Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Hybrid Security Model for IoT Integration with LEACH Clustering and Blockchain

Mannava sainadh charan

2200050031ecs@gmail.com

koneru lakshmaih education foundation https://orcid.org/0009-0005-0167-0430

Bavvannagari harini

koneru lakshmaih education foundation

Tavidisetty Mokshita valli

koneru lakshmaih education foundation

J Rajasekhar

konerulakshmaih education foundation

Research Article

Keywords: Internet of Things, LEACH, Blockchain, Security, Clustering, Energy Efficiency

Posted Date: March 31st, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9270061/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

Hybrid Security Model for IoT Integration with LEACH Clustering and Blockchain

Abstract

The rapid increase in the number of Internet of Things (IoT) networks has caused significant security issues. IoT devices have limited resources and are vulnerable to various attacks since they use a centralized architecture and poor routing [1]. This research proposes a hybrid security system based on blockchain technology and the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol to address security issues in IoT networks. LEACH clustering helps to reduce energy consumption and extend the lifetime of the network. Blockchain also makes sure that data communication is safe, decentralized, and can't be changed. The smart thing is that only the clusterheads do blockchain tasks, so the system doesn't have to deal with too much communication. That makes it perfect for large IoT systems. Tests demonstrate that this configuration uses less energy, keeps your data safer, and fights off security attacks better than prior IoT solutions [2].

Index Terms—Internet of Things, LEACH, Blockchain, Security, Clustering, Energy Efficiency

INTRODUCTION

Intelligent applications are required, such as smart cities, industrial automation, alarming and monitoring of health care systems. Internet of Things is also linked to high security risks even though its benefits are many due to lack of sufficient computational power, tremendous scale implementation, and absence of centralized trust applications [3]. Conventional security systems do not appear to be appropriate in IoT environments due to their high computational and power demands.

Clustering based routing protocols such as Low-Energy Adaptive Clustering Hierarchy (LEACH) are widely employed to improve energy efficiency in wireless sensor and IoT networks. However, LEACH does not essentially provide strong security guarantees [4].

Blockchain technology can provide decentralization, immutability, and transparency, therefore it may be an important method for securing IoT systems. In this paper, LEACH and blockchain are integrated to strike a balance between energy usage and secure communication.

LITERATURE SURVEY

When people look at studies on IoT networks, they usually divide them into three key parts: sensing and communication, routing that uses less energy, and security and trust management. The initial aim was to reduce energy consumption, especially at the network layer. Heinzelman and his team came up with the LEACH protocol that placed sensor nodes into clusters effectively [5]. Periodically, each cluster selects a new Cluster Head (CH), and nodes transmit their data to the CH rather than sending it to the base station. This reduces the overall energy consumption since the CH may aggregate data and distribute the responsibility. Later, researchers like Akyildiz and Comeau studied LEACH and similar protocols to extend the lifetime of the network and consume energy uniformly. However, the initial protocols lacked security [6].

However, people turned to blockchain technology when they started to worry about security issues in the larger IoT systems. Nakamoto's idea of creating a blockchain network indicated that one doesn't need a central authority to obtain a ledger that everyone can trust. After that, other scholars, such as Khan, Xu, and Uddin, tried to integrate blockchain technology with the Internet of Things, allowing devices to store and verify data on the shared ledgers [4][5][6]. The problem, however, was that most IoT devices lacked the required computational power to support the required activities for the blockchain network.

To address the problem, scientists tried to mix and match the solutions. For example, Emira and Al-Turjman tried to develop configurations that would allow only the more powerful devices, such as gateways, to perform the more difficult work of the blockchain network, while the other devices, such as the sensors, would perform the easier work [7][13]. Nie and others tried to take it a step further and develop lightweight consensus procedures to reduce the required work while ensuring security at the same time [6]. All the above solutions are based on the same idea of creating a layered architecture that allows IoT devices to perform their detecting functions while moving the more difficult work to other places.

Amjad and his team have attempted something new. They have used the combination of blockchain and clustering protocols like LEACH. In the new method proposed by the team, only cluster heads are used with the blockchain. Sensor nodes are left to perform their traditional functions of collecting and communicating data. This has the advantage of conserving energy while still benefiting from the advantages of the blockchain. Reyna and Dorri have also discussed the broader picture of the strategies for the implementation of the blockchain in IoT networks through the development of hierarchical models of the blockchain.

