Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2022.026934
Article

Tech Science Press

Security Data Sharing of Shipbuilding Information Based on Blockchain

Jun Zhu[1,*], Chaosong Yan[2], Yinglong Ouyang[3], Yao Chen[4] and Xiaowan Wang[5]

[1]School of Computer Science and Technology, Harbin Engineering University, Heilongjiang, 150001, China
[2]Olin Business School, Washington University in St. Louis, St. Louis, 63130, Missouri, USA
[3]China Minsheng Banking Corp., Beijing Xicheng District, 100621, China
[4]Wuxi University, Wuxi, 214105, China
[5]Xi'an University of Posts & Telecommunications, Xi'an, 710061, China
*Corresponding Author: Jun Zhu. Email: zhujun15121869283@163.com
Received: 07 January 2022; Accepted: 11 February 2022

Abstract: The shipbuilding industry has problems such as long transaction cycles, many participating suppliers, and data sensitivity. A time-dimensional shipbuilding information security sharing scheme based on an alliance chain is proposed to solve this problem. The blockchain can better deliver value and protect user privacy, the blockchain can directly complete the instant transfer of value through smart contracts and tokens on the blockchain. We divide the program into three parts: data preprocessing, data storage, and data sharing. For data sensitivity, data confidentiality and reliability are handled separately. Aiming at the problem of user privacy leakage in data storage, a privacy-protecting blockchain shared storage solution is proposed; for deduplication, two deduplication algorithms between storage nodes and within storage alliances are proposed to ensure Data information is not disclosed. Storage nodes are allowed to perform data deduplication, data sharing and down-loading, and use off-chain transactions to solve the blockchain performance problems caused by frequent transactions. The scheme in this paper carries out theoretical analysis from three aspects of correctness, security and performance. Finally, this paper has carried out a comparative experimental analysis on the scheme, and the experimental results show that the proposed scheme is feasible and efficient.

Keywords: Blockchain; data sharing; shipbuilding

1 Introduction

In actual work, due to the design of multiple platforms for manufacturing equipment and information systems, it is difficult to collect information such as demand collection and status tracking, which seriously affects the efficiency of interconnection and interoperability and restricts the application of intelligent manufacturing. Traditional ship design and manufacturing enterprise information systems often have problems such as low transparency and low efficiency. These problems potentially affect the final time of ship delivery and acceptance and the life cycle of products. The critical task of improving the cooperation efficiency of related enterprises in the ship design and manufacturing industry is to realize

the vertical integration of the manufacturing industry's internal systems. And the horizontal integration of value chain and information flow between different manufacturing and design companies to realize the intelligent interconnection of manufacturing plants and design companies. The traditional information system in the design and manufacturing industry does not have collating and in-depth mining of the effectively collected data. These tasks often rely on critical employees familiar with the business and a leadership team with constructive thinking. Through blockchain technology and extensive data analysis, these tasks can be evaluated to effectively establish an evaluation model for enterprises' high-quality development and help enterprises efficiently locate problems in cooperation.

The ship design and manufacturing industry have an increasingly urgent demand for information construction. The establishment of intelligent factories and design institutes' interconnection has become the top priority of high-quality products in the ship design manufacturing industry. Blockchain technology uses P2P storage architecture and hybrid communication protocols to realize crossplatform information interconnection efficiently. Blockchain technology plays a vital role in high-quality production because of its efficient way of storing data and its inability to tamper with data. For example, in the traditional production model, the operation, production, and maintenance of equipment are often recorded in isolated systems. Once a production accident occurs, it is difficult for the relevant departments to ensure the records' authenticity and consistency, and it is impossible to establish relevant plans for accidents. Make improvements. By introducing blockchain technology, the cost of discovering, tracking, and solving problems can be significantly reduced, and at the same time, the performance and business level of all units in the blockchain can be evaluated more effectively.

Although the blockchain has many revolutionary advantages and shows considerable development potential in the shipbuilding industry, there are still many shortcomings in the direct application of blockchain technology in the shipbuilding industry. All aspects of ship design and manufacturing usually involve the enterprise's confidential information, and the direct use of distributed storage will bring about the risk of leakage. Therefore, leaks have become a vital obstacle preventing companies from getting on the chain.

