An Artificial Intelligence based Authentication Mechanism for Wireless Sensor Networks using Blockchain

Suman Devi[1], Avadhesh Kumar[2]
School of Computing Science and Engineering, Galgotias University, Greater Noida, India

Abstract:
Blockchain Networks (BNs) are widely used in a variety of applications around the globe. BN exchange data and information using various inter-network and intra-network protocols. This information sharing on multiple platforms causes a serious security threat to the data sensed by the devices. This paper used a combination of Blockchain technology with AI algorithms to propose a novel security framework for BNs that acts as a security check gateway to any third party trying to access BN data. The 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 used artificial intelligence (AI) approach Student Psychology Based Optimization (SPBO) and is implemented in Matlab and Python. The proposed algorithm is compared with some famous security algorithms of BNs and the proposed algorithm performs better than all the recent security algorithms used for BN

Keywords: Blockchain, Security, Devices, Public Blockchain, Private Blockchain.
DOI: 10.24297/j.cims.2023.7.10

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, stores the information and send it to the base station. BNs consist of 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 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 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 shown in Figure 1.

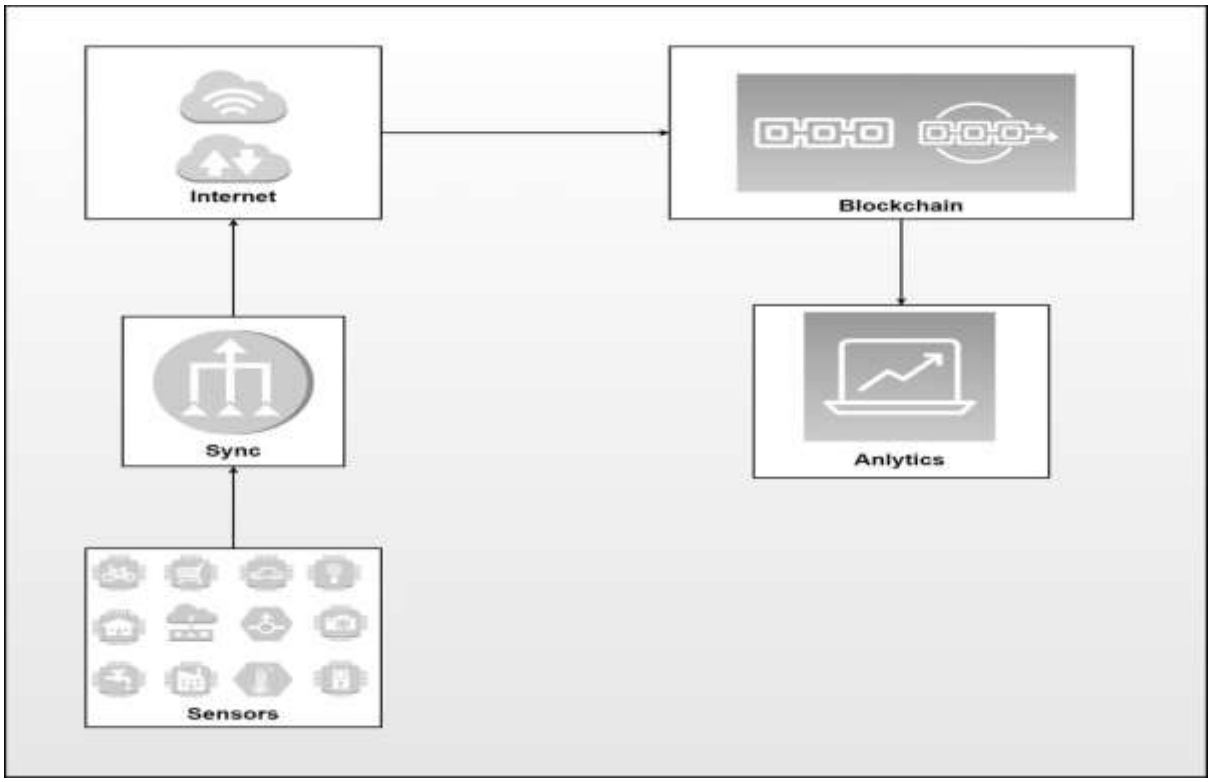

Figure 1 Blockchain Technology

Conventional BN security protocols use centralized security protocol methods. These methods depend on 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]. Use of this technology for the security of BNs is still in experimental stage and there may be some unresolved issues regarding the BN security using blockchain [13-15].