So, if we take a step back, we can see the development of the field. Initially, they were trying to save energy. Then, they were trying to improve the security of the IoT networks. Now, they are trying to find a balance between the two. The proposed architecture is based on the fact that the combination of the LEACH cluster heads and the blockchain will result in IoT networks that are safe, efficient, and scalable[13].

RELATED WORK

Research studies have been conducted to increase the energy efficiency of IoT networks through the application of clustering-based routing protocols. The main objective of the LEACH and its variants is to increase the network's longevity through the optimization of cluster head selection. Although the standards are helpful in increasing the network's efficiency, they lack security features.

It has been proposed that the application of blockchain-based IoT security frameworks can make the sharing of data safe and sound. However, using the blockchain technology directly in the IoT devices makes them consume a lot of processing and communication resources. The existing solutions do not offer the right balance between security and efficiency. The proposed hybrid solution avoids the mentioned problem since it only uses the blockchain at the cluster head level.

PROPOSED HYBRID SECURITY MODEL

The framework that has been proposed has been designed with a hierarchical and energy-effective topology that integrates the LEACH protocol with blockchain technology to facilitate fast interaction between IoT networks. The LEACH protocol organizes IoT sensor networks into clusters. The cluster head selection is done randomly based on the amount of power that is left with the cluster head and the probability that thresholds will be met. This ensures that there is an eye kept on the power consumption of the network.

The cluster head collects information from different parts of the same area and integrates them to minimize unnecessary transmissions. Blockchain technology has been integrated into this framework to ensure that sensor nodes do not overload themselves with tasks that require power that is insufficient. Every cluster head is designed to be a blockchain node that ensures that information is valid, transactions are made, and a ledger is kept to track information. Cryptographic hash functions are used to verify that information is valid and cannot be altered.

SYSTEM ARCHITECTURE

Fig. 1 shows how the intended LEACH and blockchain-based IoT network will work as a whole.

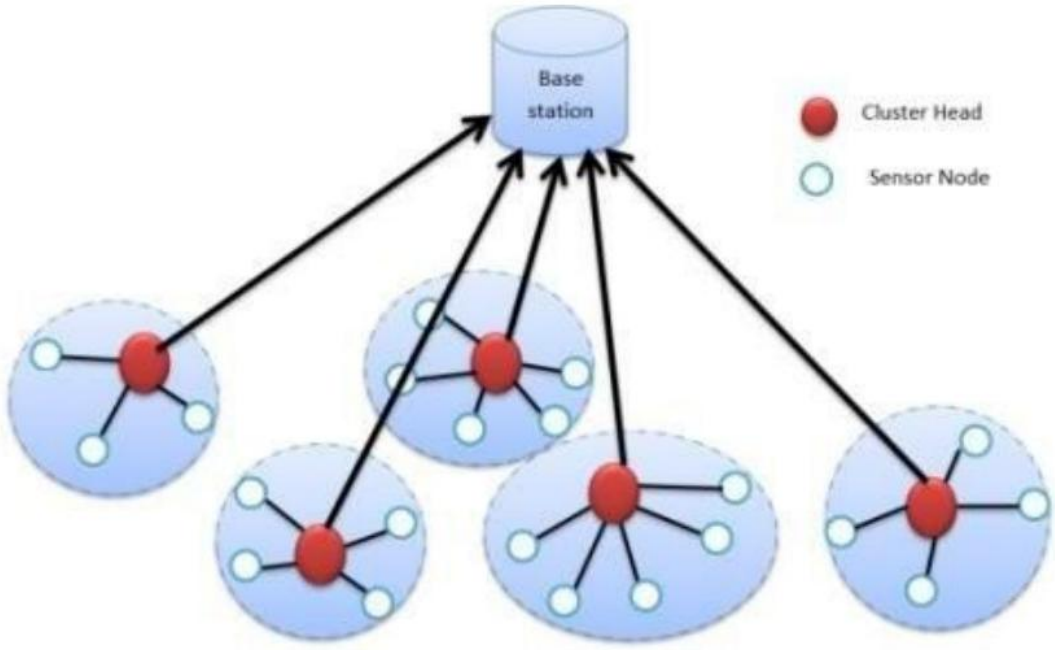


Fig. 1. **Architecture of the proposed LEACH and blockchain-based IoT network**

WORKING FLOW AND ALGORITHM

A. Working Flow

Initially, IoT sensor nodes are randomly deployed in the sensing region with equal initial energy. During the setup phase, clusters are formed using the LEACH protocol. Based on predefined probability and remaining energy, eligible nodes self-elect as Cluster Heads. Other nodes join the nearest CH to reduce communication cost.