Shipbuilding enterprise cooperative alliances inevitably involve issues, such as profit distribution and resource allocation. The distribution of enterprise cooperative alliances' interests and resources needs to be based on sensitive data such as output and sales. The centralized storage of these sensitive data related to enterprises' interests and cooperative alliances may lead to data loss, tampering, and forgery, leading to inconsistent negotiation and uneven distribution of benefits due to inconsistent data during the subsequent distribution of alliance benefits. To solve enterprise data storage security, academic researchers from all walks of life have successively invested in innovative research and proposed many solutions, such as encrypting data through symmetric encryption technology and asymmetric encryption technology accessing data through user passwords and dynamic verification codes. Time identity verification, data backup, and recovery through corresponding security backup software, but these solutions only involve the storage security of individual enterprise data and are not enough to solve the alliance data storage security problem in the enterprise cooperative alliance model.

For the cloud manufacturing service platform, its main body is composed of enterprises distributed in different geographical areas, and the related business is relatively loose. The technical level, service level, performance ability, and financial strength of the enterprise are uneven, and each participant's information in each link is scattered. Lack of mutual trust, the authenticity, reliability, and integrity of information are not easy to guarantee [1,2]. Besides, different tasks have different trust and security requirements for manufacturing service resources. For example, tasks involving confidential commercial data have higher security requirements, and service resources also have different credibility according to their service reputation and service mode differences. Therefore, a reliable trust mechanism play a highly critical role in the cloud manufacturing service platform's regular operation. In information systems, the relevant

theories of trust evaluation have achieved many research results [3,4]. Bo [5] established a reputation evaluation framework based on the two dimensions of reputation and collaboration. The trust in virtual group pairs is divided into two parts: reputation and cooperation trust. They proposed a fuzzy multi-attribute based on a binary fuzzy language representation—decision analysis method to evaluate virtual team pairs' complete trust. Ren et al. [6] combined the existing direct and indirect (recommended) trust evaluation model and the third-party trust evaluation model to solve the lack of objectivity of the direct and indirect trust model. Ge et al. [7] aimed at the subjectivity, ambiguity, and uncertainty of trust, using fuzzy mathematics and probability theory, gave the mathematical definition of trust, and established trust, including comprehensive trust evaluation trust calculation.

Wang [8] established a trust evaluation model based on the historical service information of cloud resource providers from the four quality of service (Quality of Service, QoS) parameters: availability, reliability, turnover efficiency, and data integrity, and proposed a way to achieve this. Trust management system of trust model. Li et al. [9] introduced a third-party expert group's trust evaluation, integrated subjective trust, and objective trust into the trust evaluation process, combined a dynamic hierarchical fuzzy system and trust evaluation, and proposed a multi-attribute fuzzy trust suitable for cloud manufacturing environments. They evaluated the access control plan. Fang et al. [10] gave a trust chain discovery algorithm considering the storage of credentials and authorization to prevent the leakage of adequate sensitive information. In summary, existing research provides an excellent theoretical basis for solving the problem of trust evaluation of business entities brought about by the cloud manufacturing service model's technical characteristics, such as remote services and distributed collaborative services.

Therefore, this article aims at the information encryption processing of the alliance chain and proposes a blockchain-based shipbuilding information security sharing scheme for the current innovation and development of the shipbuilding industry's production organization model. A time-dimensional shipbuilding information security sharing scheme based on an alliance chain is proposed to solve this problem. We divide the program into three parts: data preprocessing, data storage, and data sharing. For internal attacks and external attacks, data confidentiality and reliability are handled separately, and storage nodes are allowed to perform data deduplication, and data sharing and downloading through off-chain transactions solve the blockchain performance problems caused by frequent transactions.

2 Related Work

The proposal and development of blockchain technology provides a new idea for designing storage systems-a decentralized shared storage system based on blockchain. The concept of blockchain was first proposed by Zhang in 2008 [11]. The blockchain solves the double-spending problem and the Byzantine problem by combining technologies such as Merkle trees, asymmetric encryption, consensus mechanism, and time stamping. And it has the characteristics of decentralization, trustlessness, traceability, and non-tamperability. At the same time, based on the blockchain technology, Nakamoto designed a decentralized digital currency transaction system-Bitcoin in the paper, and achieved great success, which has attracted widespread attention from academia and industry.

In recent years, the blockchain technology has achieved considerable development, has been widely used in all walks of life, and a large number of very successful systems have emerged. In 2014, the proposal of Ethereum greatly enriched the application fields and application scenarios of blockchain [12]. Ethereum is an open-source public blockchain platform that provides users with a decentralized Ethereum virtual machine. Users can easily deploy smart contracts on Ethereum and develop their own blockchain applications quickly and conveniently. In the storage field, some very successful blockchain projects have also appeared, such as Sia [13], Metadisk [14], Filecoin [15], Storj [16], YottaChain [17] and Filenet [18].

