Blockchain based Authentication for end-nodes and efficient Cluster Head selection in Wireless Sensor Networks

Sana Amjad[1], Usman Aziz[2], Muhammad Usman Gurmani[1], Saba Awan[1], Maimoona Bint E Sajid[1], Nadeem Javaid[1,*]

[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
[2]Department of Computer Science, COMSATS University Islamabad, Attock 43600, Pakistan
Email: Sanaamjad702@gmail.com, usmanaziz91@gmail.com,
usmankhangurmani@gmail.com, sabaawan046@gmail.com, maimoonasajid176@yahoo.com,
*Correspondence: nadeemjavaidqau@gmail.com; www.njavaid.com

***Abstract*—In this paper, a secure blockchain based identity authentication for end-nodes is proposed in wireless sensor networks (WSNs). Moreover, to resolve the issue of limited energy in WSNs, a mechanism of cluster head (CH) selection is also proposed. The nodes in a network are authenticated on the basis of credentials to prevent from malicious activities. The malicious nodes harm the network by providing false data to nodes. Therefore, a blockchain is integrated with the WSN to make the network more secure as it allows only authenticated nodes to become a part of the network. Moreover in a WSN, sensor nodes collect the information and send it towards CH for further processing. The CH aggregates and processes the information; however, its energy depletes rapidly due to extra workload. Therefore, the CH is replaced with the node that has the highest residual energy among all nodes. The simulation result shows the network lifetime increases after CH replacement. Moreover, it shows that he transaction cost is very low during authentication phase.**

***Index Terms*—Blockchain, Wireless Sensor Networks, Identity Authentication.**

I. Introduction

The wireless sensor networks (WSNs) are useful in sensing the environmental or physical changes in healthcare, surveillance, transportation, etc. The sensors in WSN are randomly deployed for environmental monitoring [1], [2]. The sensor nodes have many constraints, which are limited battery, less computation capabilities, low storage, etc., [3], [4].

Satoshi Nakamoto introduced blockchain in 2008 that has emerged as a promising technology to address the issues of data securitand remove dependency on the third party [5]. The blockchain is used in the field of healthcare, energy trading, smart grids etc. It gives a secure, decentralized, a distributed mechanism for storage and addresses the single point of failure issue. The blockchain provides a tamper-proof ledger in which a new record is added after being validated by the miners. The miner nodes validate the transactions by different consensus mechanisms: proof of work (PoW), proof of authority (PoA), proof of stack(PoS) etc., [6], [7]. In the PoW, all the interested nodes participate and solve a mathematical puzzle. The node, which solves the puzzle first is responsible for validating the transaction and adding a block in the blockchain. This process consumes a lot of computational power, which is not suitable for energy constrained WSNs. Moreover, the blockchain uses the smart contracts in which all the business rules are stored and it removes the need of any external third party. In PoA, only pre-selected nodes are responsible for mining, these nodes are selected on the bases of their capabilities. Because, the miners are pre-selected node; therefore, they do not have to solve the mathematical puzzle that requires high computation. Moreover, blockchain plays an important role in WSN and provides security and privacy in them [8], [9]. It provides security by detecting the malicious nodes in the network. There are many techniques for malicious nodes detection [10], [11]. However, blockchain faces the issue of high storage cost which is not suitable for WSN that are not resource enriched.

In the WSNs, sensor nodes gather data from the environment and forward it to CH for further processing. The CH process the data and forward it to the base station (BS). The nodes in the network are registered as well as authenticated to prevent from malicious acts. In [12], CHs send the sensed data to BS; however, there is no registration and authentication mechanism for the network nodes. The malicious nodes can enter into the network and make it vulnerable.

Whenever a node fails due to energy depletion in the network, it affects the whole networks' performance. There is no mechanism in [13], [14] for the selection of CH. When any CH fails to perform due to serve the network due to its low energy, there is no criteria of selecting a new CH.