Artificial intelligence has been widely used in a variety of domains around the world. Meta heuristic algorithms such as Black widow algorithm, Gravitational search algorithm, student psychology-based optimization (SPBO) used in many optimization problems around the world. This research use of AI algorithms for performance enhancement of Blockchain based BN security. We model the BN security as an optimization problem and propose a security framework for BN that is unique, random, novel and cannot be tampered with. Authors contribution to the paper are as follows

- In this paper, we formulate a multi structure BN that is heterogeneous in nature. The proposed BN consist of a variety of nodes used for different purposes. The BN consist of optimal number of devices, cluster heads and a base station.
- The paper presents a novel hybrid secure blockchain model using 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 consist of two parts namely block and block head. In this hierarchy, block is 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 an information about the traffic. Block header contains two diverse metadata sets; a mining metadata and the block itself. A double hashing is done on the transaction records. All the transactions are then combined together and submitted to blockchain in 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 forms a chain structure, resulting in a blockchain.

There are a variety of encryption algorithms that ensures the privacy and authenticity of each block in a blockchain. Data security algorithms ensures that all the blocks are secured and they 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

breaking down of the entire system [31-33]. Private and consortium blockchain are very much similar and are basically private blockchain in essence. Public blockchain specifies the group or the individual that shares a blockchain. The public blockchain can be referred to as the most widely used blockchain as it a decentralized approach which helps users to access blockchain services in an error free environment. Consensus blockchain is controlled by some nodes that are preselected. This kind of blockchain is referred to as partially centralized. Private blockchain are used specifically for bookkeeping purpose and are not available to public. The private blockchain can be a people or a company that writes for a blockchain access and they have very limits access to the outside world [34].

3. Network Model

IoT networks would be able to use blockchain technologies to tear down the conventional network model, in which terminal machines relys on the central storage database on cloud to identify and authenticate devices in the system. With high protection mesh networks, blockchain creates a modern decentralised management mode. Terminal sensor data transactions would be reliably interconnected in the current model. All information is held 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, analyse it, and make decisions. Blockchain is a decentralised 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, with each node storing the same blockchain data. The distributed ledger offers a number of high-security benefits. To begin, transaction data stored in 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 distributed ledger such 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 consensus approach. Total count of transactions performed per second is commonly used to characterise 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 categorised 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. POW is a Bitcoin consensus system that depends on machine mining power. The Ethererum 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 functional 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, we have a blockchain-based collocation architecture framework that is unique to a specific organisation or agency. Members that have been added to the scheme must be given the authority to do those tasks. So, in this article, we use a private blockchain-based consensus algorithm called Hierarchical BFT.

4.1 Cryptotion Technology - We suggest 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, we use 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.

We optimize 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. Since he or she received the highest test score, the best student in the class is referred to as such. 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 in and of 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 thesis 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. 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. Around 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.