Sia [13] is an open source decentralized shared storage platform. Users and storage providers sign a contract, and then store the contract on the blockchain, and the contract restricts the behavior of both parties. By signing the contract, the storage provider is responsible for storing the customer's data and providing storage certification on a regular basis to ensure data integrity and availability. By providing storage certification, the storage provider can obtain token rewards until the end of the contract. However, Sia did not consider the issue of data security, nor did it consider the issue of data deduplication, so there are security and storage efficiency issues.

Metadisk [14] and Storj [16] are blockchain shared storage systems based on Ethereum. There is no centralized cloud service provider in the system to provide data storage services. Instead, users in the network sell their free hard disk space to the network to form a public storage market for data owners. Such users are called: Storage provider. When the data owner wants to upload a file, the data owner encrypts and divides the file locally, and then uploads it to the storage provider in a distributed manner. In order to prevent data unavailability caused by equipment failure, the system provides a redundancy strategy, that is, while storing files, a certain amount of file backups is stored. In addition, the system introduces the blockchain into the distributed storage system and uses the characteristics and technologies of the blockchain such as decentralization, immutability, and smart contracts to further increase the security of the system.

Filecoin [15] is a decentralized storage network, which complements Interplanetary file system (IPFS) [19]. IPFS provides storage services for Filecoin, and Filecoin provides token incentives for IPFS, encouraging users to provide storage resources for the IPFS system. The Chinese translation of IPFS is" Interplanetary File System", which is a peer-to-peer (P2P) distributed file system. The IPFS protocol defines how files are stored, indexed, and transmitted in a distributed system, enabling permanent and decentralized storage and sharing of files. The IPFS+Filecoin system improves system efficiency and reduces system costs.

YottaChain [17] inherited the existing storage design of IPFS, added data security mechanisms, and used zero-knowledge encryption to encrypt files, ensuring that only the data owner can know the contents of the stored data files. On the basis of zero-knowledge encryption, YottaChain implements data deduplication on stored files, saves storage space, and increases the utilization rate of storage space. In addition, YottaChain has designed and implemented a file permission system and authorization mechanism to ensure that only authorized persons can open files.

Filenet [15] is an incentive layer built on the IPFS protocol, and its goal is to create a low-cost and high efficiency decentralized data storage network. Filenet provides a data promotion system that allows users to obtain storage space to store and retrieve data without paying fees [20]. When the data is retrieved more times, the data will gradually enter the public network and become popular data, and this data can participate in mining.

In summary, the decentralized shared storage system overcomes the shortcomings of the centralized storage system to a certain extent. It reduces the cost of data storage by using idle resources [21]. At the same time, it stores multiple data backups in the system through a data redundancy mechanism. Ensure the reliability of user data. However, the current popular decentralized shared storage systems, such as Sia, Metadisk, Filecoin, Storj, YottaChain and Filenet, are all developed based on public chains [22]. Yes, the data in the blockchain is open and transparent, and anyone can obtain the data in the block. The data in these blockchains includes data summary information, transaction information, user address information, etc., and attackers can obtain user privacy information by analyzing this public information [23]. Therefore, the current blockchain shared storage system has privacy leakage problems. In addition, in Sia, IPFS and Filenet systems, no file encryption measures are taken, so there are data security issues [24].

3 Secure Data Sharing Scheme

3.1 Design Goals

Due to the dynamic and open nature of the shared storage system, data loss, data damage, and data leakage problems will be caused. Simultaneously, because the blockchain data is publicly readable, it will cause the leakage of user and storage node identity information and data information. Besides, the existing shared storage solution's payment system and storage system are highly coupled, and there are problems of difficulty in expansion and compatibility.

In order to overcome the problems mentioned above, the design goals of this project are as follows:

- Coupling: Decouple the storage system and payment system to improve system scalability and compatibility.
- Reliability: When the storage node is randomly offline or fails, the probability of data loss is extremely low.
- Deduplication: In the case of data encryption, the storage node can identify and delete duplicate data.
- Protection: In the process of data upload, download, and deduplication, users and storage nodes will not expose any data information and accurate identity information.

