	NO	YES	NO	NO
Literature [20]	SP	Smart contract	NO	NO	YES	NO	YES	NO	NO
Proposed work	Multiple DUs	Smart contract	YES	YES	YES	YES	NO	YES	YES

avoid finding a trusted third party. Compared with sampling verification, the hybrid Merkle DAG structure based on the data domain can realize the deterministic verification of multicopy data and improve the efficiency and accuracy of data integrity audits. At the same time, this paper designs an efficient retrieval mechanism for data integrity audit history, realizes efficient retrieval of data integrity verification history and multiparty verification, ensures the consistency of data history, and enhances data credibility. The scheme in this paper does not realize the dynamic modification of data, which reduces data storage flexibility. Still, it can increase the historical consistency of data, which is suitable for data sharing discussed in this paper.

Table 2: Cloud server functions.

Cloud server	User	Feature id
Server1	Do_A	Peer1, Org1, Ca1, Kafka1, Zookeeper1, Orderer1
Server2	Do_B	Peer2, Org2, Ca2, Kafka2, Zookeeper2
Server3	Du_A	Peer3, Org3, Ca3, Kafka3, Zookeeper3, Orderer2
Server4	Du_B	Peer4, Org4, Ca4, Kafka4, Zookeeper4
Server5	Sp_A	Peer5, Org5, Ca5, Kafka5, Zookeeper5, Orderer3
Server6	Sp_B	Peer6, Org6, Ca6, Kafka6, Zookeeper6

5.4. Experimental Detail. In this paper, 6 Alibaba Cloud servers are deployed in the experiment and their functional identifiers are shown in Table 2. Cloud server configuration is Intel Xeon Platinum 8269CY @2.5 GHz processor, 256 GB memory, Ubuntu 16.04 64-bit operating system. We implemented CBC mode 128-bit key AES encryption through Java. It is proved that the metadata generation stage is implemented by go language programming, the concurrency mechanism of go language is used to speed up the calculation speed, and the SHA256 algorithm is used for data digest extraction. Part of the BLS signature verification is implemented through Java's JPBC library. The blockchain part is enforced based on Hyperledger Fabric 2.2. The endorsement strategy of the blockchain system is as follows: (a) the smart contract is installed on the peer nodes in the six servers, and (b) during the blockchain transaction, the peer nodes in the six servers all endorse the marketing.

The proof metadata generation process is similar to the proof generation process. In this paper, the proof metadata generation efficiency is tested. To verify the system's efficiency and the integrity of the small data volume, the data widely exist in the big data environment. The speed of generating proof metadata for the data domain containing a large number of small data was tested by conducting evidence verification efficiency tests.

5.5. Proof of the Metadata Generation Efficiency Test. Figure 5 and Table 3 show a test to demonstrate the efficiency of metadata generation on data with a data volume of 1 to 10 GB. In this test, the number of data copies is 3, the parameter $N_{\max}$ in the multibranch Merkle tree structure is 27, and the data domain-based hybrid Merkle DAG structures with data block sizes of 16 MB, 24 MB, and 32 MB are, respectively, constructed. Finally, Figure 6 shows a test to demonstrate the efficiency of metadata generation on data under 1 GB in Table 4. Again, the number of data copies is 3, the parameter $N_{\max}$ in the multibranch Merkle tree structure is 27, and the data domain-based hybrid Merkle DAG structures with data block sizes of 1 MB, 4 MB, and 8 MB are, respectively, constructed.

It can be seen from the two sets of curves that the same amount of data is processed in blocks of different sizes and the time consumption is the same. In practical applications, the data block size can be determined according to the size of the data volume and actual requirements. It is proved that the time of metadata generation is proportional to the

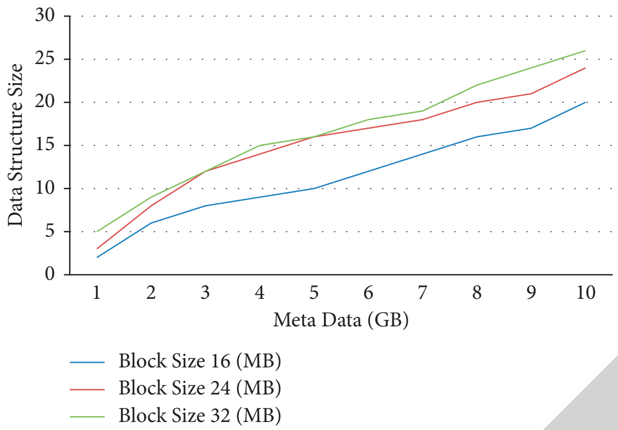

Figure 5: 1–10 GB proof metadata generation test.

