Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 45 (2024), No. 2, pp. 581–594
DOI : 10.47974/JIOS-1596

An artificial intelligence based authentication mechanism for wireless sensor networks using blockchain

Suman Devi *
Avadhesh Kumar †
School of Computing Science and Engineering
Galgotias University
Greater Noida 203201
Uttar Pradesh
India

Abstract

Blockchain Networks (BNs) are widely used in a variety of applications around the globe. BN exchanges data and information using various inter-network and intra-network protocols. The sharing of this information across multiple platforms poses a significant security threat to the data sensed by the devices. This paper uses a combination of blockchain technology with AI algorithms to propose a novel security framework for BNs that acts as a security check gateway for any third party trying to access BN data. This paper proposed a hybrid security framework using blockchain. In order to provide a clear and efficient authentication scheme, global blockchain and local blockchain are separately used for BN authentication. The proposed work uses an artificial intelligence (AI) approach - Student Psychology Based Optimization (SPBO) is implemented in Matlab and Python. This approach is compared with some famous security algorithms of BNs, and it performs better than all the existing security algorithms used for BN.

Subject Classification: *68M18.*

Keywords: *Blockchain, Devices, Private blockchain, Public blockchain, Security, SPBO.*

1. Introduction

Blockchain networks (BNs) are widely used in a variety of applications around the globe. BNs are scattered across a specific area; they sense the useful information, store it and send it to the base station. BNs consist of

* *E-mail:* **suman14vashisth@gmail.com (Corresponding Author)**
† *E-mail:* **avadheshkumar@galgotiasuniversity.edu.in**

© Taru Publications

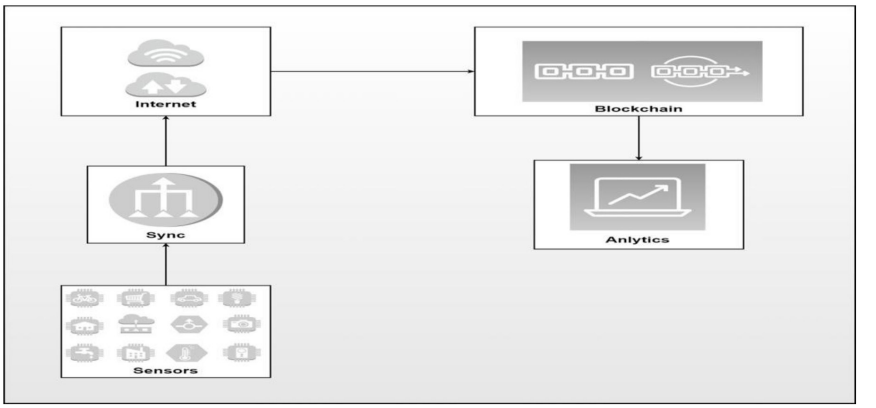


Figure 1

Blockchain Technology

cheap, tiny devices that are battery operated and are power constrained. BNs are frequently used in agriculture, traffic monitoring, defense, disaster management, and medical apparatus [1-5]. In the modern era, BN can be divided into centralized and distributed services [6]. In centralized BN, devices aggregate the data and transmit it to the sink, whereas in distributed BN service, other nodes and networks can directly obtain data from devices, resulting intra and internetwork communication. Although intra and inter network communication provides flexibility to BNs, it also raises security concerns. It is important to protect the identity of devices and safeguard its data and information [7]. An architecture of Blockchain Technology with BN is shown in Figure 1.

Conventional BN security protocols use centralized security protocol methods. These methods depend on a third-party certificate, such as a trusted certification authentication center [8-10]. But the involvement of third party brings the risk of single point failure [11-12]. The use of this technology for the security of BNs is still in an experimental stage, and there may be some unresolved issues regarding BN security using blockchain [13-15].