Sensor nodes collect environmental data and transmit it to their respective CHs during the steady-state phase. CHs put the data together to get rid of duplicates and send it to the blockchain layer, where safe transactions are made and checked. The verified data blocks are subsequently sent safely to the base station or cloud server. The process is done again and over again in rounds to make sure that the load is balanced and the network lasts longer.

Here is the working flow figure of the proposed LEACH and blockchain-based IoT network

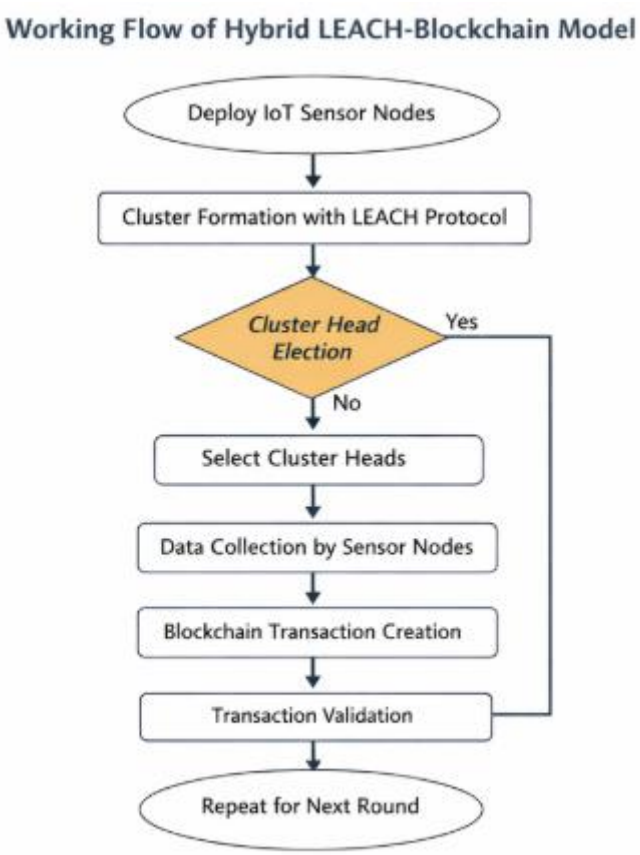


Fig 2: Working flow of the proposed LEACH and blockchain-based IoT network

B. Algorithm

1) Set unique IDs and initial energy for all IoT sensor nodes.
2) Randomly deploy nodes in the sensing area.
3) Form clusters using the LEACH protocol.
4) Select Cluster Heads based on highest residual energy.
5) Assign remaining nodes to the nearest CH.
6) Collect data from member nodes.
7) Aggregate data at CHs.
8) Convert aggregated data into blockchain transactions.
9) Validate transactions using hash verification.
10) Store validated transactions in a distributed ledger.
11) Transmit secure data to the base station.
12) Repeat the process for the next round.

This is the algorithm diagram for the proposed IoT network based on LEACH and blockchain.