Table 3: 1–10 GB proof metadata generation test.

Metadata (GB)	Block size (MB)		
	Block size (16 MB)	Block size (24 MB)	Block size (32 MB)
1	2	3	5
2	6	8	9
3	8	12	12
4	9	14	15
5	10	16	16
6	12	17	18
7	14	18	19
8	16	20	22
9	17	21	24
10	20	24	26

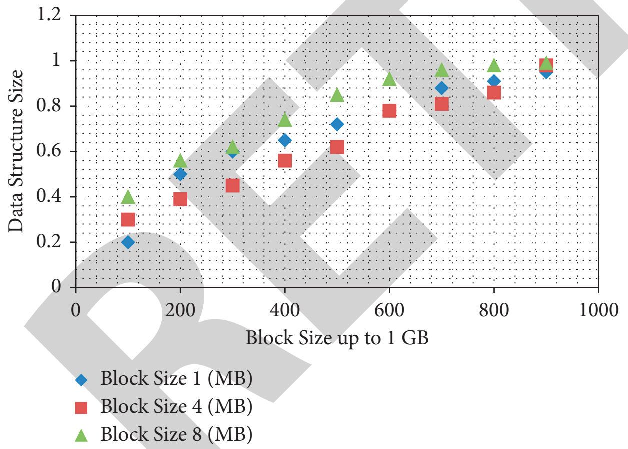

Figure 6: Generating test for attestation of metadata within 1 GB.

amount of data. The balanced relationship between the time consumed and the amount of data is about 1.25 s/GB, and the data processing efficiency is high.

Figure 7 shows a test to prove the efficiency of metadata generation on 1,000 to 10,000 pieces of small unstructured data. The size of unstructured data is about 1 MB, the number of data copies is 3, the parameter in the multibranch Merkle tree structure is 27, and the construction data block is a significant data field-based Merkle DAG file structure as small as 1 MB. It can be seen from the obtained curve that the speed of metadata generation is proportional to the number of data pieces, about 870 pieces per second, and the data processing efficiency is high.

Table 4: Generating test for metadata within 1 GB.

Metadata (MB)	Block size (MB)		
	Block size (1 MB)	Block size (4 MB)	Block size (8 MB)
100	0.2	0.3	0.4
200	0.5	0.39	0.56
300	0.6	0.45	0.62
400	0.65	0.56	0.74
500	0.72	0.62	0.85
600	0.78	0.78	0.92
700	0.88	0.81	0.96
800	0.91	0.86	0.98
900	0.95	0.98	0.99

5.6. Evidence Verification Efficiency Test. Figure 8 shows the efficiency test of the authenticity of evidence for data with a volume of 100–900 MB. It can be seen from the results that the time consumption of the integrity evidence has

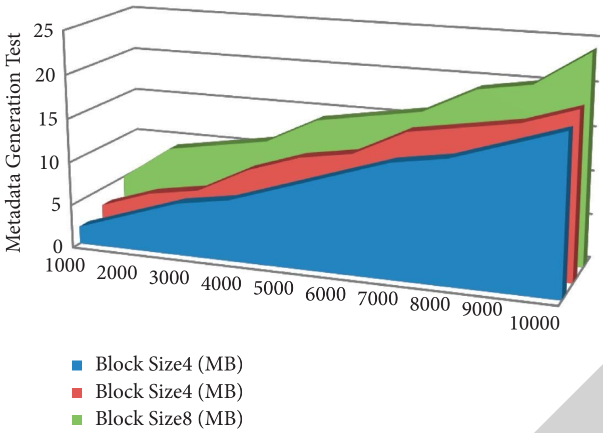

Figure 7: Unstructured small data proof metadata generation test.

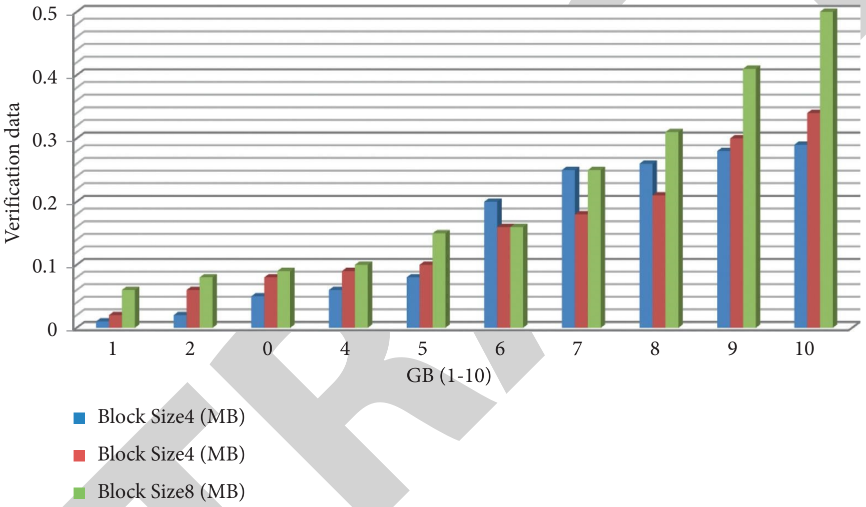

Figure 8: 1 ~ 10 GB data proof verification test.

nothing to do with the size of the data and the time for verifying the authenticity of the evidence is about 40 ms, which can quickly verify the authenticity of the evidence.