AI has been widely used in a variety of domains around the world. Meta heuristic algorithms such as Black Widow Algorithm, Gravitational Search Algorithm, and Student Psychology-Based Optimization (SPBO) are used in many optimization problems around the world. This research uses AI algorithms for the performance enhancement of Blockchain based BN security. This model serves as an optimization problem and propose a

security framework that is unique, random, novel, and cannot be tampered. The main contribution in this paper are as follows:

- This paper formulates a multi structure BN that is heterogeneous in nature. It consists of a variety of nodes used for different purposes. The BN consists of an optimal number of devices, cluster heads and, a base station.
- The paper presents a novel hybrid secure blockchain model using an AI approach (SPBO). The Hybridization is obtained in order to divide and categorize devices according to their security and encryption key requirements.
- A hybrid security framework for BN provides a clear and efficient authentication scheme; global blockchain and local blockchain are separately used for BN identification.

In rest of the paper, section 2 explains literature reviews, A network model is presented in section 3. Proposed algorithm is presented in section 4. Results are drawn in section 5 and concluded in section 6.

2. Literature Review

Blockchain was first introduced as a part of the Bitcoin in 2008 [16]. Authors and researchers around the world have used blockchain technology in a variety of fields and areas [17-20], such as resource scheduling in cloud applications [21], and it is also employed in intelligent optimal algorithms to enhance the performance [22-26]. Every block in a blockchain consists of two parts, namely block and block head. In this hierarchy, blocks are the transitions stored in the database, which can be of any format or structure [27]. For instance, a block may be a health information, a transaction related to currency, a system log, or information about the traffic. The block header contains two diverse metadata sets: a mining metadata and the block itself. A double hashing is done on the transaction records [28]. All the transactions are then combined together and submitted to the blockchain in the form of blocks. An efficient password technology is applied in order to combine all the blocks in a specific order. Therefore, all the blocks combined together form a chain structure, resulting in a blockchain.

There are a variety of encryption algorithms that ensure the privacy and authenticity of each block in a blockchain. Data security algorithms ensure that all the blocks are secured and cannot be tampered with by any

outside agent [29-30]. The blockchain is majorly dependent on the consensus system and the major ingredient of a blockchain is a node. The consensus mechanism ensures that even if a specific node fails in the blockchain, all the other nodes have no effect of a single failure and all other nodes keep working uninterrupted. This approach solves the limitation of traditional centralized system, where failure of one node results in the breakdown of the entire system [31-33]. Private and consortium blockchains are very similar and basically private blockchain in essence. The public blockchain specifies the group or individual that shares a blockchain. The public blockchain can be referred to as the most widely used blockchain as it has a decentralized approach that helps users to access blockchain services in an error free environment. The consensus blockchain is controlled by some nodes that are preselected. This kind of blockchain is referred to as partially centralized. Private blockchains are used specifically for bookkeeping purposes and are not available to the public. The private blockchain can be a person or a company that writes for blockchain access and they have very limits access to the outside world [34-44].

3. Network Model

IoT networks would be able to use blockchain technologies to tear down the conventional network model, in which terminal machines rely on the central storage database on the cloud to identify and authenticate devices in the system. With high protection mesh networks, blockchain creates a modern decentralised management mode. In the current model, terminal sensor data transactions are reliably interconnected. All information is stored on a server that is open to attack. Since the scheme lacks stringent authentication and encryption mechanisms, this is the case. On the server side, users can simulate sensor data, analyze it, and make decisions. Blockchain is a decentralized blockchain with advanced authentication features such as signatures, consensus checking, and numerous storage replicas. IoT transmission and data collection characteristics.

Encrypted transactions, consensus authentication, and distributed storage are the three mechanisms that make up the blockchain-based infrastructure. The device gathers data from the periphery in the early stages. To encrypt the transmitted data, the device uses its ID as a public key. Any nodes in a blockchain scheme serve as authentication nodes, and others serve as storage nodes. The verification node's job is to accept

transactions, check their legitimacy, run consistency algorithms, and shape blocks. The blocks are stored in the storage nodes as hash indexes, ensuring that all nodes have the same blockchain data. The distributed ledger offers a number of high-security benefits. To begin, transaction data is stored in the blockchain that cannot be modified or removed. As a result, it is an irreversible ledger. Second, the system hashes of firmware and applications are recorded in a distributed ledger so that users can securely verify transactions for tampering. Finally, the blockchain distributed ledgers have scalability. If a node is disconnected or destroyed, the sensor data is preserved in other nodes, thanks to the consensus node.