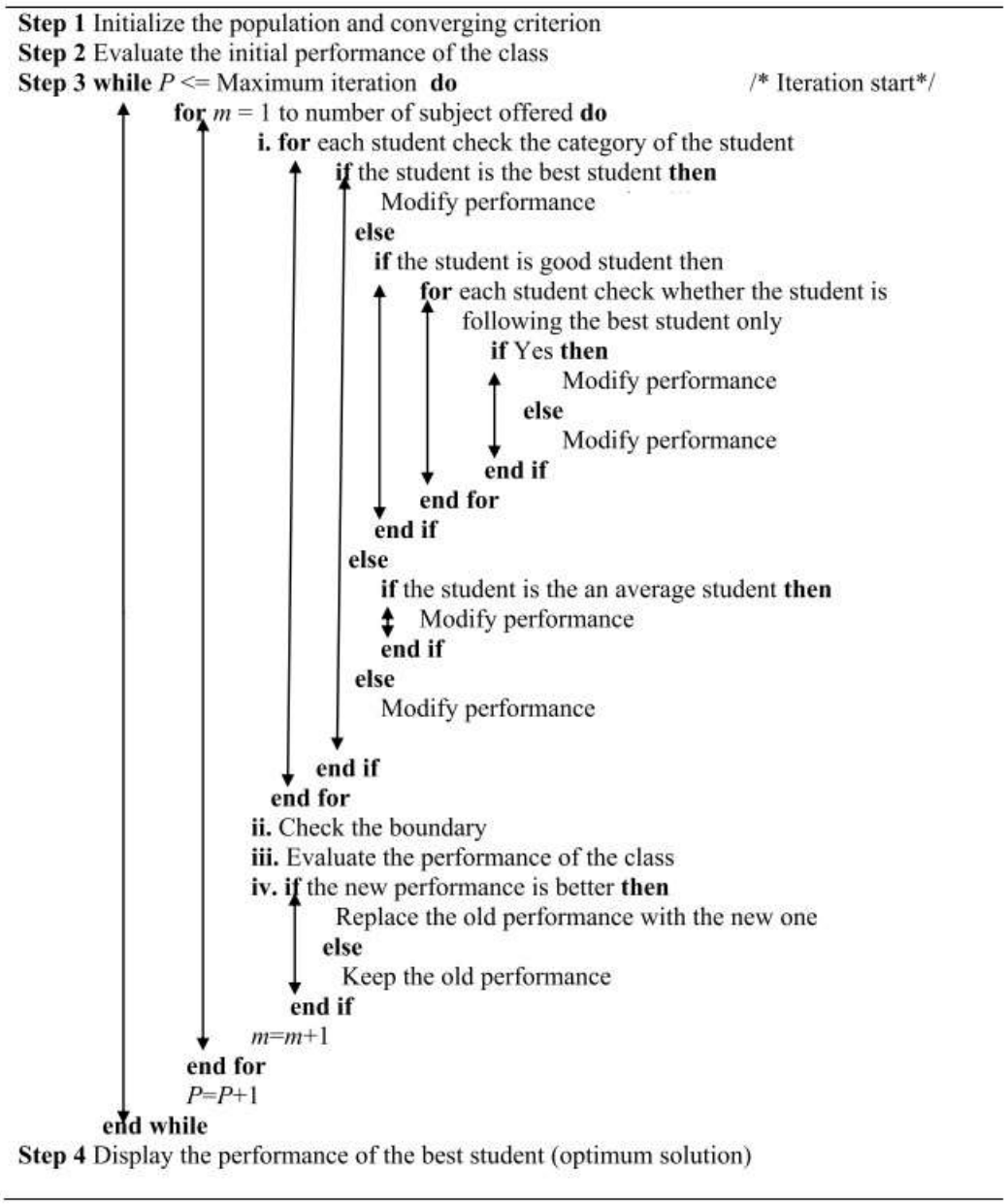

Figure 2 Flowchart of the SPBO algorithm

5. Experiment And Simulation

We build a blockchain cluster in a distributed system to replicate and validate our model in the actual trial. Simultaneously, we 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 (Figure 3). Proposed Blockchain-based device efficiency is clearly superior to that of a single-centre server to some degree.

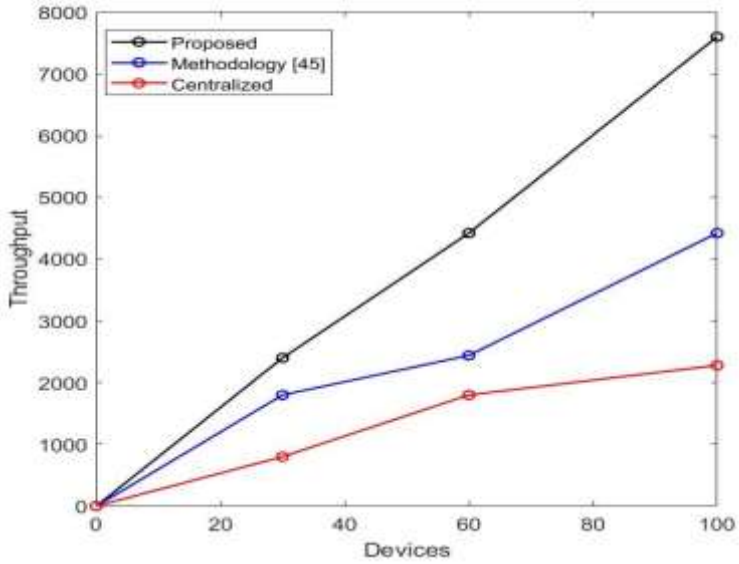

Figure 3 Proposed work compared for throughput.

With the number of devices rising, there are two forms. We've 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 6806 tx/s when number of nodes is four, as seen in Fig.4. The device transaction processing speed approaches 14326 tx/s when number of nodes exceeds 31.