The list of contributions of this paper are as following:

- nodes' authentication is performed to prevent the network from malicious activities,
- a smart contract is used to resolve the trust issue by removing third party, and
- the CH is selected on the basis of nodes' highest energy by using low-energy adaptive clustering hierarchy (LEACH) protocol.

II. Related work

In this section, relevant studies of blockchain in WSNs are dicussed based upon limitations addressed.

A. Registration and authentication of nodes

The nodes in the IoT environment cooperate to provide the services. However, in [6] and [14], nodes' identity authentication is compromised, any node can enters in network and behaves maliciously which affects the network performance. The node identity authentication relies on the central authentication server.

The sensors play an important part in IoT for different purposes and one of them is nodes' identity authentication. However, sensors have very low computational power. In [13], the authentication issue occurs because of non authenticated nodes can enter in network and act maliciously. While in [15], users' privacy and authenticity need to be assured. As in [16] the routing protocol is used to authenticate the devices; however, the trust issue is created due to centralized authority. In [17], the wireless body area network consists of sensors that gather the data of human body parts and send it to the local node publically. However, the nodes in the network are not authenticated.

B. Storage issues in network nodes

In [18], the sensor nodes have some constraints such as low storage and low computational power. Moreover, some nodes in the network behave selfishly and do not store the data. The PoW mechanism is used in previous work that consumes much computational power. Whereas, in [19], a static routing protocol is not good for the internet of underwater things (IoUT) and there is a storage issue in the centralized system. Also, in [20], PoW consensus is used. However, it consumes high computational power and storage.

In addition to the problems discussed above, in [21], IoT is integrated with the blockchain in a centralized manner and PoW is used for the mining process. However, it creates central point of failure due to central authority. In the network each node stores data that is generated by other nodes. However, the storage issue occurs. While in [22], the nodes data record is stored in a centralized system that creates single point of failure. Whereas in [23], blockchain is integrated with IoTs. However, it is not suitable for keeping a copy of the ledger due to storage constraints.

C. Data privacy of nodes

In [12], no mechanism is proposed for data protection due to which any malicious node can steal data and harm the network. Whereas in [24], the controlling and take care of the manufacturing products in the industry are done by the workers; however, data transparency issue occurs. The workers can steal the restricted product information. Moreover, the misuse of important records is another issue. Also, in [6], the data security and privacy of sensor nodes are compromised in the WSNs.

In [25], crowdsensing is essentially used to collect information using different devices. However, no data privacy protection mechanism is used. As in [26], the dynamic WSNs play an important role in collecting data; however, the untrusted behavior of nodes occurs. Whereas, in [15], users' data privacy and authenticity need to be assured. Whereas in [27], the information-centric network (ICN) is integrated with a WSN. The caching data is duplicated and shared in the network. However, data privacy and security concerns may occur. While in [28], the concept of a smart city is developed with the integration of IoT. However, due to data growth and no management, data security issues occur. In [29], the data is transmitted from sensor nodes to IoT devices; however, there is no mechanism for data protection.

D. Excessive energy consumption

In [18], the sensing nodes in the network selfishly behave and do not store the data. The PoW mechanism is used in previous work that consumes much computational power. Also, in [20], blockchain technology is used in different fields for trading and supply chain purposes. PoW is used as consensus mechanism that consumes high computational power.

In [23], blockchain is integrated with IoT. However, IoT nodes are less competitive and are not able to keep a copy of the ledger due to low energy. Whereas, in [30], IOTA is a distributed ledger that provides fast and tamper-proof information. However, the ndes' information gathering rate is very low. The IoT sensors may have the very low computational power and their energy may decreases very fast. It creates a problem for IoT to validate the transactions very fast. While in [31], sensor nodes do not have enough battery to survive in the network and not able to communicate for a long time. In [32], the wireless body area networks work evolutionary with the healthcare applications. However, it consumes a lot of energy consumption.