4. Proposed Algorithm

A blockchain ecosystem's consensus paradigm is at its heart. The system's output value, which includes delays, throughput, and other metrics, is determined by a consensus approach. The total count of transactions performed per second is commonly used to characterize throughput. Other indices, such as the time it takes to generate a block and the time it takes to complete a transaction, are equally significant. At the moment, blockchain is categorized into 3 categories: public, permissioned, and partnership. From the user's perspective, the public blockchain provides unrestricted access to the framework. To access the scheme, you must have permission from the permissioned blockchain and alliance one. The kind of blockchain used is often different due to the different circumstances. The system of majority agreement is the primary theoretical distinction of blockchain. Proof of Work (POW) is a Bitcoin consensus system that depends on machine mining power. The Ethereum consensus method employs proof-of-stake. They are visual representations of a public blockchain app. To reach consensus, the Hyperledger scheme uses the IBM-developed Practical Byzantine Fault Tolerant (PBFT). Union blockchain mostly uses PBFT. Hyperledger introduced a member management mechanism to enable it to be used in a private setting. In BN, a blockchain-based collocation architecture framework that is unique to a specific organization or agency. Members that have been added to the scheme must be given the authority to do those tasks. So, in this article, a private blockchain-based consensus algorithm called Hierarchical BFT used.

4.1 *Cryptotion Technology*

This research suggests BCE-BN, a block-based BN encryption algorithm, to address the information security issues that occur in BN while also ensuring the confidentiality of information transmitted. Key pair creation, encryption, signature, and authentication are the four parts of the algorithm.

Key pair generation. Make a key pair out of the information you've gathered so far. The BN device generates a key pair for each device in the wireless sensor network in an anonymous manner, with the ID node serving as the public key.

Encryption - It is a mathematical procedure that generates a ciphertext from plaintext and an encryption key. To produce ciphertext, this paper uses an asymmetric encryption algorithm with plaintext and the node's private key as input. The ciphertext isn't protected in any way.

Signature - The sender node encrypts the transaction data using his ID as the public key, produces encrypted cyphertext, and sends it to the recipient. Although maintaining the accuracy of the records, this signature approach prevents anyone from forging it.

Verification - All the nodes in the network can use the public key to check the validity of the information to decide if it was sent by the source node. If the verification is successful, the data is sent to the target node and stored in the blockchain framework. The data is discarded if the validation fails.

This research optimizes the entire operation using AI algorithm SPBO.

4.2 *Student Psychology Based Optimization Algorithm*

Several optimization algorithms have been possible in recent years, and they are now being used in a number of fields. How good a student does on an exam is determined by the number of points he or she receives. The student who receives the highest test score is referred to as the best student in the class. Students in most schools strive to boost their grades so that they can be the top student in the class. Students must put in more effort into the subjects given to them in order to do this. After researching their behaviour and speaking with them, the writers of the current paper learned about the observed psychology of students. Over the last four years, this research has taken place in a variety of schools, colleges, and universities in West Bengal, India. To be the highest in class, students must achieve a higher grade than the majority of their classmates as shown in

Figure 2. To achieve this goal, they must devote more time and resources to the subjects assigned to them. They must compete in all of their subjects in order to increase their overall score. As a result, students must put forward effort in each subject in order to increase their overall grades. The skill, consistency, and commitment of a student in a subject, on the other hand, determine his or her progress in that subject. As a result, it's necessary to keep in mind that exam grades will not increase at the same pace for all candidates and that outcomes will differ from one student to the next. Students' desire to do well in school is often influenced by their psychology. Any student aspires to outperform the best student by putting in the same or more effort. At the same time, certain students strive to match the commitment of the class's best student, as well as to go beyond and above the effort of the average student. Students' effort determines how well they do. Students may also attempt to bring in more effort topic by topic to increase their average test score and their interest in a subject decides how much effort they put forward in that subject.