3.2 System Model

The blockchain shared storage system realizes the sharing of storage resources and bandwidth resources through the p2p network without a central server. As shown in Fig. 1, the shipbuilding blockchain shared storage system model includes three types of nodes: storage nodes, alliance company query nodes, and blockchain nodes.

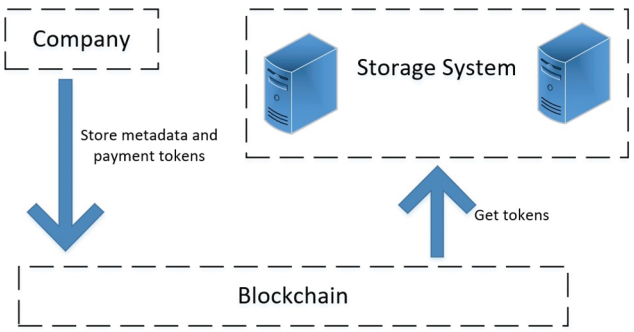

Figure 1: System model

3.3 Data Sharing Scheme Based on Threshold Secret Sharing and Authentication Protocol

Multiple users participating in data sharing, that is, multiple nodes (set to n), can generate the system private key in the following distributed way.

(1) Each node participating in data sharing randomly selects a number $x_i \in Z_q^*$ and a polynomial with order $t-1$.

$$f_i(z) \equiv x_i + a_{i,1}z + a_{i,2}z^2 + \cdots + a_{i,t-1}z^{t-1} \bmod l \tag{1}$$

Obviously, there is the following formula.

$$x_i = f_i(0) \tag{2}$$

(2) Each node participating in data sharing calculates the following formulas.

$$S_{i,j} = f_i(j) \tag{3}$$

And the $S_{i,j}$ is safely sent to another node in the blockchain.

(3) The system private key can be obtained by the following formula.

$$q = \sum_{i=1}^{n} x_i \tag{4}$$

Authentication Protocol of Node

Any node that wants to join the blockchain network can join the network through the following authentication protocol.

(1) Node u randomly selects a random number r_1, and then computes the following signature.

$$y_1 = Sig_U(V,\ r_1) \tag{5}$$

(2) Node u sends its own implicit certificate (IC_U, r_1) and y_1 to the management node v.

(3) The management node v uses certificate to verify the public key of node U.

(4) The management node v verifies whether the signature y_1 is valid.

(5) If the signature y_1 is correct, the authentication of node u is completed. After authentication, the node u can join the network.

4 Experiment

Based on theoretical analysis and performance analysis, this section is based on the klauspost [25] erasure code library, go crypto [26] cryptographic library, go pbc [27] library, and web3.js [28] library for privacy protection. The blockchain shared storage solution was implemented. The solution is mainly written in Golang language, using Truffle [29] suite to build a private Ethereum environment, using Solidity language to write smart contracts and two languages, go and nodejs, interact through the RPC protocol. The specific cryptographic algorithms and parameters used in the implementation of the scheme are as follows:

- The hash function uses SHA256.
- The encryption uses AES 128.
- The Bloom filter false detection rate is set to 10-4.
- The erasure code parameter is set to (32, 16), which means The data is encoded into 32 data blocks, and any more than 16 data blocks can restore the original data.

The software environment of this experiment is: 64-bit Windows 10 Professional operating system, Golang language version is 1.12.1 x64, development environment is Visual Studio Code, blockchain platform is Ethereum private chain, Truffle version is 5.0 .9, Node version is 10.15.3; hardware environment is: Advanced Micro Devices(AMD) A10-5800 K processor, clocked at 3.8 GHz, 8GB dual-channel memory, frequency is 1600 MHz, Micron BX500 series 240G solid-state hard drive, the interface type is SATA3, sequential reading The writing speed is 540 and 500 MB/s respectively.

To better evaluate the program's performance, this section analyzes the privacy protection-oriented blockchain shared storage program's performance in the three stages of data preprocessing, data storage, and data deduplication through experiments and compared it with other related programs [30]. The experimental results as shown in Fig. 2.