E. Malicious nodes detection and removal from networks

In a WSN, localization of sensor nodes is the major issue nowadays. There are some nodes in the WSN, which give the wrong location and act maliciously. In this way, network security is compromised in [33]. Whereas, in [34], there is no proper mechanism for the detection of malicious nodes. Moreover, there is no traceability mechanism for the detection of malicious nodes. Also, in [35], the industrial IoT (IIoT) is being used in different fields such as manufacturing, healthcare. However, some service provisioning challenges occur. In service provisioning challenges, the untrusted service provider can act maliciously and provide the wrong services. On the other side, the client can acts maliciously by repudiating against the services.

In [18], the nodes in the network selfishly behave and do not store the data. Whereas in [36], sensor nodes communicate by finding the routing path. However, no best way is used to find the malicious node and secure the data to be infected. While in [37], the range based localization approach needs hardware for finding the precise location and it becomes very costly. Moreover, the range-free approach is affected by the malicious nodes in the network. In [38], cloud based computing is performed; however, data is retrieved through the internet and no data security mechanism is performed.

F. Single point of failure issue due to centralized authority

In [14], nodes' identity authentication is compromised, which affects the network performance. The node identity authentication relies on central authentication servers that are considered third parties and cause single point of failure. Whereas in [39], authors compare the centralized and distributed network model. In a centralized system, the data sent to the cloud directly; however, data bandwidth and data latency issues arise. In a distributed system, fog computing is used; however, a single point of failure issue arises.

In [16], in the routing protocol, the central devices are used to authenticate the devices; however, a trust issue is created due to centralized authority. While in [22], shellfish products are the most popular food throughout the globe. Its freshness is needed for long time storage. Cold storage is needed for maintaining its freshness. A WSN is a beneficial and great impact on managing the cold operation. However, their records are stored in a centralized system that creates single-point failure and malicious attacks. In [40], the central authority is used for data storage. However, single-point of failure issue is created.

In the Table 1, the problems, their solutions and validation parameters are mentioned. For intrusion prevention of malicious nodes, an authentication scheme is used. By using authentication scheme, only authenticated nodes enter into the network. The node battery issue resolved by selecting the highest energy node using the LEACH protocol [41].

III. Proposed System Model

In the proposed system model, a blockchain based model is proposed for establishing the secure communication between authentic nodes and CH.

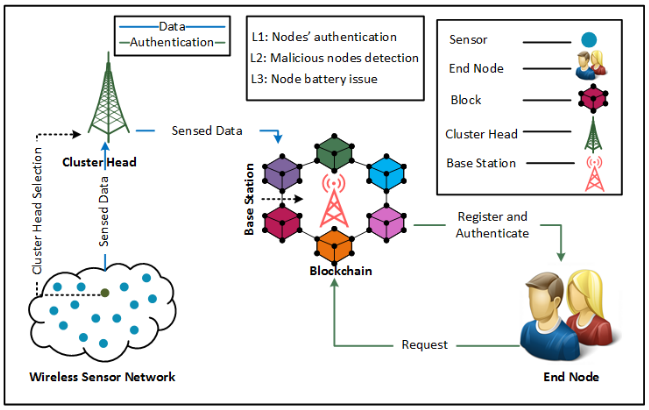

Fig. 1: System model for end-nodes authentication and CH selection

A. System components

The system model comprises of three primary entities: end-nodes, CH and BS.

1) Sensor node:: In a WSN, the sensor nodes sense data from the environment. These nodes are resource constrained and not able to store the large amount of data. Therefore, they send data to the CH for further computation and storage.

2) Cluster head:: The CH receives data from sensor nodes, processes and stores it on BS. Our proposed model provides a mechanism for the selection of CH on the basis of its residual energy, when the battery of existing CH depletes. For this, the energy of each sensor node in the network is calculated and the node with highest residual energy is selected as cluster head.