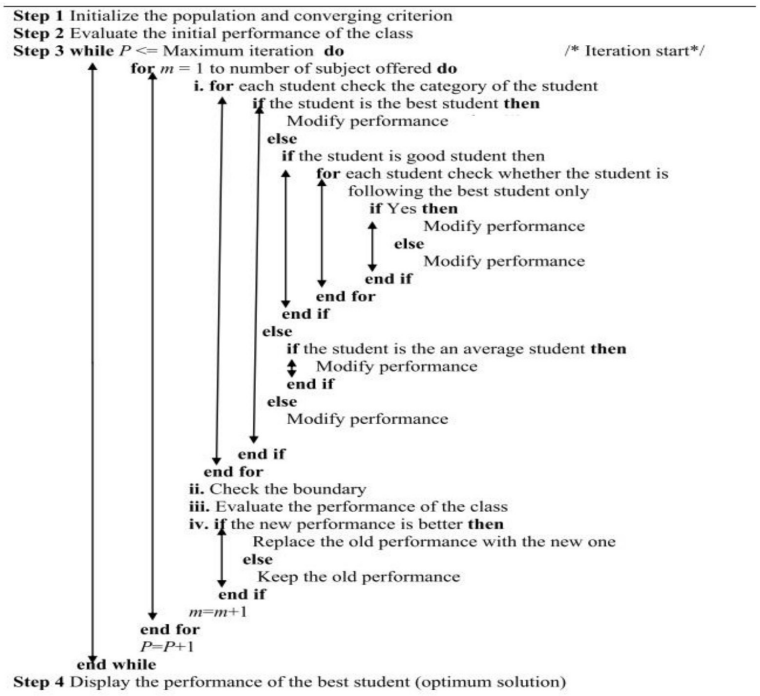


Figure 2

Flowchart of the SPBO algorithm

5. Experiment and Simulation

This approach builds a blockchain cluster in a distributed system to replicate and validate the model in the actual trial. Simultaneously, author consider the impact of different variables on the whole blockchain scheme and then use system latency and system throughput as the two metrics to assess the system's overall efficiency as shown in Figure 3. The proposed blockchain-based device efficiency is clearly superior to that of a single-centre server to some degree as compared to the traditional centralized methods and the methodology of [45].

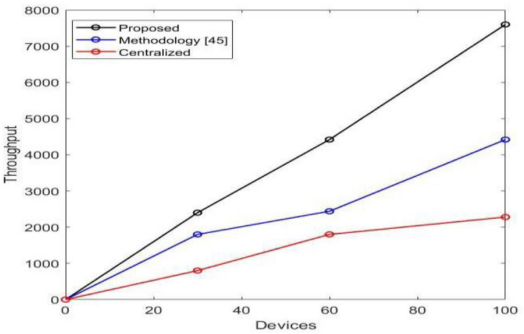


Figure 3

Proposed work compared for throughput.

With the number of devices rising, there are two forms. Research also carried out tests to see how fast our blockchain-based data management network can handle transactions. The transaction process speed is then reported in our experiments. The speed of transaction process is around

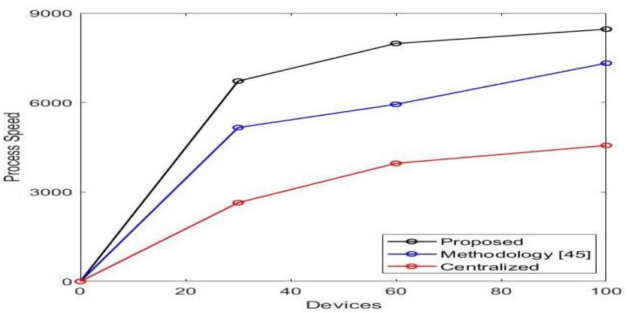


Figure 4

Proposed work compared for Processing speed.

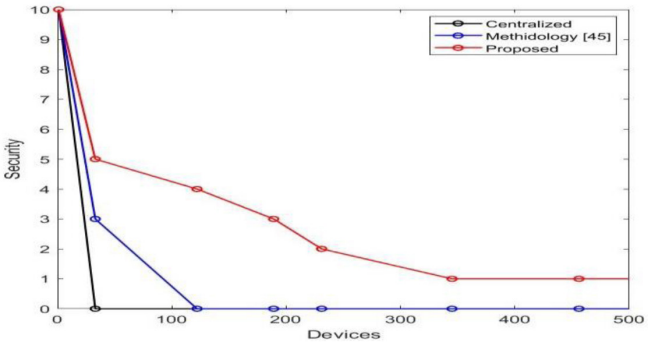


Figure 5

Proposed work compared for security with increasing devices.