5.7. Performance Analysis. The experimental results show that the data integrity proof metadata generation and integrity audit speed are high, which can meet the requirements of data heterogeneity and a large amount of data. It should be noted that the above tests are all performed based on 3 data copies and the time consumed by the test is the time used to perform data integrity certification on the 3 data copies at the same time. Therefore, if you reduce the number of replicas, you will reduce the time consumption proportionally. In actual use, the data owner can select an appropriate number of data copies or not use copy technology according to the importance of the data.

6. Conclusion

According to the data characteristics in the big data environment, this paper builds a multiparty and efficient audit mechanism for data integrity based on blockchain and realizes efficient multicopy audits of small unstructured data and large-volume data. The data integrity audit process is realized through intelligent contracts. The audit history is traced to learn multiparty supervision of the audit process, ensuring historical consistency before data sharing and increasing data credibility. However, the generation of the proof metadata in the scheme of this paper needs to be realized based on generating a random sequence. In future, the work will focus on studying a more flexible proof metadata generation method.

Data Availability

The data used to support the findings of this study is available from the author Aditi Sharma upon request (asharma.csed.cf@ietlucknow.ac.in).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] B. Ravishankar, P. Kulkarni, and M. V. Vishnudas, "Blockchain-based database to ensure data integrity in cloud computing environments," in *Proceedings of the 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI)*, pp. 1–4, Bengaluru, India, February 2020.

[2] A. A. Adekunle and S. R. Woodhead, "On efficient data integrity and data origin authentication for wireless sensor networks utilising block cipher design techniques," in *Proceedings of the 2009 3rd International Conference on Next Generation Mobile Applications*, pp. 419–424, Services and Technologies, Cardiff, UK, September 2009.

[3] L. Zhou, A. Fu, J. Feng, and C. Zhou, "An efficient and secure data integrity auditing scheme with traceability for cloud-based EMR," in *Proceedings of the ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, June 2020.

[4] D. Shen, H. Liu, L. Zhou, and B. Zhang, "Design of trusted aviation data exchange platform based on blockchain," in *Proceedings of the 2020 IEEE 2nd International Conference on Civil Aviation Safety and Information Technology ICCASIT*, pp. 704–708, Weihai, China, Octomber 2020.

[5] A. Terentyev, "Chain of digital data blocks linked by a numeric linear block correction code, as an alternative to the blockchain technology," in *Proceedings of the 2021 14th International Conference Management of large-scale system development (MLSD)*, pp. 1–5, Moscow, Russian Federation, September 2021.

[6] C. Wang, S. Chen, Z. Feng, Y. Jiang, and X. Xue, "Block chain-based data audit and access control mechanism in service collaboration," in *Proceedings of the 2019 IEEE International Conference on Web Services (ICWS)*, pp. 214–218, Milan, Italy, July 2019.

[7] S. Yunling and M. Xianghua, "An Overview of Incremental hash function based on pair block chaining," in *Proceedings of the 2010 International Forum on Information Technology and Applications*, pp. 332–335, Kunming, China, July 2010.

[8] J. Indumathi and A. Shankar, "Block chain based internet of medical things for uninterrupted, ubiquitous, user-friendly, unflappable, unblemished, unlimited health care services (BC IoMT U6 HCS)," *IEEE Access*, vol. 8, pp. 216856–216872, 2020.

[9] C. Rahalkar and D. Gujar, "Content addressed P2P file system for the web with blockchain-based meta-data integrity," in *Proceedings of the 2019 International Conference on Advances in Computing, Communication and Control (ICAC3)*, pp. 1–4, Mumbai, India, December 2019.

[10] S. a. Khan, A. Jadhav, I. e. Bharadwaj, M. Rooj, and S. Shiravale, "Blockchain and the identity based encryption scheme for high data security," in *Proceedings of the 2020 4th International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 1005–1008, Erode, India, March 2020.