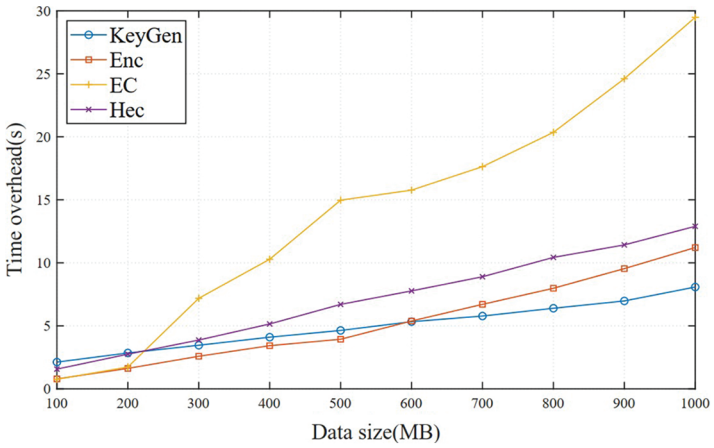

Figure 2: Comparison of influence of node reliability on data reliability

Fig. 2 shows the computational time overhead of each step of data preprocessing for different sizes of data. Among them, KeyGen represents the execution time of the key generation algorithm, Enc represents the execution time of data encryption, EC represents the execution time of erasure code encoding, and Hec represents the time required to calculate the hash of 32 code blocks [31]. The experimental results show that with the increase of data, the time overhead increases almost linearly, and the calculation delay is negligible relative to the network delay of transmitting data. In algorithm execution, EC is the most time-consuming operation [32]. It takes 29.5 s to encode 1000 MB of data, and other operations take about 10 s. These time overheads are mainly limited by the reading and write rate of the hard disk. The calculation time of the slow hash function in the KeyGen operation is constant, about 1.5 s, so it can effectively increase the data's difficulty being attacked by the offline dictionary.

Fig. 3 compares the influence of node reliability on data reliability under different redundancy modes. As the reliability of storage nodes increases, the reliability of data stored through erasure code redundancy and triple-copy redundancy also increases. However, the increase in reliability of data stored through erasure code redundancy is higher than that of the three-copy redundancy method. For example, when the node reliability is 0.9, the data reliability of redundant storage using three copies is 99.9%, and the reliability of data redundant storage using erasure codes is 99.99999987%. However, in practical applications, data reliability of 99.9% is far from enough, but when the node reliability is 0.3, triple copy redundancy is 64.32% higher than that of erasure code redundancy. Therefore, low-reliability nodes can be used to store duplicate data, which improves data response time and makes full use of the storage and bandwidth resources of low-reliability nodes.

Fig. 4 compares this paper's gas consumption and the YottaChain [18] scheme in the data storage phase. It can be seen from the figure that the gas consumption of the two schemes increases linearly with the increase of the number of uploaded files [33]. However, this scheme's increase in gas consumption is much lower than that of YottaChain. The reason is that this solution only saves the Bloom filter on the blockchain during data storage, thus avoiding saving all data summary information on the blockchain. However, due to the Bloom filter's preset bit array, the gas consumption when uploading a small amount of data will be slightly higher than that of the YottaChain solution.

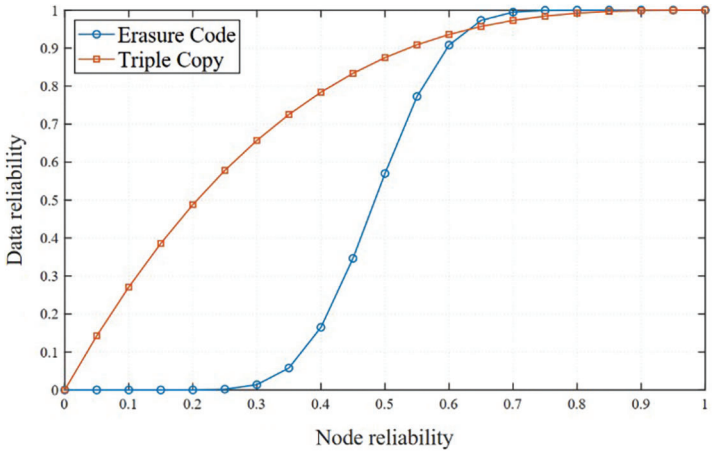

Figure 3: Computational overhead of data of different sizes during data preprocessing