6806 tx/s when the number of nodes is four, as seen in Figure 4. The device transaction processing speed approaches 14326 tx/s when number of nodes exceeds 31. The proposed approach clearly indicates that the process speed is better than that of the other two approaches as shown in Figure 4

The proposed algorithm is compared with the existing algorithms in terms of security with an increasing number of devices. In this modern era, network devices are increasing exponentially, and it is crucial to provide security to the data used. As shown in Figure 5, the proposed algorithm provides better security as compared to the compared algorithms. Although security decreases with increasing number of devices, even then suggested work performs better.

The number of network devices are growing at an unprecedented rate in the digital world, making it critical to ensure QoS in blockchain. In

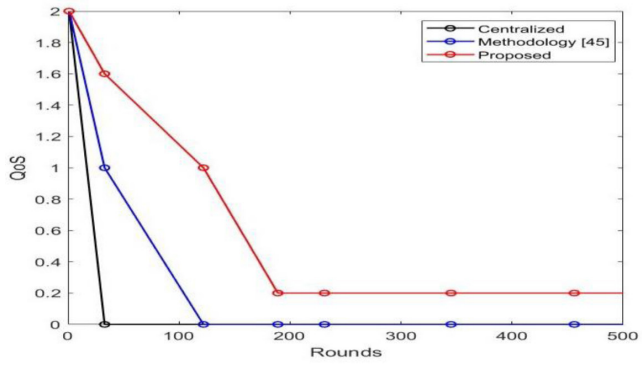


Figure 6

Proposed work compared for QoS of the blockchain.

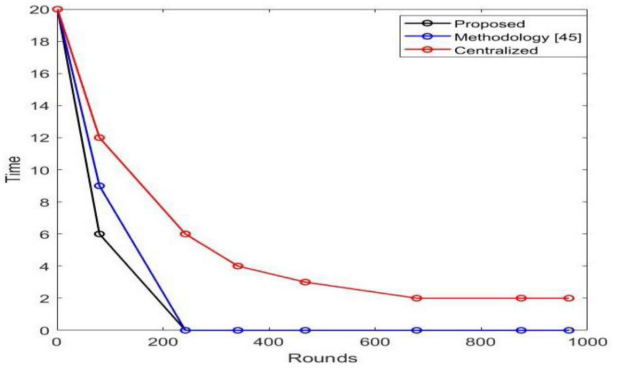


Figure 7

Proposed work compared in terms of Computation time.

comparison to the other algorithms, as seen in Figure 6, the proposed algorithm provides better QoS. Even if the QoS of the proposed algorithm decreases as the number of devices grows, it still outperforms current algorithms.

Figure 7 compares the proposed algorithm with existing algorithms in terms of computation speed. Computation speed is an important parameter to understand the complexity of the algorithm. Blockchains consist of a number of devices, hence the algorithms implemented on the blockchain should be light and platform independent. As seen in Figure 7, the proposed algorithm has better computation speed.

6. Conclusion

The proposed algorithm has high-performance efficiency and scalability, and the approach is more robust and straightforward because of the digital signature scheme. Our tests also demonstrate that the blockchain has lower latency and higher throughput than unified server mode. The throughput of a blockchain scheme increases in lockstep with the number of nodes. The blockchain-based database architecture is more robust and reliable, making it suitable for securely storing sensor data transactions. The proposed approach is tested against some of the famous existing blockchain technologies over a variety of parameters and the proposed approach performs better than the existing algorithms over all the testing parameters.

References

[1] Kumar, Anil, Ravinder Kumar, and Sartaj Singh Sodhi. "A novel privacy preserving blockchain based secure storage framework for electronic health records." *Journal of Information and Optimization Sciences* 43.3 : 549-570.1407-1418 (2022).

[2] Abou Jaoude, Joe, and Raafat George Saade. "Blockchain applications–usage in different domains." *IEEE Access* 7 : 45360-45381 (2019).

