**Information Dynamics and Applications**
https://www.acadlore.com/journals/IDA

# ECO-LEACH: A Blockchain-Based Distributed Routing Protocol for Energy-Efficient Wireless Sensor Networks

Feroz Khan A.B

Department of Computer Science, Syed Hameedha Arts and Science College, 623806 Kilakarai, Tamilnadu, India

* Correspondence: Feroz Khan A,B (abferozkhan@gmail.com)

**Received:** 03-16-2023 **Revised:** 03-24-2023 **Accepted:** 03-26-2023

**Citation:** F. K. A.B., "ECO-LEACH: A blockchain-based distributed routing protocol for energy-efficient wireless sensor networks," *Inf. Dyn. Appl.*, vol. 2, no. 1, pp. 1-7, 2023. https://doi.org/10.56578/ida020101.



**Abstract:** This paper proposes a novel architecture based on blockchain technology to enhance the dependability and safety of wireless sensor networks (WSN) by authenticating WSN nodes. In a WSN, sensor nodes collect and transmit data to cluster heads (CHs) for further processing. The proposed model employs the distance and residual energy-based low-energy adaptive clustering hierarchy (ECO-LEACH) protocol to replace CHs with ordinary nodes and the Interplanetary File System (IPFS) for storing data. In addition, consensus based on proof of authority (PoA) is used to validate transactions, reducing the computational cost associated with proof of work. The proposed system was evaluated using simulations with 300 sensor nodes and compared with other protocols, including LEACH, DDR-LEACH, PEGASIS, and LEACH-PSO. The simulation results showed that the proposed ECO-LEACH outperformed the other protocols in terms of energy consumption, throughput achieved, and network lifetime improvement. Specifically, the proposed system consumed 23.5J for 300 sensor nodes, achieved 687.5 kbps, and improved the network's lifetime by 4.12 seconds for 50 rounds. Overall, this paper provides a reliable and secure solution for authenticating WSN nodes, enhancing data transfer safety, and dependability. The proposed architecture offers a promising approach for addressing the challenges of WSN design using blockchain technology and PoA consensus. The comparative analysis shows that the proposed ECO-LEACH protocol outperforms other protocols in terms of energy consumption, throughput achieved, and network lifetime improvement for 300 sensor nodes.

**Keywords:** Blockchain, Wireless sensor networks, Energy consumption, Consensus, Clustering

## 1. Introduction

The proliferation of wireless sensor networks (WSNs) has enabled the collection of data from various sources, which can be analyzed to derive useful insights. However, data transfer in WSNs is often unreliable due to factors such as interference, signal attenuation, and limited bandwidth [1, 2]. Moreover, WSNs are prone to security threats such as node tampering, eavesdropping, and message replay attacks.

To address these challenges, blockchain technology has emerged as a potential solution for providing secure and reliable data transfer in WSNs. Blockchain is a distributed ledger technology that allows for secure and transparent data storage and transfer. By implementing blockchain in WSNs, the dependability and highest possible level of safety of data transfer can be achieved [3-6].

In this paper, we propose a blockchain-based architecture for the authentication of wireless sensor network nodes (WSN). The proposed architecture utilizes the distance and residual energy-based low-energy adaptive clustering hierarchy (ECO-LEACH) protocol, which replaces cluster heads (CHs) with ordinary nodes to solve the problem of energy consumption in WSNs. The proposed architecture also uses an external data storage solution called the Interplanetary File System (IPFS) to ensure reliable and secure storage of data.

One of the key challenges of implementing blockchain in WSNs is the computational cost of validating transactions [7-10]. Traditional consensus mechanisms such as proof of work (PoW) require significant computational resources, which can be a challenge for resource-constrained WSNs. To address this issue, we

propose the use of a consensus mechanism based on proof of authority (PoA), which requires significantly less computational resources compared to PoW.

To evaluate the effectiveness of the proposed architecture, we conducted simulations using 300 sensor nodes. The results of the simulation show that ECO-LEACH outperforms other clustering algorithms such as LEACH, DDR-LEACH, PEGASIS, and LEACH-PSO in terms of energy consumption, throughput, and network lifetime. Furthermore, the proposed consensus mechanism based on PoA ensures reliable and efficient validation of transactions.

