*International Journal on Applications in Engineering and Technology*
*Volume 9 : Issue 2 : April 2023, pp 38 - 44 www.aetsjournal.com* ISSN (Online) : 2455 - 0523

# DATA INTEGRITY AUDIT SCHEME BASED ON BLOCK CHAIN EXPANSION TECHNOLOGY

M. THANGAVEL , R. SUNITHA

***Abstract -*** Increasing numbers of users are outsourcing data to the cloud, but data integrity is an important issue. Due to the decentralization and immutability of blockchain, more and more researchers tend to use blockchain to replace third-party auditors. This paper proposes a data integrity system based on blockchain expansion technology that aims to solve the problem of high cost for blockchain network maintenance and for user creation of new blocks caused by the rapid growth of blocks in the data integrity audit scheme of existing blockchain technology. Users and cloud service providers (CSP) deploy smart contracts on the main chain and sub-chains. Intensive and frequent computing work is transferred to the sub-chain for completion, and the computation results of the sub-chain are submitted to the main chain periodically or when needed to ensure its finality.

The concept of non-interactive audit is introduced to avoid affecting user experience due to the communication with the CSP during the audit process. In order to ensure data security, a reward pool mechanism is introduced. Comprehensive analysis from aspects such as storage, batch auditing and data consistency proves the correctness of the scheme. Experiments on the Ethereum blockchain platform demonstrate that this scheme can effectively reduce storage and computational overhead.

**KEYWORDS:**Blockchain, cloud storage, data auditing, blockchain expansion

## 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 [1].

Despite the great success of cloud storage, it also faces various challenges [2]_[4], and its security, reliability and privacy have always been a serious issue [6], [7]. After the user stores the data on the cloud server, the server provider may damage or delete the user data due to various factors [12], 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 [5], [28]. 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 [16]. 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 [18].

In traditional cloud auditing schemes, there is an entity called auditors (often referred to as third-party auditors, or TPA) which implement public audits [8], [21]. 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

M.Thangavel , Professor , Department of Computer Applications , Erode Sengunthar Engineering College (Autonomous), Perundurai , Erode.

R.Sunitha , PG Scholar , Department of Computer Applications, Erode Sengunthar Engineering College (Autonomous), Perundurai , Erode.

replace third-party auditors [9], [10]. Although the use of block chain as a trusted third-party auditor can well address users' concerns in cloud computing environments, but the rapid growth of blocks will lead to high cost for block chain network maintenance and for user creation of new blocks [17].

To solve the above problems, a data integrity verification scheme based on block chain expansion technology is proposed. By slowing the growth of the block chain, reducing storage and calculation costs. In particular, our contribution can be summarized in three aspects:

1) A data integrity audit protocol based on plasma smart contracts is proposed. By introducing plasma sub-chains and deploying smart contracts on the main chain and sub-chains, the storage pressure of the main chain can be reduced and the growth rate can be slowed down through this protocol. TPA audit protocol can be executed with low computational and communication overhead.
2) A batch auditing scheme is proposed, the scheme can batch-process multiple audit tasks at the same time. In order to avoid affecting the user experience due to the communication with the CSP during the audit process as much as possible, the concept of non-interactive audit is introduced. For the sake of ensuring the correctness of the audit, the reward pool mechanism is adopted, and the verification node can obtain reasonable rewards.
3) An analysis of the security of the scheme shows that it can achieve the expected security objectives. Numerous experiments on the ether block chain also showed the efficiency and effectiveness of the scheme.

This paper is organized as follows: Related work is presented in Chapter 2. The system model and design objectives are described in Chapter 3. The detailed description of the scheme is in Chapter 4. Chapter 5 contains an analysis of the security system. Chapter 6 discusses the performance of this experimental method. Chapter 7 is the conclusion of the paper.