3) Base station:: The blockchain is deployed on BS, which has sufficient resources for performing the validating transactions. The BS stores sensing data and the credentials of registered nodes. The CH then send data to BS for storage.

4) End-node:: Nodes' registration and authentication scheme is used to prevent network from malicious activities. The authentication scheme use in this paper is motivated by [14], the authentication scheme is used in this paper. In the proposed system model, this scheme is used for private blockchain. The unknown end-node sends a request to the blockchain for registration. Initially, the blockchain checks either this node is already registered in the network or not. If end-node is already registered, then it will not be re-registered in the network and proceed further otherwise, the blockchain registers it. When any end-node wants some data from the network, then it will authenticate firstly. The end-node is authenticated on the bases of its credentials stored on the blockchain at the time of registration. At the request time the end-node provides its credentials, if these credentials are same with the credentials stored on the blockchain, then it will be considered as authenticated node. Otherwise, this specific end-node will be announced as a malicious node and rapidly removed from the network. After authentication, the end-user is allowed to get the data from the network.

5) Smart contract:: A smart contract is a digital contract, which is deployed on blockchain for handling the transactions without the involvement of any third party. In this paper, PoA consensus mechanism is used for nodes' authentication that consumes less computational power because pre selected nodes perform mining process.

IV. Simulation Results and Discussion

This section demonstrates the analysis of the proposed solution. Fig. 2 depicts the message size during registration and authentication phase. During registration, nodes send request to enter in the network. The nodes send their credentials for registration. Their credentials are stored in BS, whenever end-node enters in the network first it is authenticated. The authentication is performed by BS. The message size for registration is high because much of the network resources like bandwidth and throughput are used in sending the data to the blockchain.

TABLE I: Mapping of problems to solutions and validations

Limitations	Proposed Solutions	Validations
L1. Nodes' registration and authentication [12]. L2. Malicious nodes detection [12]	S1. Authentication technique	V1. Message size V2. Transaction cost
L3. Node battery issue [13], [14]	S2. LEACH protocol	V3. Network lifetime