[3] Tahir, Mohammad, et al. "A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities." *IEEE Access* 8 : 115876-115904 (2020).

[4] Krichen, Moez, et al. "Blockchain for modern applications: A survey." *Sensors* 22.14 : 5274 (2022).

[5] Wang, Qiang, and Min Su. "Integrating blockchain technology into the energy sector—from theory of blockchain to research and application of energy blockchain." *Computer Science Review* 37 : 100275 (2020).

[6] Cui, Zhihua, et al. "A hybrid blockchain-based identity authentication scheme for multi-WSN." *IEEE Transactions on Services Computing* 13.2 : 241-251 (2020).

[7] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." *Future Generation Computer Systems* 82 : 395-411 (2018).

[8] Wu, Fan, et al. "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks." *Future Generation Computer Systems* 82 : 727-737 (2018).

[9] Hsiao, Sung-Jung, and Wen-Tsai Sung. "Employing blockchain technology to strengthen security of wireless sensor networks." *IEEE Access* 9 : 72326-72341 (2021).

[10] Hsiao, Sung-Jung, and Wen-Tsai Sung. "Utilizing blockchain technology to improve wsn security for sensor data transmission." *Comput. Mater. Contin* 68 : 1899-1918 (2021).

[11] Ali, Shahab, et al. "A blockchain-based secure data storage and trading model for wireless sensor networks." Advanced Information Networking and Applications: Proceedings of the 34th International Conference on Advanced Information Networking and Applications (AINA-2020). Springer International Publishing, 2020.

[12] Ramasamy, Lakshmana Kumar, et al. "Blockchain-based wireless sensor networks for malicious node detection: A survey." *IEEE Access* 9 : 128765-128785 (2021).

[13] Huang, Junqin, et al. "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism." *IEEE Transactions on Industrial Informatics* 15.6 : 3680-3689 (2019).

[14] Bao, Zijian, et al. "IoTChain: A three-tier blockchain-based IoT security architecture." *arXiv preprint arXiv:1806.02008* (2018).

[15] Hammi, Mohamed Tahar, et al. "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT." *Computers & Security* 78 : 126-142 (2018).

[16] Guo, Huaqun, and Xingjie Yu. "A survey on blockchain technology and its security." *Blockchain: Research and Applications* 3.2 : 100067 (2022).

[17] Mishra, Anil Kumar, and Yogomaya Mohapatra. "Hybrid blockchain based medical data sharing with the optimized CP-ABE for e-Health systems." *International Journal of Information Technology* : 1-10 (2023).

[18] Miah, Muhammed, Shah Jahan Miah, and Santosh Venkatraman. "Blockchain: At a glance idea for information science researchers." *Journal of Information and Optimization Sciences* 42.7 : 1589-1624 (2021).

[19] Monrat, Ahmed Afif, Olov Schelén, and Karl Andersson. "A survey of blockchain from the perspectives of applications, challenges, and opportunities." *IEEE Access* 7 : 117134-117151 (2019).

[20] Antonucci, Francesca, et al. "A review on blockchain applications in the agri-food sector." *Journal of the Science of Food and Agriculture* 99.14 : 6129-6138 (2019).

[21] Liu, Mengting, et al. "Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing." *IEEE Transactions on Wireless Communications* 18.1 : 695-708 (2018).

[22] Cai, Xingjuan, Xiao-zhi Gao, and Yu Xue. "Improved bat algorithm with optimal forage strategy and random disturbance strategy." *International Journal of Bio-Inspired Computation* 8.4 : 205-214 (2016).

[23] Cui, Zhihua, et al. "Optimal LEACH protocol with modified bat algorithm for big data sensing systems in Internet of Things." *Journal of Parallel and Distributed Computing* 132 : 217-229 (2019).

[24] Alkhli, Sultan. "Sea Turtle Foraging Optimization-Based Controller Placement with Blockchain-Assisted Intrusion Detection in Software-Defined Networks." *Computers, Materials & Continua* 75.3 (2023).

[25] Li, Lun, et al. "Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles." *IEEE Transactions on Intelligent Transportation Systems* 19.7 : 2204-2220 (2018).