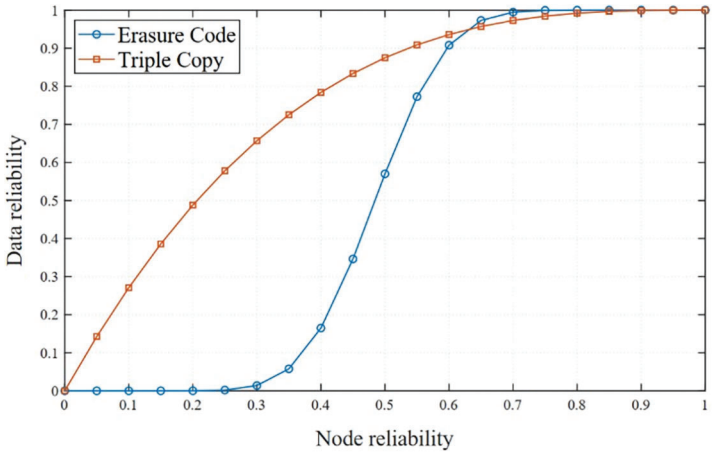

Figure 4: Comparison of gas consumption of different schemes during data upload

5 Conclusion

To solve the problem of massive data storage and privacy protection, this chapter designs a privacy protection-oriented blockchain shared storage scheme. Given users' privacy leakage in data storage, a privacy-protecting blockchain shared storage solution is proposed; in response to data deduplication, two deduplication algorithms between storage nodes and within storage alliances are proposed so that no data information is required to be leaked. The situation achieves data deduplication. Then, theoretically analyze the scheme from three aspects of correctness, safety, and performance. Finally, a comparative experimental analysis of the scheme was carried out, and the experimental results verified the feasibility and effectiveness of the proposed scheme.

Funding Statement: This work was supported in part by the National Natural Science Foundation of China under Grant 62072249. Yao Chen received the grant and the URLs to sponsors' websites is https://www.nsfc.gov.cn/.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] F. Tao, Y. Cheng, L. Zhang and A. Y. Nee, "Advanced manufacturing systems: Socialization characteristics and trends," *Journal of Intelligent Manufacturing*, vol. 28, no. 5, pp. 1079–1094, 2017.

[2] J. Li, F. Tao, Y. Cheng and L. Zhao, "Big data in product lifecycle management," *The International Journal of Advanced Manufacturing Technology*, vol. 81, no. 1, pp. 667–684, 2015.

[3] Z. -P. Fan, W. -L. Suo, B. Feng and Y. Liu, "Trust estimation in a virtual team: A decision support method," *Expert Systems with Applications*, vol. 38, no. 8, pp. 10240–10251, 2011.

[4] K. Yan, Y. Cheng and F. Tao, "A trust evaluation model towards cloud manufacturing," *The International Journal of Advanced Manufacturing Technology*, vol. 84, no. 1–4, pp. 133–146, 2016.

[5] L. Bo, "Access control oriented quantified trust degree representation model for distributed systems," *Journal on Communications*, vol. 31, no. 12, pp. 45, 2010.

[6] Y. J. Ren, K. Zhu, Y. Q. Gao, J. Y. Xia, S. Zhou *et al.,* "Long-term preservation of electronic record based on digital continuity in smart cities," *Computers, Materials & Continua*, vol. 66, no. 3, pp. 3271–3287, 2021.

[7] C. P. Ge, W. Susilo, J. Baek, Z. Liu, J. Y. Xia *et al.,* "A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 7, pp. 1–12, 2021.

[8] J. Wang, C. Y. Jin, Q. Tang, N. X. Xiong and G. Srivastava, "Intelligent ubiquitous network accessibility for wireless-powered MEC in UAV-assisted B5G," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 2801–2813, 2021.

[9] T. Li, W. D. Xu, L. N. Wang, N. P. Li, Y. J. Ren *et al.,* "An integrated artificial neural network-based precipitation revision model," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 5, pp. 1690–1707, 2021.

[10] L. M. Fang, M. H. Li, Z. Liu, C. T. Lin, S. L. Ji *et al.,* "A secure and authenticated mobile payment protocol against off-site attack strategy," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 2, pp. 1–12, 2021.

[11] X. R. Zhang, W. F. Zhang, W. Sun, X. M. Sun and S. K. Jha, "A robust 3-D medical watermarking based on wavelet transform for data protection," *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.

[12] P. Manuel, "A trust model of cloud computing based on quality of service," *Annals of Operations Research*, vol. 233, no. 1, pp. 281–292, 2015.

[13] Y. J. Ren, J. Qi, Y. P. Liu, J. Wang and G. Kim, "Integrity verification mechanism of sensor data based on bilinear map accumulator," *ACM Transactions on Internet Technology*, vol. 21, no. 1, pp. 1–20, 2021.