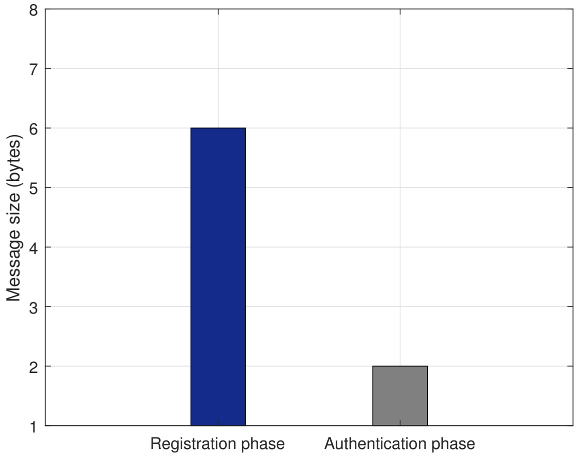

Fig. 2: Registration and authentication message size for end-nodes

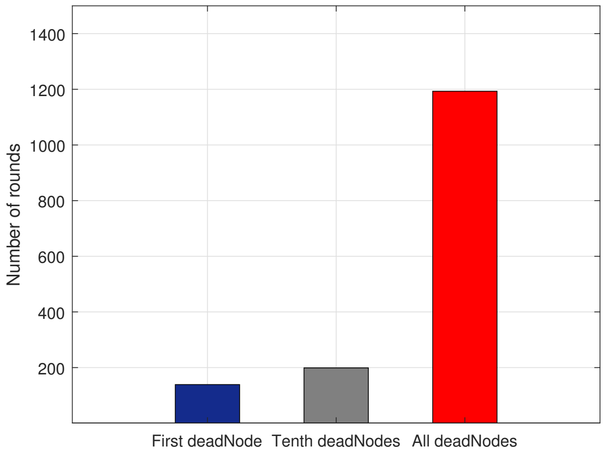

Fig. 3: Network lifetime

On the other hand, during authentication, less network resources are used because BS has only to match the credentials to verify end-nodes' credentials. Only authenticated nodes take part in the network. PoA consensus mechanism is used in our proposed model to validate transactions. In this way, malicious nodes are not allowed in the network to do malicious activities. Fig. 3 illustrates the network lifetime and shows the number of dead nodes based on number of rounds. There are 200 sensor nodes and from these sesors, CH is selected on the basis of highest residual energy. The energy of first CH depletes at round No. 180. The energy of ten node depletes at round No. 200. The energy of all the nodes depletes at round No. 1200. This shows that the network has good lifetime. The use of LEACH protocol is to prolong the network lifetime and reduce the energy consumption of nodes.

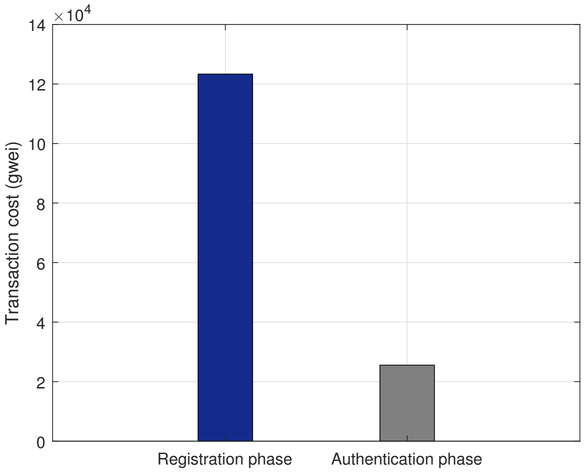

Fig. 4: Transaction cost

Fig. 4 illustrates the transaction cost of registration and authentication of end-nodes. The transaction cost in registration phase is greater than the authentication phase. Because during registration phase, blockchain stores all the information of nodes one by one to register end-nodes that takes much cost as compared to authentication phase. During authentication phase only the nodes have to authenticate from the information that is already provided during registration phase. That is the reason it does not take much time for authentication process.

V. Conclusion and future work

The aim of this paper is to enhance the network lifetime as well as to prevent it from malicious nodes. Therefore, identity authentication scheme is used to register the nodes and then authenticate them. The unknown nodes first register themselves and then authenticate them to enter in the network. In this way, only legitimate nodes become a part of the network. The LEACH protocol is integrated with blockchain to enhance the network lifetime because CHs with low energy are replaced by highest energy CH node. On other side, identity authentication scheme is used to make the network more secure because only legitimate nodes can enter in the network. In the future work, services will be provided to legitimate nodes. The sensed data will be stored in a storage system.

Also, the computational cost will be checked as comparison for authentication and storage.

REFERENCES

[1] Fu, M. H. (2020). Integrated Technologies of Blockchain and Biometrics Based on Wireless Sensor Network for Library Management. Information Technology and Libraries, 39(3).

[2] Kumari, S., and Om, H. (2016). Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. Computer Networks, 104, 137-154.

[3] Jiang, Q., Zeadally, S., Ma, J., and He, D. (2017). Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. IEEE Access, 5, 3376-3392.

[4] Farooq, H., Arshad, M. U., Akhtar, M. F., Abbas, S., Zahid, B., Javaid, N. (2019, November). Block-VN: A distributed blockchain-based efficient communication and storage system. In International Conference on Broadband and Wireless Computing, Communication and Applications (pp. 56-66). Springer, Cham.

[5] Padmavathi, U., and Rajagopalan, N. (2021). Concept of Blockchain Technology and Its Emergence. In Blockchain Applications in IoT Security (pp. 1-20). IGI Global.

[6] Moinet, A., Darties, B., and Baril, J. L. (2017). Blockchain based trust and authentication for decentralized sensor networks. arXiv preprint arXiv:1706.01730.