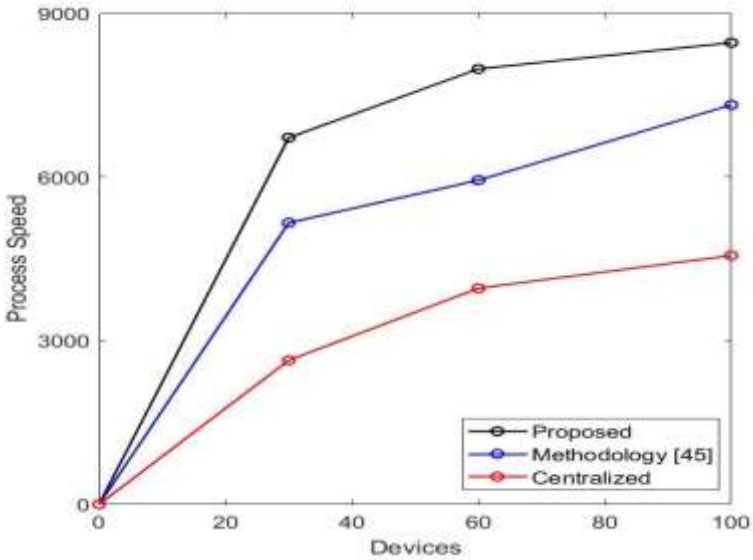

Figure 4 Proposed work compared for Processing speed.

The proposed algorithm is compared with the existing algorithms in terms of security with increasing number of devices. In this modern era, the 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 other algorithms. Although the security decreases with increasing number of devices, even then suggested work performs better.

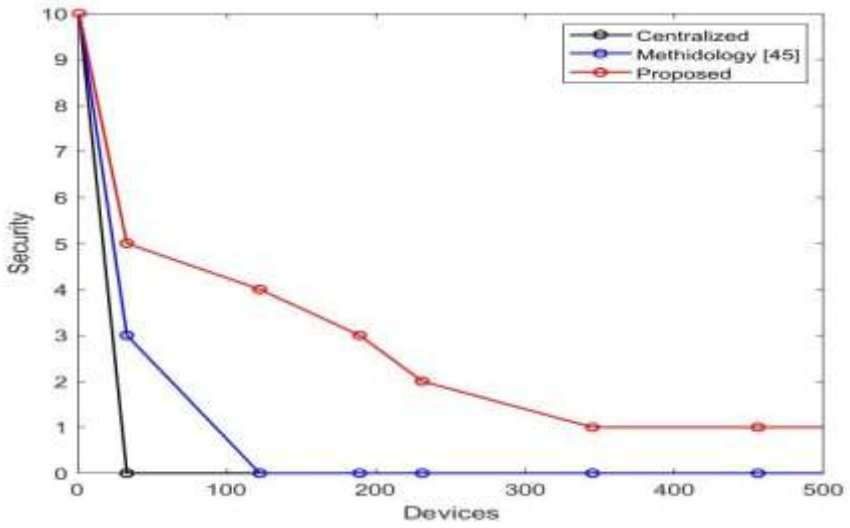

Figure 5 Proposed work compared for security with increasing devices.

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

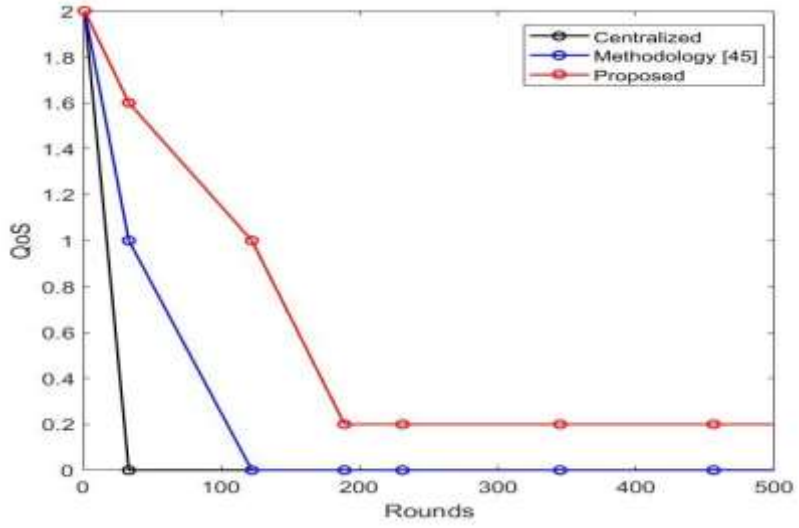

Figure 6 Proposed work compared for QoS of the blockchain.