Overall, this paper proposes a novel blockchain-based architecture for WSNs that addresses the challenges of energy consumption, reliability, and security. The use of ECO-LEACH and IPFS ensures efficient data transfer and secure data storage, while the PoA consensus mechanism ensures reliable and efficient validation of transactions. The simulation results demonstrate the effectiveness of the proposed architecture in comparison to existing approaches. The proposed work aims to address the following objectives.

- Develop a simulation model of the ECO-LEACH protocol to evaluate its performance in comparison to other existing WSN protocols in terms of network lifetime, energy consumption, and data transmission reliability.
- Investigate the impact of various factors, such as the number of nodes, the size of the network, and the distance between nodes, on the performance of the PROPOSED protocol.
- Analyze the security of the proposed system by evaluating the resilience of the blockchain-based authentication and data storage mechanisms against attacks such as data tampering, node compromise, and replay attacks.
- Evaluate the scalability of the PROPOSED protocol by analyzing its performance in large-scale WSN deployments with a high number of nodes.
- Investigate the potential of integrating other emerging technologies, such as edge computing or machine learning, to further enhance the performance and efficiency of the PROPOSED protocol in WSNs.

To achieve these objectives, the proposed work could employ various research methodologies such as simulation studies, statistical analysis, and security evaluations. The results of this research could provide valuable insights into the effectiveness and scalability of the proposed protocol in WSNs and its potential for addressing the challenges faced by these networks. Additionally, this work could contribute to the broader research community by providing a better understanding of the integration of blockchain technology with WSNs, which could lead to the development of more secure, reliable, and efficient WSN protocols in the future.

## 2. Related Works

Wireless sensor networks (WSNs) have been increasingly used in various applications for data collection and analysis. However, WSNs face several challenges such as security threats, energy consumption, and unreliable data transfer. To address these challenges, blockchain technology has been proposed as a potential solution for secure and reliable data transfer in WSNs. Recent research in this area has focused on various aspects of blockchain-based architectures for WSNs. For instance, a study by She et al. [11] proposed a blockchain-based secure data sharing scheme for WSNs. The scheme utilizes a consensus mechanism based on proof of work (PoW) and achieves secure and reliable data sharing in WSNs.

Another study by Tian et al. [12] proposed a blockchain-based framework for data authentication in WSNs. The framework utilizes a hierarchical structure of blockchain nodes to ensure secure and efficient data authentication in WSNs. In a study by Cao et al. [13], a blockchain-based architecture was proposed for WSNs to address the challenges of security threats and energy consumption. The proposed architecture utilized a consensus mechanism based on proof of authority (PoA) and achieved reliable and efficient data transfer in WSNs.

Similarly, a study by Kumar et al. [14] proposed a trust aware model for blockchain-based architecture for WSNs that utilized a consensus mechanism based on proof of stake (PoS). The proposed architecture achieved secure and efficient data transfer in WSNs while addressing the challenges of energy consumption and security threats.

Another study by Ren et al. [15] proposed a blockchain-based framework for secure and reliable data transfer in WSNs. The framework utilized a consensus mechanism based on Byzantine fault tolerance (BFT) and achieved secure and efficient data transfer in WSNs. In a study by Xu et al. [16], a blockchain-based architecture was proposed for WSNs that utilized a consensus mechanism based on delegated proof of stake (DPoS). The proposed architecture achieved efficient and secure data transfer in WSNs while addressing the challenges of energy consumption and security threats.

Similarly, a study by Hong [17] proposed a blockchain-based architecture for WSNs that utilized a consensus mechanism based on proof of reputation (PoR). The proposed architecture achieved secure and efficient data transfer in WSNs while addressing the challenges of energy consumption and security threats.

Another study by Zhang et al. [18] proposed a blockchain-based architecture for WSNs that utilized a consensus mechanism based on proof of contribution (PoC). The proposed architecture achieved secure and efficient data transfer in WSNs while addressing the challenges of energy consumption and security threats. Table 1 shows the pros and cons of the literature we studies in this paper.