[11] A. A. Adekunle and S. R. Woodhead, "Zone based systems design framework for the realisation of efficient block cipher based message authentication code algorithms," in *Proceedings of the 2010 International Conference on Availability, Reliability and Security*, pp. 216–221, Krakow, Poland, February 2010.

[12] R. Aloulou, A. Meddeb-Makhlouf, B. Gassara, and A. Fakhfakh, "Securing a power management chain for Smart Grids," in *Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 1713–1718, Limassol, Cyprus, June 2020.

[13] M. A. Agca, "A holistic abstraction to ensure trusted scaling and memory speed trusted analytics," in *Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 1428–1434, Las Vegas, NV, USA, December 2019.

[14] K. L. S. Priya and C. Rupa, "Block chain technology based electoral franchise," in *Proceedings of the 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, pp. 1–5, Bangalore, India, March 2020.

[15] A. Bhawiyuga, A. Wardhana, K. Amron, and A. P. Kirana, "Platform for Integrating Internet of Things Based Smart Healthcare System and Blockchain Network," in *Proceedings of the 2019 6th NAFOSTED Conference on Information and Computer Science (NICS)*, pp. 55–60, Hanoi, Vietnam, December 2019.

[16] M. Zaid, M. Waheed Akram, N. Ahmed, and S. Saleem, "Web server integrity protection using blockchain," in *Proceedings of the 2019 International Conference on Frontiers of Information Technology (FIT)*, pp. 239–2395, Islamabad, Pakistan, December 2019.

[17] Z. Il-Agure, B. Attallah, and Y.-K. Chang, "The Semantics of Anomalies in IoT Integrated BlockChain Network," in *Proceedings of the 2019 Sixth HCT Information Technology Trends (ITT)*, pp. 144–146, Ras Al Khaimah, United Arab Emirates, November 2019.

[18] M. K. Pawar, P. Patil, M. Sharma, and M. Chalageri, "Secure and scalable decentralized supply chain management using ethereum and IPFS Platform," in *Proceedings of the 2021 International Conference on Intelligent Technologies (CONIT)*, pp. 1–5, Hubli, India, June 2021.

[19] A. Sahi, D. Lai, and Y. Li, "An efficient hash based parallel block cipher mode of operation," in *Proceedings of the 2018 3rd International Conference on Computer and Communication Systems (ICCCS)*, pp. 33–40, Nagoya, Japan, April 2018.

[20] S. Ghimire, J. Y. Choi, and B. Lee, "Using blockchain for improved video integrity verification," *IEEE Transactions on Multimedia*, vol. 22, no. 1, pp. 108–121, 2020.

[21] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–5, Montreal, Canada, Octomber 2017.

[22] V. A. Kanade, "Securing drone-based ad hoc network using blockchain," in *Proceedings of the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, pp. 1314–1318, Coimbatore, India, March 2021.

[23] D. S. Prathiwi, W. Astuti, and T. A. B. Wirayuda, "Watermarking scheme for authenticity and integrity control of digital medical image using reed-muller codes and hash block chaining," in *Proceedings of the 2015 3rd International Conference on Information and Communication Technology (ICoICT)*, pp. 23–29, Nusa Dua, Bali, Indonesia, May 2015.

[24] D. Tyagi, S. Ghosh, A. Rana, and V. Kansal, "A Comparative Analysis of Potential Factors and Impacts that Affect Blockchain Technology in Software: Based Applications," in *Proceedings of the 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, pp. 127–136, Moradabad, India, December 2020.

[25] J. Morrison, "Context integrity measurement architecture: a privacy-preserving strategy for the era of ubiquitous computing," in *Proceedings of the 2016 IEEE 7th Annual*

Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 1–10, New York, NY, USA, Octomber 2016.

[26] T. Mingming, “Research on the application of blockchain technology in accounting information system,” in *Proceedings of the 2020 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*, pp. 330–334, Zhangjiajie, China, July 2020.

[27] B. D. Cahya Putri and R. Fitri Sari, “The effect of latency on selfish-miner attack on block receive time Bitcoin network using NS3,” in *Proceedings of the 2018 12th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, pp. 1–5, Yogyakarta, Indonesia, Octomber 2018.

[28] M. Zhang, H. Zhang, Y. Yang, and Q. Shen, “PTAD:Provable and traceable assured deletion in cloud storage,” in *Proceedings of the 2019 IEEE Symposium on Computers and Communications (ISCC)*, pp. 1–6, Barcelona, Spain, July 2019.

[29] H. Zhu, Y. Wang, X. Hei, W. Ji, and L. Zhang, “A blockchain-based decentralized cloud resource scheduling architecture,” in *Proceedings of the 2018 International Conference on Networking and Network Applications (NaNA)*, pp. 324–329, Xi’an, China, Octomber 2018.