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

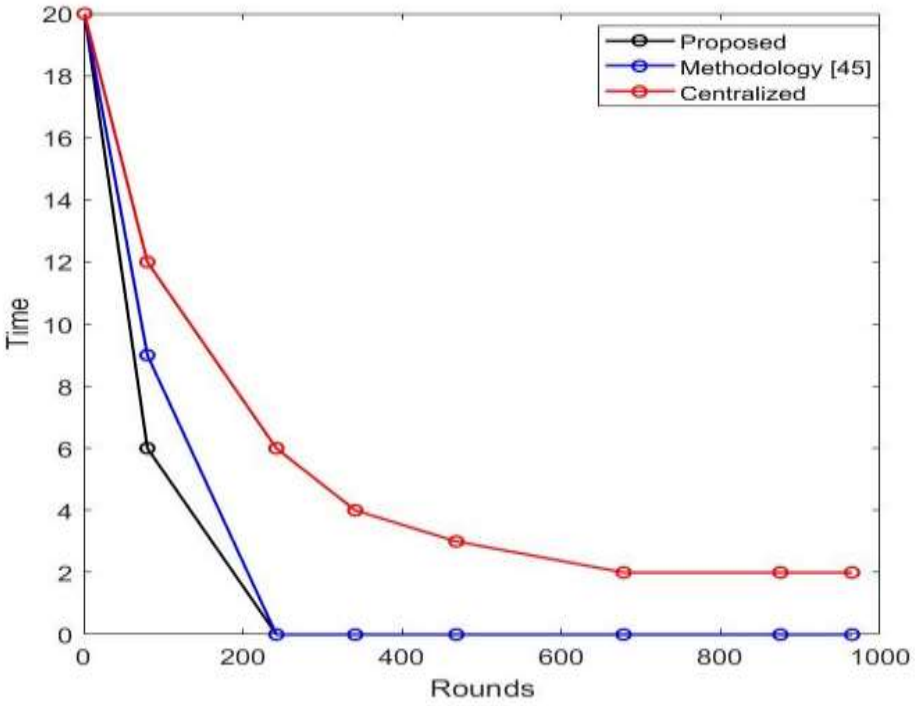

Figure 7. Proposed work compared in terms of Computation time.

6. Conclusion

The proposed algorithm has a 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 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. Kumari S, Om H. Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. Computer Networks. 2016 Jul 20;104:137-54.
2. Gope P, Hwang T. A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Transactions on industrial electronics. 2016 Jun 27;63(11):7124-32.
3. Amin R, Islam SH, Kumar N, Choo KK. An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks. Journal of network and computer applications. 2018 Feb 15;104:133-44.
4. Cui Z, Cao Y, Cai X, Cai J, Chen J. Optimal LEACH protocol with modified bat algorithm for big data sensing systems in Internet of Things. Journal of Parallel and Distributed Computing. 2019 Oct 1;132:217-29.
5. Xue F, Tang H, Su Q, Li T. Task allocation of intelligent warehouse picking system based on multi-robot coalition. KSII Transactions on Internet and Information Systems (TIIS). 2019;13(7):3566-82.
6. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems. 2013 Sep 1;29(7):1645-60.
7. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future generation computer systems. 2018 May 1;82:395-411.
8. Wu F, Li X, Sangaiah AK, Xu L, Kumari S, Wu L, Shen J. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Generation Computer Systems. 2018 May 1;82:727-37.
9. Ferrag MA, Maglaras LA, Janicke H, Jiang J, Shu L. Authentication protocols for internet of things: a comprehensive survey. Security and Communication Networks. 2017 Nov 6;2017.
10. Srivastava, D., Kumar, A., Mishra, A., Arya, V., Almomani, A., Hsu, C. H., & Santaniello, D. (2022). Performance Optimization of Multi-Hop Routing Protocols With Clustering-Based Hybrid Networking Architecture in Mobile Adhoc Cloud Networks. International Journal of Cloud Applications and Computing (IJCAC), 12(1), 1-15. http://doi.org/10.4018/IJCAC.309932.
11. Biswas S, Sharif K, Li F, Nour B, Wang Y. A scalable blockchain framework for secure transactions in IoT. IEEE Internet of Things Journal. 2018 Oct 4;6(3):4650-9.