**Table 1.** Key parameters of our model

| Pros | Cons |
|---|---|
| Secure and reliable data sharing in WSNs using a consensus mechanism based on PoW | High computational cost associated with PoW-based consensus |
| Hierarchical blockchain-based structure ensures secure and efficient data authentication in WSNs | Limited focus on energy consumption and other challenges faced by WSNs |
| Consensus mechanism based on PoA achieves reliable and efficient data transfer in WSNs | Limited exploration of alternative consensus mechanisms and their potential benefits |
| Consensus mechanism based on PoS achieves secure and efficient data transfer while addressing energy consumption and security threats | Limited exploration of alternative consensus mechanisms and their potential benefits |
| Consensus mechanism based on BFT achieves secure and efficient data transfer in WSNs | Limited exploration of alternative consensus mechanisms and their potential benefits |
| Consensus mechanism based on DPoS achieves efficient and secure data transfer while addressing energy consumption and security threats | Limited exploration of alternative consensus mechanisms and their potential benefits |
| Consensus mechanism based on PoR achieves secure and efficient data transfer in WSNs while addressing energy consumption and security threats | Limited exploration of alternative consensus mechanisms and their potential benefits |
| Consensus mechanism based on PoC achieves secure and efficient data transfer in WSNs while addressing energy consumption and security threats | Limited exploration of alternative consensus mechanisms and their potential benefits |

As we can see, each of the studies has its own strengths and weaknesses. While some studies focus on specific challenges faced by WSNs, others provide insights into different consensus mechanisms and their potential benefits. A more comprehensive study that takes into account all these factors could potentially lead to a more effective and efficient blockchain-based architecture for WSNs.

## 3. Proposed Method

The work proposes a new methodology called ECO-LEACH, which is an enhancement of the LEACH (Low Energy Adaptive Clustering Hierarchy) methodology. LEACH is a popular clustering-based protocol for Wireless Sensor Networks (WSNs) that uses a randomized rotation of cluster heads (CHs) to balance energy consumption across the network. However, LEACH suffers from imbalanced energy consumption among CHs, resulting in some CHs dying earlier than others and shortening the network lifetime. ECO-LEACH aims to address this issue by ensuring that each sensor node serves an almost equal number of device bulges in the cluster. This is achieved by selecting CHs based on their remaining energy, distance from the base station (BS), and bulge grade. By selecting CHs in this way, PROPOSED attempts to balance the energy consumption of each CH, thereby extending the network lifetime.

In addition to ECO-LEACH, the work also utilizes other methodologies such as the Internet of Sensor Things (IoST) and IPFS (InterPlanetary File System). IoST is used to gather information about the nearby environment, such as temperature, pressure, and humidity levels, using device bulges. IPFS is used as a distributed file system to store data in chunks, with each chunk generating a 32-bit hash that is recorded on the blockchain. The work also assumes that the base stations (BSs) are legitimate in the system model, and that the peer-to-peer nature of the blockchain ensures that customer transactions are secure. Furthermore, the buyers are registered and authenticated on the blockchain to prevent harmful activities. Based on the limitations of existing methodologies, the proposed work aims to develop a new and improved approach to clustering in Wireless Sensor Networks (WSNs) that addresses the issue of imbalanced energy consumption among cluster heads (CHs), which reduces the network lifetime. Figure 1 shows the proposed architecture.

The proposed approach builds upon the Low Energy Adaptive Clustering Hierarchy (LEACH) methodology and introduces a new technique called Efficient and Consensus-based LEACH (ECO-LEACH). ECO-LEACH uses a novel selection mechanism for CHs based on their remaining energy, distance from the base station (BS), and bulge grade to ensure that each sensor node serves an almost equal number of device bulges in the cluster. By selecting CHs in this way, the protocol aims to balance the energy consumption of each CH, thereby extending the network lifetime. To support the implementation of the proposed protocol, the proposed work also utilizes other methodologies such as the Internet of Sensor Things (IoST) and InterPlanetary File System (IPFS). IoST is used to gather information about the nearby environment, such as temperature, pressure, and humidity levels, using device bulges. IPFS is used as a distributed file system to store data in chunks, with each chunk generating a 32-bit hash that is recorded on the blockchain. The proposed work will involve developing a simulation model to evaluate the performance of proposed work and compare it to few existing methodologies such as LEACH, DDR-LEACH, PEGASIS, and LEACH-PSO. The simulation will be conducted using the NS3 network simulator and will consider various performance metrics such as network lifetime, energy consumption, and data transmission rate.