[14] Y. J. Ren, Y. Leng, Y. P. Cheng and J. Wang, "Secure data storage based on blockchain and coding in edge computing," *Mathematical Biosciences and Engineering*, vol. 16, no. 4, pp. 1874–1892, 2019.

[15] J. Wang, H. Han, H. Li, S. He, P. K. Sharma *et al.,* "Multiple strategies differential privacy on sparse tensor factorization for network traffic analysis in 5G," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1939–1948, 2022.

[16] T. Li, Q. Qian, Y. J. Ren, Y. Z. Ren and J. Y. Xia, "Privacy-preserving recommendation based on kernel method in cloud computing," *Computers, Materials & Continua*, vol. 66, no. 1, pp. 779–791, 2021.

[17] C. P. Ge, Z. Liu, J. Y. Xia and L. M. Fang, "Revocable identity-based broadcast proxy re-encryption for data sharing in clouds," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1214–1226, 2021.

[18] X. R. Zhang, X. Sun, X. M. Sun, W. Sun and S. K. Jha, "Robust reversible audio watermarking scheme for telemedicine and privacy protection," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.

[19] Y. J. Ren, F. Zhu, J. Wang, P. Sharma and U. Ghosh, "Novel vote scheme for decision-making feedback based on blockchain in internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 8, pp. 1–10, 2021.

[20] C. P. Ge, W. Susilo, Z. Liu, J. Y. Xia, L. M. Fang *et al.,* "Secure keyword search and data sharing mechanism for cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 6, pp. 2787–2800, 2021.

[21] Y. J. Ren, F. J. Zhu, S. P. Kumar, T. Wang, J. Wang *et al.,* "Data query mechanism based on hash computing power of blockchain in internet of things," *Sensors*, vol. 20, no. 1, pp. 1–22, 2020.

[22] V. Buterin, "A Next-generation smart contract and decentralized application platform," *White Paper*, vol. 3, no. 37, pp. 1, 2014.

[23] D. Moody, R. Peralta, R. Perlner, A. Regenscheid, A. Roginsky *et al.,* "Report on pairing-based cryptography," *Journal of Research of the National Institute of Standards and Technology*, vol. 120, pp. 11, 2015.

[24] Y. J. Ren, J. Qi, Y. P. Cheng, J. Wang and O. Alfarraj, "Digital continuity guarantee approach of electronic record based on data quality theory," *Computers, Materials & Continua*, vol. 63, no. 3, pp. 1471–1483, 2020.

[25] C. P. Ge, W. Susilo, J. Baek, Z. Liu, J. Y. Xia *et al.,* "Revocable attribute-based encryption with data integrity in clouds," *IEEE Transactions on Dependable and Secure Computing*, vol. 99, pp. 1, 2021.

[26] C. Chen, K. Li, S. G. Teo, X. Zou, K. Li *et al.,* "Citywide traffic flow prediction based on multiple gated spatio-temporal convolutional neural networks," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 14, no. 4, pp. 1–23, 2020.

[27] X. R. Zhang, X. Sun, W. Sun, T. Xu and P. P. Wang, "Deformation expression of soft tissue based on BP neural network," *Intelligent Automation & Soft Computing*, vol. 32, no. 2, pp. 1041–1053, 2022.

[28] M. Duan, K. Li, X. Liao and K. Li, "A parallel multiclassification algorithm for big data using an extreme learning machine," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 6, pp. 2337–2351, 2017.

[29] J. Chen, K. Li, K. Bilal, K. Li, S. Y. Philip *et al.,* "A bi-layered parallel training architecture for large-scale convolutional neural networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 5, pp. 965–976, 2018.

[30] Y. J. Ren, Y. Leng, J. Qi, K. S. Pradip, J. Wang *et al.,* "Multiple cloud storage mechanism based on blockchain in smart homes," *Future Generation Computer Systems*, vol. 115, pp. 304–313, 2021.

[31] A. S. Tolmay, "An investigation into the personal interaction items which best explain the variation in trust within automotive supply chains," *International Journal of Information Systems and Supply Chain Management*, pp. 1592–1607, 2020.

[32] X. Zhou, K. Li, Y. Zhou and K. Li, "Adaptive processing for distributed skyline queries over uncertain data," *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 2, pp. 371–384, 2015.

[33] M. Ali, S. U. Khan and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences*, vol. 305, pp. 357–383, 2015.