[7] Abubaker, Z., Gurmani, M. U., Sultana, T., Rizwan, S., Azeem, M., Iftikhar, M. Z., Javaid, N. (2019, November). Decentralized Mechanism for Hiring the Smart Autonomous Vehicles Using Blockchain. In International Conference on Broadband and Wireless Computing, Communication and Applications (pp. 733-746). Springer, Cham.

[8] Goyat, R., Kumar, G., Saha, R., Conti, M., Rai, M. K., Thomas, R., ... and Hoon-Kim, T. (2020). Blockchain-based Data Storage with Privacy and Authentication in Internet-of-Things. IEEE Internet of Things Journal.

[9] Abbas, S., Javaid, N. (2019, December). Blockchain based Vehicular Trust Management and Less Dense Area Optimization. In 2019 International Conference on Frontiers of Information Technology (FIT) (pp. 250-2505). IEEE.

[10] Christidis, K., and Devetsikiotis, M. (2018). Blockchains and smart contracts for the Internet of Things. Journal of Fintech, Blockchain, and Smart Contracts, 1(1), 7-12.

[11] Magazzeni, D., McBurney, P., and Nash, W. (2017). Validation and verification of smart contracts: A research agenda. Computer, 50(9), 50-57.

[12] Haseeb, K., Islam, N., Almogren, A., and Din, I. U. (2019). Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things. Ieee Access, 7, 185496-185505.

[13] Hong, S. (2020). P2P networking based internet of things (IoT) sensor node authentication by Blockchain. Peer-to-Peer Networking and Applications, 13(2), 579-589.

[14] Cui, Z., Fei, X. U. E., Zhang, S., Cai, X., Cao, Y., Zhang, W., and Chen, J. (2020). A hybrid BlockChain- based identity authentication scheme for multi-WSN. IEEE Transactions on Services Computing, 13(2), 241-251.

[15] Kolumban-Antal, G., Lasak, V., Bogdan, R., and Groza, B. (2020). A Secure and Portable Multi-Sensor Module for Distributed Air Pollution Monitoring. Sensors, 20(2), 403.

[16] Ramezan, G., and Leung, C. (2018). A blockchain-based contractual routing protocol for the internet of things using smart contracts. Wireless Communications and Mobile Computing, 2018.

[17] Xu, J., Meng, X., Liang, W., Zhou, H., and Li, K. C. (2020). A secure mutual authentication scheme of blockchain-based in WBANs. China Communications, 17(9), 34-49.

[18] Ren, Y., Liu, Y., Ji, S., Sangaiah, A. K., and Wang, J. (2018). Incentive mechanism of data storage based on blockchain for wireless sensor networks. Mobile Information Systems, 2018.

[19] Uddin, M. A., Stranieri, A., Gondal, I., and Balasurbramanian, V. (2019). A lightweight blockchain based framework for underwater iot. Electronics, 8(12), 1552.

[20] Liu, M., Yu, F. R., Teng, Y., Leung, V. C., and Song, M. (2018). Computation offloading and content caching in wireless blockchain networks with mobile edge computing. IEEE Transactions on Vehicular Technology, 67(11), 11008-11021.

[21] Liu, Y., Wang, K., Lin, Y., and Xu, W. (2019). LightChain: A Lightweight Blockchain System for Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 15(6), 3571-3581.

[22] Feng, H., Wang, W., Chen, B., and Zhang, X. (2020). Evaluation on frozen shellfish quality by blockchain based multi-sensors monitoring and SVM algorithm during cold storage. IEEE Access, 8, 54361-54370.

[23] Danzi, P., Kalør, A. E., Stefanović, Č., and Popovski, P. (2019). Delay and communication tradeoffs for blockchain systems with lightweight IoT clients. IEEE Internet of Things Journal, 6(2), 2354-2365.