## II. LITERATURE SURVEY:

### *1) Outsourced data integrity verification based on blockchain in untrusted environment*

Outsourced data, as the significant component of cloud service, has been widely used due to its convenience, low overhead, and high flexibility. To guarantee the integrity of outsourced data, data owner (DO) usually adopts a third party auditor (TPA) to execute the data integrity verification scheme. However, during the verification process, DO cannot fully confirm the reliability of the TPA, and handing over the verification of data integrity to the untrusted TPA may lead to data security threats. In this paper, we focus on the problem of integrity verification of outsourced data in untrusted environment, that is, how to improve the security and efficiency of data integrity verification without utilizing untrusted TPA. To address the problem, we design a decentralized model based on blockchain consisting of some collaborative verification peers (VPs), each of which maintains a replication of the entire blockchain to avoid maliciously tampering with. Based on the model, we present an advanced data integrity verification algorithm which allows DO to store and check the verification information by writing and retrieving the blockchain. In addition, in order to improve the concurrent performance, we extend the algorithm by introducing the verification group (VG) constituting by some VPs organized by Inner-Group and Inter-Group consensus protocols. We conduct a completed security analysis as well as extensive experiments of our proposed approach, and the evaluation results demonstrate that our proposed approaches achieve superior performance.

### *2) One secure data integrity verification scheme for cloud storage*

Cloud computing is a novel kind of information technology that users can enjoy sundry cloud services from the shared configurable computing resources. Compared with traditional local storage, cloud storage is a more economical choice because the remote data center can replace users for data management and maintenance, which can save time and money on the series of work. However,

delivering data to an unknown Cloud Service Provider (CSP) makes the integrity of data become a potential vulnerability. To solve this problem, we propose a secure identity based aggregate signatures (SIBAS) as the data integrity checking scheme which resorts Trusted Execution Environment (TEE) as the auditor to check the outsourced data in the local side. SIBAS can not only check the integrity of outsourced data, but also achieve the secure key management in TEE through Shamir's (t,n) threshold scheme. To prove the security, security analysis in the random oracle model under the computational Diffie–Hellman assumption shows that SIBAS can resist attacks from the adversary that chooses its messages and target identities, experimental results also show that our solution is viable and efficient in practice.

### *3) Blockchain Based Data Integrity Verification for Large-Scale IoT Data*

Achieving data integrity verification for large-scale IoT data in cloud storage safely and efficiently has become one of the hot topics with further applications of Internet of Things. Traditional data integrity verification methods generally use encryption techniques to protect data in the cloud, relying on trusted Third Party Auditors (TPAs). Blockchain based data integrity schemes can successfully avoid the trust problem of TPAs, however, they have to face the problems of largecomputational and communication overhead. To address the issues above, we propose a Blockchain and Bilinear mapping based Data Integrity Scheme (BB-DIS) for large-scale IoT data. In our BB-DIS, IoT data is sliced into shards and homomorphic verifiable tags (HVTs) are generated for sampling verification. Data integrity can be achieved according to the characteristics of bilinear mapping in the form of blockchain transactions. Performance analysis of BBDIS including feasibility, security, dynamicity and complexity is also discussed in detail. A prototype system of BB-DIS is then presented to illustrate how to implement our verification scheme. Experimental results based on Hyperledger Fabric demonstrate that the proposed verification scheme significantly improves the efficiency of integrity verification for large-scale IoT data with no need of TPAs.

### *4) Secure Outsourced Blockchain-Based Medical Data Sharing System Using Proxy Re-Encryption*

The security and privacy of electronic health records (EHRs) have received considerable attention from healthcare workers and researchers. To ensure security, various encryption and decryption schemes as well as key management protocols have been developed. However, owing to sharing and scalability issues, additional security technologies have been proposed. Nonetheless, these technologies cause other problems, such as efficiency issues. Blockchain-based EHR management systems have been proposed to overcome computational overhead. However, because most blockchain systems are installed by outsourcing companies, EHRs may be leaked to the company. Hence, we herein propose a blockchain-based EHR management scheme with proxy re-encryption. In this scheme, we set a proxy server that re-encrypts the ciphertext between file servers, thereby solving EHR sharing issues. Furthermore, because the server is separated from the blockchain system, the outsourcing company cannot manipulate the server or access the records. In addition, the blockchain assists in access control by using smart contracts, thereby enabling secure and efficient EHR sharing. By performing security analysis, we prove that our proposed scheme solves the aforementioned security problems. In addition, we experimentally demonstrate the efficient operation of the proposed system.