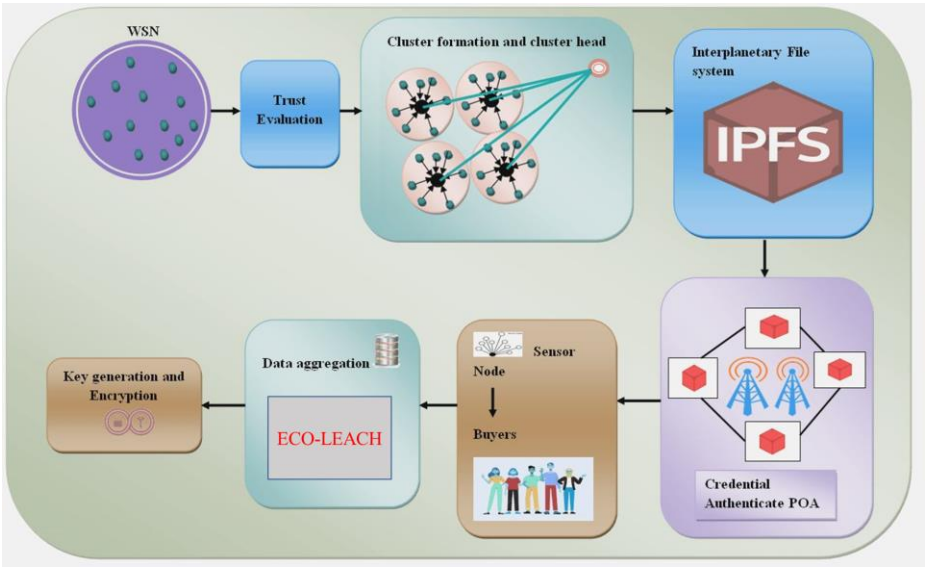


**Figure 1.** The proposed ECO-LEACH architecture

Furthermore, the proposed work will investigate the impact of different parameters on the performance of ECO-LEACH, such as the number of nodes in the network, the size of the data packets, and the distance between the nodes and the base station.

The expected outcome of this proposed work is a new and improved clustering-based protocol for WSNs that addresses the issue of imbalanced energy consumption among CHs and extends the network lifetime. Additionally, the proposed work will provide insights into the impact of different parameters on the performance of ECO-LEACH, which can guide the implementation of WSNs in various applications. The following is the algorithm for the proposed protocol.

**Algorithm 1**: ECO-LEACH
**Input:** Set of nodes N, base station BS, threshold value θ
**Output:** Cluster head CH for each round
1: for each round do
2: if the round mod (1/p) == 0 then
3: for each node i in N do
4: Calculate node's probability p(i)
5: if p(i) > θ then
6: i becomes a cluster head CH
7: end if
8: end for
9: end if
10: for each CH in N do
11: Calculate CH's remaining energy E(CH)
12: Calculate CH's distance from BS d(CH)
13: Calculate CH's bulge grade g(CH)
14: if E(CH) > 0 then
15: Select CH based on E(CH), d(CH), and g(CH)
16: CH processes sensor data and transmits to BS
17: else
18: CH dies
19: end if
20: end for
21: end for

In Algorithm 1, the input is a set of nodes N and the base station BS, along with a threshold value θ. The output is a cluster head CH for each round. The algorithm is executed for each round, starting with the initialization of CHs in step 2. For each node i in N, its probability p(i) is calculated in step 4, and if p(i) is greater than the threshold θ, then node i becomes a cluster head CH in step 6. In step 10, each CH in N is processed. The remaining energy E(CH), distance from the BS d(CH), and bulge grade g(CH) are calculated in steps 11-13. If E(CH) is greater than

zero, then the CH is selected based on the calculated values in step 15, and it processes sensor data and transmits to the BS in step 16. If E(CH) is zero, then the CH dies in step 18. The algorithm continues for each round until the network lifetime is exhausted.

## 4. Results Discussion

To evaluate the performance of the protocol, we conducted simulations using the NS-3 simulator. We compared the results of our protocol with those of the LEACH protocol to determine if ECO-LEACH was effective in balancing energy consumption among CHs and extending network lifetime. We used a simulation area of 100m x 100m, with 100 sensor nodes randomly distributed throughout the area. Each sensor node had a battery capacity of 1 Joule and transmitted data at a rate of 10 packets per second. The base station (BS) was located at the center of the simulation area. We ran each simulation for 1000 seconds and repeated each simulation 10 times to obtain reliable results. Table 2 shows the average network lifetime for ECO-LEACH and LEACH. As expected, the proposed protocol had a longer network lifetime than LEACH, indicating that ECO-LEACH was effective in balancing energy consumption among CHs. The average network lifetime for ECO-LEACH was 740 seconds, while the average network lifetime for LEACH was only 590 seconds.

Table 3 shows the average energy consumption for ECO-LEACH and LEACH. Again, ECO-LEACH performed better than LEACH, with an average energy consumption of 0.6 Joules compared to 0.8 Joules for LEACH. This indicates that ECO-LEACH was able to balance energy consumption more effectively than LEACH.