[24] Rathee, G., Balasaraswathi, M., Chandran, K. P., Gupta, S. D., and Boopathi, C. S. (2020). A secure IoT sensors communication in industry 4.0 using blockchain technology. Journal of Ambient Intelligence and Humanized Computing, 1-13.

[25] Jia, B., Zhou, T., Li, W., Liu, Z., and Zhang, J. (2018). A blockchain-based location privacy protection incentive mechanism in crowd sensing networks. Sensors, 18(11), 3894.

[26] Tian, Y., Wang, Z., Xiong, J., and Ma, J. (2020). A blockchain-based secure key management scheme with trustworthiness in DWSNs. IEEE Transactions on Industrial Informatics, 16(9), 6193-6202.

[27] Mori, S. (2018). Secure caching scheme by using blockchain for information-centric network-based wireless sensor networks. Journal of Signal Processing, 22(3), 97-108.

[28] Sharma, P. K., and Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. Future Generation Computer Systems, 86, 650-655.

[29] Guerrero-Sanchez, A. E., Rivas-Araiza, E. A., Gonzalez-Cordoba, J. L., Toledano-Ayala, M., and Takacs, A. (2020). Blockchain mechanism and symmetric encryption in a wireless sensor network. Sensors, 20(10), 2798.

[30] Rovira-Sugranes, A., and Razi, A. (2019). Optimizing the Age of Information for Blockchain Technology With Applications to IoT Sensors. IEEE Communications Letters, 24(1), 183-187.

[31] Sergii, K., and Prieto-Castrillo, F. (2018). A rolling blockchain for a dynamic WSNs in a smart city. arXiv preprint arXiv:1806.11399.

[32] Shahbazi, Z., and Byun, Y. C. (2020). Towards a secure thermal-energy aware routing protocol in Wireless Body Area Network based on blockchain technology. Sensors, 20(12), 3604.

[33] Kim, T. H., Goyat, R., Rai, M. K., Kumar, G., Buchanan, W. J., Saha, R., and Thomas, R. (2019). A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks. IEEE Access, 7, 184133-184144.

[34] She, W., Liu, Q., Tian, Z., Chen, J. S., Wang, B., and Liu, W. (2019). Blockchain trust model for malicious node detection in wireless sensor networks. IEEE Access, 7, 38947-38956.

[35] Xu, Y., Ren, J., Wang, G., Zhang, C., Yang, J., and Zhang, Y. (2019). A blockchain-based nonrepudiation network computing service scheme for industrial IoT. IEEE Transactions on Industrial Informatics, 15(6), 3632-3641.

[36] Kumar, M. H., Mohanraj, V., Suresh, Y., Senthilkumar, J., and Nagalalli, G. (2020). Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN. Journal of Ambient Intelligence and Humanized Computing, 1-9.

[37] Goyat, R., Kumar, G., Rai, M. K., Saha, R., Thomas, R., and Kim, T. H. (2020). Blockchain Powered Secure Range-Free Localization in Wireless Sensor Networks. Arabian Journal for Science and Engineering, 45(8), 6139-6155.

[38] Rahman, A., Islam, M. J., Khan, M. S. I., Kabir, S., Pritom, A. I., and Karim, M. R. (2020). Block-SDoTCloud: Enhacing Security of Cloud Storage through Blockchain-based SDN in IoT Network.

[39] Rathore, S., Kwon, B. W., and Park, J. H. (2019). BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. Journal of Network and Computer Applications, 143, 167-177.

[40] Lee, Y., Rathore, S., Park, J. H., and Park, J. H. (2020). A blockchain-based smart home gateway architecture for preventing data forgery. Human-centric Computing and Information Sciences, 10(1), 1-14.

[41] Heinzelman, W. R., Chandrakasan, A., Balakrishnan, H. (2000, January). Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd annual Hawaii international conference on system sciences (pp. 10-pp). IEEE.