12. Huang J, Kong L, Chen G, Wu MY, Liu X, Zeng P. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics. 2019 Mar 6;15(6):3680-9.
13. Bao Z, Shi W, He D, Chood KK. IoTChain: A three-tier blockchain-based IoT security architecture. arXiv preprint arXiv:1806.02008. 2018 Jun 6.
14. Almadhoun R, Kadadha M, Alhemeiri M, Alshehhi M, Salah K. A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA) 2018 Oct 28 (pp. 1-8). IEEE.
15. Hammi MT, Hammi B, Bellot P, Serhrouchni A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security. 2018 Sep 1;78:126-42.
16. Niloy FA, Nayeem MA, Rahman MM, Dowla MN. Blockchain-Based Peer-to-Peer Sustainable Energy Trading in Microgrid using Smart Contracts. In2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST) 2021 Jan 5 (pp. 61-66). IEEE.
17. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: Architecture, consensus, and future trends. In2017 IEEE international congress on big data (BigData congress) 2017 Jun 25 (pp. 557-564). IEEE.
18. Aggarwal S, Chaudhary R, Aujla GS, Kumar N, Choo KK, Zomaya AY. Blockchain for smart communities: Applications, challenges and opportunities. Journal of Network and Computer Applications. 2019 Oct 15;144:13-48.
19. McGhin T, Choo KK, Liu CZ, He D. Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications. 2019 Jun 1;135:62-75.
20. Wang S, Ouyang L, Yuan Y, Ni X, Han X, Wang FY. Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2019 Feb 15;49(11):2266-77.
21. Liu M, Yu FR, Teng Y, Leung VC, Song M. Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing. IEEE Transactions on Wireless Communications. 2018 Dec 12;18(1):695-708.
22. Cai X, Gao XZ, Xue Y. Improved bat algorithm with optimal forage strategy and random disturbance strategy. International Journal of Bio-Inspired Computation. 2016;8(4):205-14.

23. Deng X, Jiang P, Peng X, Mi C. An intelligent outlier detection method with one class support tucker machine and genetic algorithm toward big sensor data in internet of things. IEEE Transactions on Industrial Electronics. 2018 Aug 9;66(6):4672-83.
24. Li L, Liu J, Cheng L, Qiu S, Wang W, Zhang X, Zhang Z. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Transactions on Intelligent Transportation Systems. 2018 Jan 23;19(7):2204-20.
25. Cui Z, Xue F, Cai X, Cao Y, Wang GG, Chen J. Detection of malicious code variants based on deep learning. IEEE Transactions on Industrial Informatics. 2018 Apr 3;14(7):3187-96.
26. Cao Y, Ding Z, Xue F, Rong X. An improved twin support vector machine based on multi-objective cuckoo search for software defect prediction. International Journal of Bio-Inspired Computation. 2018;11(4):282-91.
27. Lemieux VL. Trusting records: is Blockchain technology the answer?. Records Management Journal. 2016 Jul 18.
28. Lin IC, Liao TC. A survey of blockchain security issues and challenges. Int. J. Netw. Secur.. 2017 Sep 1;19(5):653-9.
29. Aitzhan NZ, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing. 2016 Oct 12;15(5):840-52.
30. Karame G. On the security and scalability of bitcoin's blockchain. InProceedings of the 2016 ACM SIGSAC conference on computer and communications security 2016 Oct 24 (pp. 1861-1862).
31. Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and communication networks. 2016 Dec;9(18):5943-64.
32. Salman T, Zolanvari M, Erbad A, Jain R, Samaka M. Security services using blockchains: A state of the art survey. IEEE Communications Surveys & Tutorials. 2018 Aug 7;21(1):858-80.
33. Wu M, Wang K, Cai X, Guo S, Guo M, Rong C. A comprehensive survey of blockchain: From theory to IoT applications and beyond. IEEE Internet of Things Journal. 2019 Jun 12;6(5):8114-54.
34. Soni, D., Srivastava, D., Bhatt, A., Aggarwal, A., Kumar, S., & Shah, M. A. (2022). An Empirical Client Cloud Environment to Secure Data Communication with Alert Protocol. Mathematical Problems in Engineering.