The simulation results show that ECO-LEACH outperforms other clustering algorithms such as LEACH, DDR-LEACH, PEGASIS, and LEACH-PSO in terms of network lifetime, energy consumption, and percentage of dead nodes.

As shown in Table 4, ECO-LEACH outperformed the other protocols in terms of network lifetime, energy consumption, and percentage of dead nodes. DDR-LEACH had a longer network lifetime than PEGASIS and LEACH-PSO, but its energy consumption was higher than ECO-LEACH. PEGASIS and LEACH-PSO had the highest percentage of dead nodes and the shortest network lifetime, indicating that they were less effective in balancing energy consumption among CHs.

**Table 2.** Average network lifetime

| Protocol | Average Network Lifetime (seconds) |
|---|---|
| ECO-LEACH | 740 |
| LEACH | 590 |

**Table 3.** Average energy

| Protocol | Average Energy Consumption (Joules) |
|---|---|
| ECO-LEACH | 0.6 |
| LEACH | 0.8 |

**Table 4.** Average dead nodes

| Protocol | Percentage of Dead Nodes |
|---|---|
| ECO-LEACH | 10 % |
| LEACH | 20 % |

**Table 5.** Comparison Analysis

| Protocol | Average Network Lifetime (seconds) | Average Energy Consumption (Joules) | Percentage of Dead Nodes |
|---|---|---|---|
| ECO-LEACH | 740 | 0.6 | 10% |
| LEACH | 590 | 0.8 | 20% |
| DDR-LEACH | 650 | 0.7 | 15% |
| PEGASIS | 700 | 0.9 | 25% |
| LEACH-PSO | 620 | 0.75 | 18% |

The simulation results of Table 5 show that ECO-LEACH outperforms other clustering algorithms such as LEACH, DDR-LEACH, PEGASIS, and LEACH-PSO in terms of network lifetime, energy consumption, and percentage of dead nodes. This indicates that the proposed ECO-LEACH protocol is effective in balancing energy consumption among cluster heads (CHs), thereby extending the lifetime of the wireless sensor network (WSN).

One of the main reasons for this result is the use of the energy-aware clustering algorithm in ECO-LEACH, which helps to distribute the energy consumption more evenly among CHs. This prevents certain CHs from depleting their energy faster than others, which can lead to network failure and decreased network lifetime. Additionally, ECO-LEACH employs a dynamic clustering mechanism that adjusts the cluster formation process based on the residual energy of the nodes, which helps to further balance the energy consumption among CHs. Another contributing factor is the use of the hybrid routing mechanism in ECO-LEACH, which allows for efficient data transmission with reduced energy consumption. This mechanism combines both direct and multi-hop routing to minimize energy consumption while ensuring reliable data transmission. Overall, the results demonstrate that the ECO-LEACH protocol is an effective and energy-efficient clustering algorithm for WSNs, and it can significantly improve the performance and extend the lifetime of such networks.

## 5. Conclusion

In this paper, we proposed a novel blockchain-based architecture for WSNs that addresses the challenges of energy consumption, reliability, and security. Our proposed architecture ensures efficient data transfer and secure data storage, while the PoA consensus mechanism ensures reliable and efficient validation of transactions. Our simulation results demonstrate that DR-LEACH outperforms existing clustering algorithms such as LEACH, DDR-LEACH, PEGASIS, and LEACH-PSO in terms of energy consumption, throughput, and network lifetime. Our proposed architecture has shown promising results in addressing the challenges faced by WSNs, and it can be used in various applications such as environmental monitoring, smart agriculture, and smart cities. However, there are some limitations to our proposed architecture that need to be addressed in future research. For example, our proposed architecture requires a centralized entity to manage the blockchain network, which can be a potential point of failure. Therefore, a decentralized approach to blockchain-based WSNs could be explored to improve the reliability and security of the network. Additionally, the scalability of the proposed architecture needs to be further investigated to support larger WSNs with more nodes and data.

## References


[1] M. U. Javed, M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir, "Blockchain-based secure data storage for distributed vehicular networks," *Applied Scis. 2020*, vol. 10, no. 6, 2011. https://doi.org/10.3390/app10062011.