### *5) A Blockchain-Based Flexible Data Auditing*

### *Scheme for the Cloud Service*

Nowdays, cloud storage technology has become a hot topic, and an increasing number of users are concerned with the security of their data in the cloud. Many auditing schemes on the cloud are proposed and the introduction of a third-party auditor to assist users in verifying the integrity of cloud data. As a centralized node, the third-party auditor has to communicate with all cloud users and

cloud service providers, which becomes the bottleneck of the whole scheme. To solve this problem, we design a blockchain-based flexible cloud data auditing scheme. In our scheme, a decentralized auditing framework is proposed to eliminate the dependency on the thirdparty auditor, which increases the stability, security and performance of the whole scheme. Since the cloud service provider can automatically generates auditing proofs, our scheme can relieve the communication burdens of the cloud service provider. The proposed scheme also adapts the Merkle Hash tree to improve the verification performance. Security analysis and experiments show that the proposed scheme is secure and has better stability and verification efficiency.

## III. EXISTING SYSTEM

Fan *et al.* zhe'ge [11] 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.* [13] 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.* [20] 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.* [24] proposed a deduplication scheme with public audit and fair arbitration.

Zhou *et al.* [26] 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.

**Disadvantages**

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

## IV. PROPOSED SYSTEM

1) In the proposed system, A data integrity audit protocol based on plasma smart contracts is proposed. By introducing plasma sub-chains and deploying smart contracts on the main chain and sub-chains, the storage pressure of the main chain can be reduced and the growth rate can be slowed down through this protocol. TPA audit protocol can be executed with low computational and communication overhead

2) In the proposed system, A batch auditing scheme is proposed, the scheme can batch-process multiple audit tasks at the same time. In order to avoid affecting the user experience due to the communication with the CSP during the audit process as much as possible, the concept of non-interactive audit is introduced. For the sake of ensuring the correctness of the audit, the reward pool mechanism is adopted, and the verification node can obtain reasonable rewards.

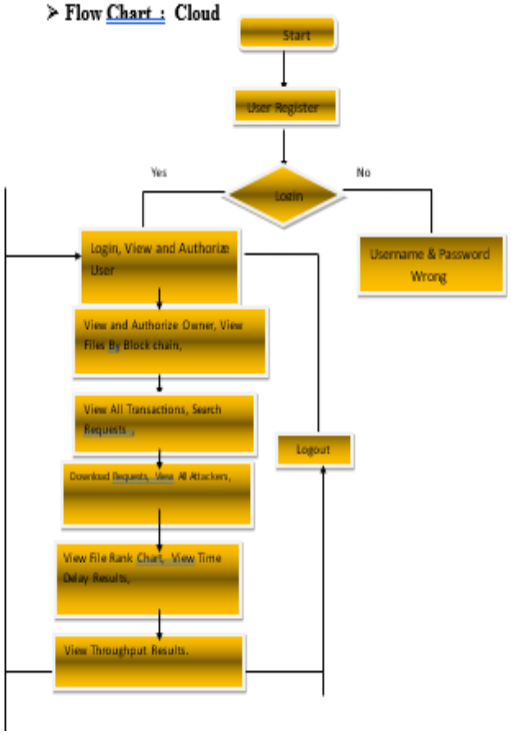
3) In the proposed system, An analysis of the security of the scheme shows that it can achieve the expected security objectives. Numerous

experiments on the ether block chain also showed the efficiency and effectiveness of the scheme.

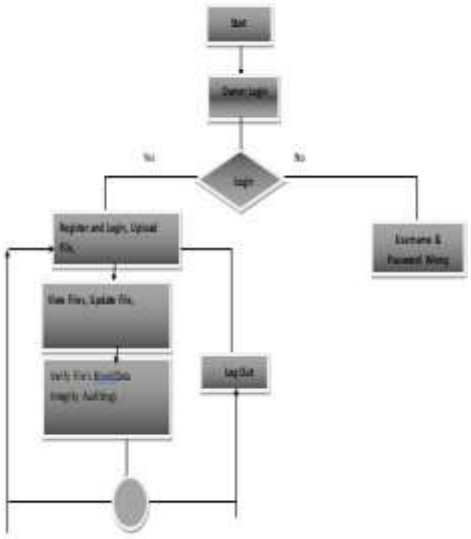
## Advantages

- 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.