[26] Sezer, Bora Bugra, Hasret Turkmen, and Urfat Nuriyev. "PPFchain: A novel framework privacy-preserving blockchain-based federated learning method for sensor networks." *Internet of Things* 22 : 100781 (2023).

[27] Panwar, Arvind, and Vishal Bhatnagar. "Analyzing the performance of data processing in private blockchain based distributed ledger." *Journal of Information and Optimization Sciences* 41.6 : 1407-1418 (2020).

[28] Jia, Meng, et al. "Redactable Blockchain From Decentralized Chameleon Hash Functions." *IEEE Transactions on Information Forensics and Security* 17 : 2771-2783 (2022).

[29] Cui, Zhihua, et al. "A hybrid blockchain-based identity authentication scheme for multi-WSN." *IEEE Transactions on Services Computing* 13.2 : 241-251 (2020).

[30] Mubarakali, Azath. "An efficient authentication scheme using blockchain technology for wireless sensor networks." *Wireless Personal Communications* 127.1 : 255-269 (2022).

[31] Mingxiao, Du, et al. "A review on consensus algorithm of blockchain." 2017 IEEE international conference on systems, man, and cybernetics (SMC). IEEE (2017).

[32] Lashkari, Bahareh, and Petr Musilek. "A comprehensive review of blockchain consensus mechanisms." *IEEE Access* 9 : 43620-43652 (2021).

[33] Alam, Shadab. "The Current State of Blockchain Consensus Mechanism: Issues and Future Works." *International Journal of Advanced Computer Science and Applications* 14.8 (2023).

[34] Hong, Sunghyuck. "P2P networking based internet of things (IoT) sensor node authentication by Blockchain." *Peer-to-Peer Networking and Applications* 13.2 : 579-589 (2020).

[35] Hong, Sunghyuck. "P2P networking based internet of things (IoT) sensor node authentication by Blockchain." *Peer-to-Peer Networking and Applications* 13.2 : 579-589 (2020).

[36] Simpson, Serin V., et al. "SECURE TRUST: a blockchain-enabled trust and reputation system for malicious node detection in IOT networks." *International Journal of Information Technology* 15.8 : 4323-4336 (2023).

[37] Singhal, Divya, Laxmi Ahuja, and Ashish Seth. "POSMETER: proof-of-stake blockchain for enhanced smart meter data security." *International Journal of Information Technology* : 1-14 (2023).

[38] Goyat, Rekha, et al. "Blockchain-Based Data Storage With Privacy and Authentication in Internet of Things." *IEEE Internet of Things Journal* 9.16 : 14203-14215 (2020).

[39] Xie, Mingyue, et al. "A survey on blockchain consensus mechanism: research overview, current advances and future directions." *International Journal of Intelligent Computing and Cybernetics* 16.2 : 314-340 (2023).

[40] Gebremariam, Gebrekiros Gebreyesus, J. Panda, and S. Indu. "Blockchain-Based Secure Localization against Malicious Nodes in IoT-Based Wireless Sensor Networks Using Federated Learning." *Wireless Communications and Mobile Computing* 2023 (2023).

[41] Khan, Asad Ullah, et al. "A blockchain scheme for authentication, data sharing and nonrepudiation to secure internet of wireless sensor things." *Cluster Computing* 26.2 : 945-960 (2023).

[42] Rehman, Abdul, et al. "Ensuring Security and Energy Efficiency of Wireless Sensor Network by Using Blockchain." *Applied Sciences* 12.21 : 10794 (2022).

[43] Ganeshan, Arulkumaran, et al. "Secure identity key and blockchain-based authentication approach for secure data communication in multi-WSN." *Concurrency and Computation: Practice and Experience* 35.28 : e7861 (2023).

[44] Feng, Libo, et al. "A blockchain-based collocation storage architecture for data security process platform of WSN." 2018 IEEE 22nd international conference on computer supported cooperative work in design (CSCWD). IEEE (2018).

[45] Hsiao, Sung-Jung, and Wen-Tsai Sung. "Employing blockchain technology to strengthen security of wireless sensor networks." *IEEE Access* 9 : 72326-72341 (2021).