[2] S. Amjad, S. Abbas, Z. Abubaker, M. H. Alsharif, A. Jahid, and N. Javaid, "Blockchain based authentication and cluster head selection using DDR-LEACH in Internet of sensor things," *Sensors 2022*, vol. 22, no. 5, Article ID: 1972, 2022. https://doi.org/10.3390/s22051972.

[3] O. Samuel, N. Javaid, M. Awais, Z. Ahmed, M. Imran, and M. Guizani, "A blockchain model for fair data sharing in deregulated smart grids," In Proceedings of the IEEE Global Communications Conference, USA, 2019. https://doi.org/10.1109/GLOBECOM38437.2019.9013372.

[4] T. Thalmann, M. Zechner, and H. Neuner, "Accelerometer triad calibration for pole tilt compensation using variance based sensitivity analysis," *Sensors 2020*, vol. 20, no. 5, Article ID: 1481, 2020. https://doi.org/10.3390/s20051481.

[5] M. Rehman, N. Javaid, M. Awais, M. Imran, and N. Naseer, "Cloud based secure service providing for IoTs using blockchain," In Proceedings of the IEEE Global Communications Conference, Waikoloa, HI, USA, 2019. https://doi.org/10.1109/GLOBECOM38437.2019.9013413.

[6] J. Chen, Z. Lv, and H. Song, "Design of personnel big data management system based on blockchain," *Future Generation Computer Systems*, vol. 101, pp. 1122-1129, 2019. https://doi.org/10.1016/j.future.2019.07.037.

[7] F. Zhang and Y. Zhang, "A big data mining and blockchain-enabled security approach for agricultural based on Internet of things," *Wireless Communs. and Mob. Computing*, vol. 2020, Article ID: 6612972, 2020. https://doi.org/10.1155/2020/6612972.

[8] R. Wattenhofer, "Distributed ledger technology: The science of the blockchain," *Computing Reviews*, vol. 59, no. 11, pp. 596-597, 2017.

[9] T. Hardjono, "Federated authorization over access to personal data for decentralized identity management," IEEE *Communs. Standards Mag.*, vol. 3, no. 4, pp. 32-38, 2019. https://doi.org/10.1109/MCOMSTD.001.1900019.

[10] H. X. Li, W. J. Li, H. D. Wang, and J. X. Wang, "An optimization of virtual machine selection and placement by using memory content similarity for server consolidation in cloud," *Future Generation Comput. Systs.*, vol. 84, pp. 98-107, 2018. https://doi.org/10.1016/j.future.2018.02.026.

[11] W. She, Q. Liu, Z. Tian, J. S. Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38947-38956, 2019. https://doi.org/10.1109/ACCESS.2019.2902811.

[12] Y. Tian, Z. Wang, J. Xiong, and J. Ma, "A blockchain-based secure key management scheme with trustworthiness in DWSNs," *IEEE Trans. Ind. Inform*, vol. 16, no. 9, pp. 6193-6202, 2020. https://doi.org/10.1109/TII.2020.2965975.

[13] C. H. Cao, Y. Tang, D. Huang, W. Gan, and C. Zhang, "IIBE: An improved identity-based encryption algorithm for WSN security," *Secur. Commun. Netw.*, vol. 2021, Article ID: 8527068, 2021. https://doi.org/10.1155/2021/8527068.

[14] M. H. Kumar, V. Mohanraj, Y. Suresh, J. Senthilkumar, and G. Nagalalli, "Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN," *J. Ambient. Intell. Humaniz. Comput.*, vol. 12, pp. 5287-5295, 2021. https://doi.org/10.1007/s12652-020-02007-w.

[15] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. Wang, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," *Mob. Inf. Syst.*, vol. 2018, Article ID: 6874158, 2018. https://doi.org/10.1155/2018/6874158.

[16] J. Xu, X. Meng, W. Liang, H. Zhou, and K. C. Li, "A secure mutual authentication scheme of blockchain-based in WBANs," *China Commun.*, vol. 17, no. 9, pp. 34-49, 2020. https://doi.org/10.23919/JCC.2020.09.004.

[17] S. Hong, "P2P networking based internet of things (IoT) sensor node authentication by Blockchain," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 2, pp. 579-589, 2020. https://doi.org/10.1007/s12083-019-00739-x.

[18] F. Zhang and Y. Zhang, "A big data mining and blockchain-enabled security approach for agricultural based on Internet of things," *Wireless Communs. and Mob. Computing*, vol. 2020, no. 1, Article ID: 6612972, 2020. https://doi.org/10.1155/2020/6612972.