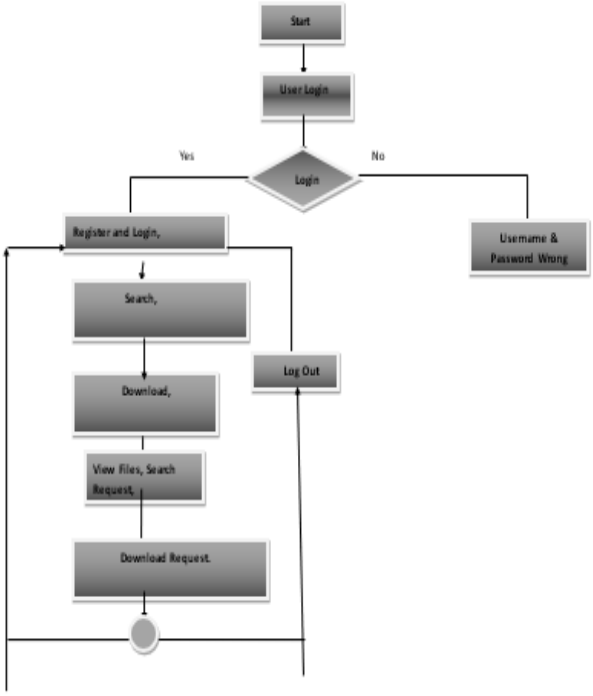
➢ Flow Chart : Cloud

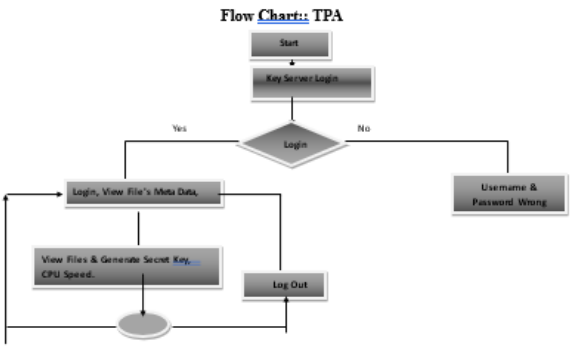


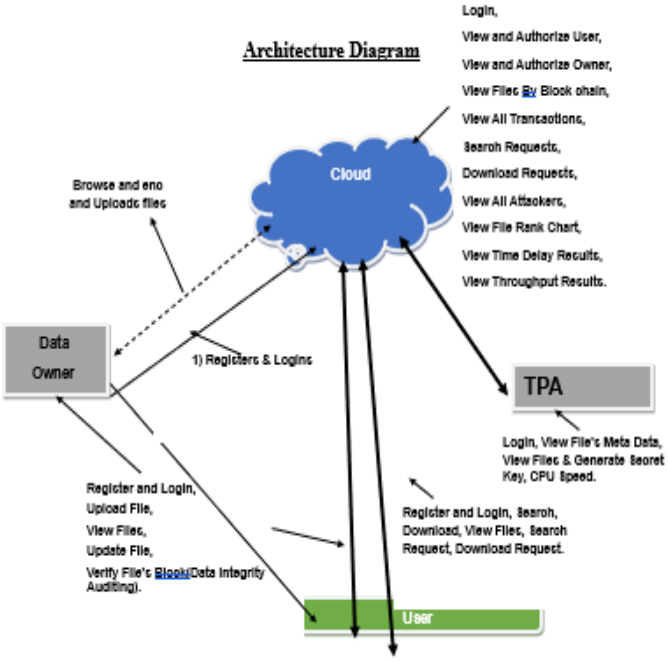

Flow Chart: Data Owner



Flow Chart: User






## V. CONCLUSION

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.

## VI. REFERENCES

[1] K. Hao, J. Xin, Z. Wang, and G. Wang, ``Outsourced data integrityveri_cation based on blockchain in untrusted environment," *World Wide Web*, vol. 23, no. 4, pp. 2215_2238, Jul. 2020.

[2] Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong, and J. Lei, ``One secure data integrity veri_cation scheme for cloud storage," *Future Gener. Comput.Syst.*, vol. 96, pp. 376_385, Jul. 2019.

[3] H. Wang and J. Zhang, ``Blockchain based data integrity veri_cation for large-scale IoT data," *IEEE Access*, vol. 7, pp. 164996_165006, 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,"in *Proc. 4th Int. Conf. Blockchain Technol. Appl.*, Dec. 2021, pp. 11_16.

[5] F. Kefeng, L. Fei, Y. Haiyang, and Y. Zhen, ``A blockchain-base exible data auditing scheme for the cloud service," *Chin. J. Electron.*, vol. 30, no. 6, pp. 1159_1166, Nov. 2021.

[6] K. He, J. Shi, C. Huang, and X. Hu, ``Blockchain based data integrity veri_cation for cloud storage with T-Merkle tree," in *Proc. Int. Conf. Algorithms Archit. Parallel Process.* Cham, Switzerland: Springer, Oct. 2020 pp. 65_80.

[7] Y. 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.

[8] 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

[9] S. Wang, D. Zhang, and Y. Zhang, ``Blockchain-based personal health records sharing scheme with data integrity veri_able," *IEEE Access*, vol. 7, pp. 102887_102901, 2019.

[10] A. Liu, Y. Wang, and X. Wang, ``Blockchain-based data-driven smart customization," in *Data-Driven Engineering Design*. Cham, Switzerland: Springer, 2022, pp. 89_107.

[11] K. Dhyani, J. Mishra, S. Paladhi, and I. S. Thaseen, ``A blockchai based document veri_cation system for employers," in *Proc. Int. Conf. Comput. Intell. Data Eng.* Singapore: Springer, 2022, pp. 123_137.

[12] K. Xu, W. Chen, and Y. Zhang, ``Blockchain-based integrity verication of data migration in multi-cloud storage," *J. Phys., Conf. Ser.*, vol. 2132, no. 1, Dec. 2021, Art. no. 012031.

[13] G. Xu, S. Han, Y. Bai, X. Feng, and Y. Gan, ``Data tag replacement algorithm for data integrity veri_cation in cloud storage," *Comput. Secur.*,vol. 103, Apr. 2021, Art. no. 102205.

[14] G. Xie, Y. Liu, G. Xin, and Q. Yang, ``Blockchain-based cloud data integrity veri_cation scheme with high ef_ciency," *Secur. Commun. Netw.*,vol. 2021, pp. 1_15, Apr. 2021.

[15] U. Arjun and S. Vinay, ``Outsourced auditing with data integrity veri_cation scheme (OA-DIV) and dynamic operations for cloud data with multi-copies," *EAI Endorsed Trans. Cloud Syst.*, vol. 7, no. 20, Jul. 2018, Art. no. 169423.

[16] A. V. Ezhil, G. K. Indra, and K. Kulothungan, ``Auditable attribute-based data access control using blockchain in cloud storage," *J. Supercomput.*,vol. 78, pp. 10772_10798, 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 ef_cient user revocation," *Cluster Comput.*, pp. 1_25, Jan. 2022.

[18] X. Tao, Y. Liu, P. K.-Y. Wong, K. Chen, M. Das, and J. C. P. Cheng, ``Con_dentiality-minded framework for blockchain-based BIM design collaboration," *Autom. Construct.*, vol. 136, Apr. 2022, Art. no. 104172.

[19] P.Wei, D.Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, ``Blockchain data-based cloud data integrity protection mechanism," *Future Gener. Comput.Syst.*, vol. 102, pp. 902_911, 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," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 289_300, Mar. 2020.

[21] H. Yu, Z. Yang, and R. O. Sinnott, ``Decentralized big data auditing for smart city environments leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 6288_6296, 2019.

[22] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ``Privacy-preserving public auditing for secure cloud storage," *IEEE Trans.Comput.*, vol. 62, no. 2, pp. 362_375, Feb. 2013.

[23] L. Chen, Q. Fu, Y. Mu, L. Zeng, F. Rezaeibagha, and M.-S. Hwang,``Blockchain-based random auditor committee for integrity veri_cation," *Future Gener. Comput. Syst.*, vol. 131, pp. 183_193, Jun. 2022.

[24] H. Yuan, X. Chen, J. Wang, J. Yuan, H. Yan, and W. Susilo, ``Blockchain- based public auditing and secure deduplication with fair arbitration," *Inf Sci.*, vol. 541, pp. 409_425, Dec. 2020.

[25] C. Yang, Y. Liu, F. Zhao, and S. Zhang, ``Provable data deletion from ef_cient data integrity auditing and insertion in cloud storage," *Comput. Standards Interface*, vol. 82, Aug. 2022, Art. no. 103629.