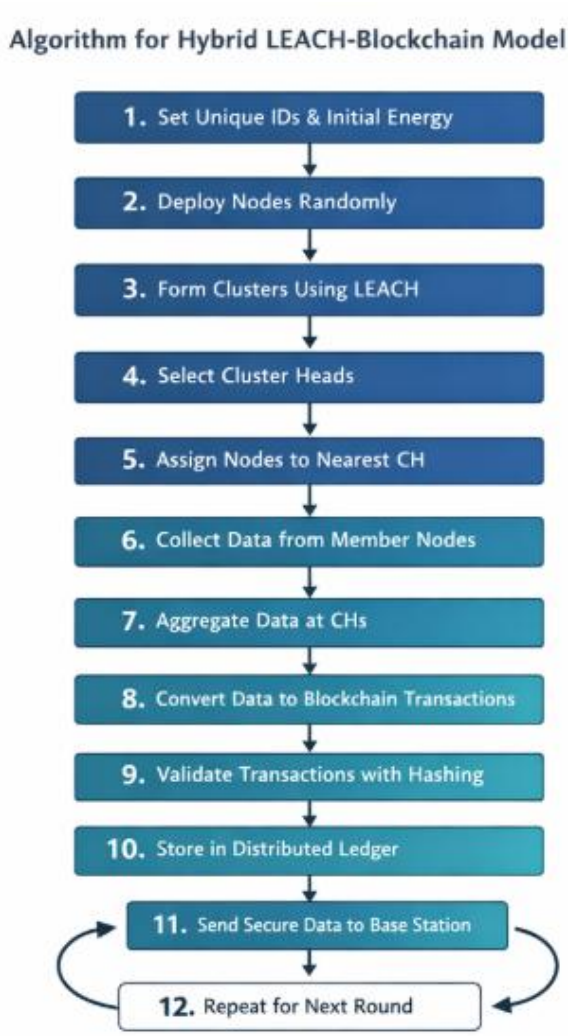


Fig 3: The algorithm for the suggested LEACH and blockchain-based IoT network

EXPERIMENTAL SETUP

We put the Hybrid LEACH–Blockchain IoT Security Model to the test in a simulation to see how it would handle real-world chaos, such clustering nodes, running a blockchain, and keeping everything working smoothly. We placed IoT sensors in random spots in a space, just like you would in the real world. No one had an unfair advantage because every sensor started with a different ID and the same quantity of energy.

LEACH was in charge of the clustering. It chose cluster heads based on the probability and whether the nodes still had enough power. The chosen cluster chiefs collected data from their group and did all the blockchain work during each cycle. That saved a lot of energy.

We simply used the cluster heads to run the blockchain. That manner, the little sensor nodes didn't have to worry about doing a lot of processing. The cluster leaders put the data into packages, locked them up with hash verification to make sure everything was honest, and saved everything in a distributed ledger. We counted the blocks as each round ended to see how long the blockchain became.

As we progressed, the simulation gave us actual statistics on the number of nodes, the number of clusters formed, the number of nodes in each cluster, the nodes selected to act as cluster heads, and the way the blockchain was expanding. We ran the simulation a number of times, modifying parameters such as the

number of clusters and the way the sensors were arranged, just to see how it would behave with a larger number of clusters and/or a more disordered network.

We were very interested in the way the nodes clustered together, the way the blockchain was tracking everything, and the way the network was behaving in terms of order and disorder, especially as we made changes to the network. The graphs helped us see the patterns, including the number of clusters, the rate, and the location of the nodes, so we could see the differences from one run to the next without getting bogged down in the details.

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Number of Nodes	100
Network Area	100 × 100 m
Initial Energy	2 J
Clustering Protocol	LEACH
Blockchain Type	Private
Simulation Rounds	1000

RESULTS AND DISCUSSION

So, we conducted some tests to see how the Hybrid LEACH-Blockchain IoT model compared to the regular LEACH model and other IoT security technologies. We were mainly interested in three things: how much energy it consumed, how long it stayed alive, and how well it was able to withstand attacks.

The results were obvious right away. This new model consumed a lot less energy. This was mainly because the cluster heads were the ones who were doing the clustering and the data aggregation. The other nodes were not burdened with the task of working with the blockchain. This meant they were conserving energy. We also made sure to choose cluster heads based on the amount of energy they had left.

This ensured that none of the nodes ran out of energy too quickly. This model was also alive for a longer time. The initial nodes and half of the nodes were alive for more rounds compared to the traditional LEACH model. This was because there was less useless information going around. We made sure to keep the costs of communication low because only the cluster heads were working with the blockchain.

This model was also secure. The information was secure because it was stored in the blockchain. This meant it was protected from being altered. This technology was very effective in detecting anyone who tried to tamper with the information. This meant it was easy to spot someone who was adding fake information or sending old information again.

There was no single point of failure here. So, in the end, it was a good compromise between safety and energy. The IoT network became not only more efficient but also much more reliable when lightweight blockchain was added to the LEACH clustering method.

Look at Figures 4 and 5. They depict what occurs when we run the Hybrid LEACH–Blockchain IoT Security Model through a few tests. You can see the clusters forming, see how the algorithm chooses cluster heads, and see how the blockchain maintains track of everything that happens along the way.

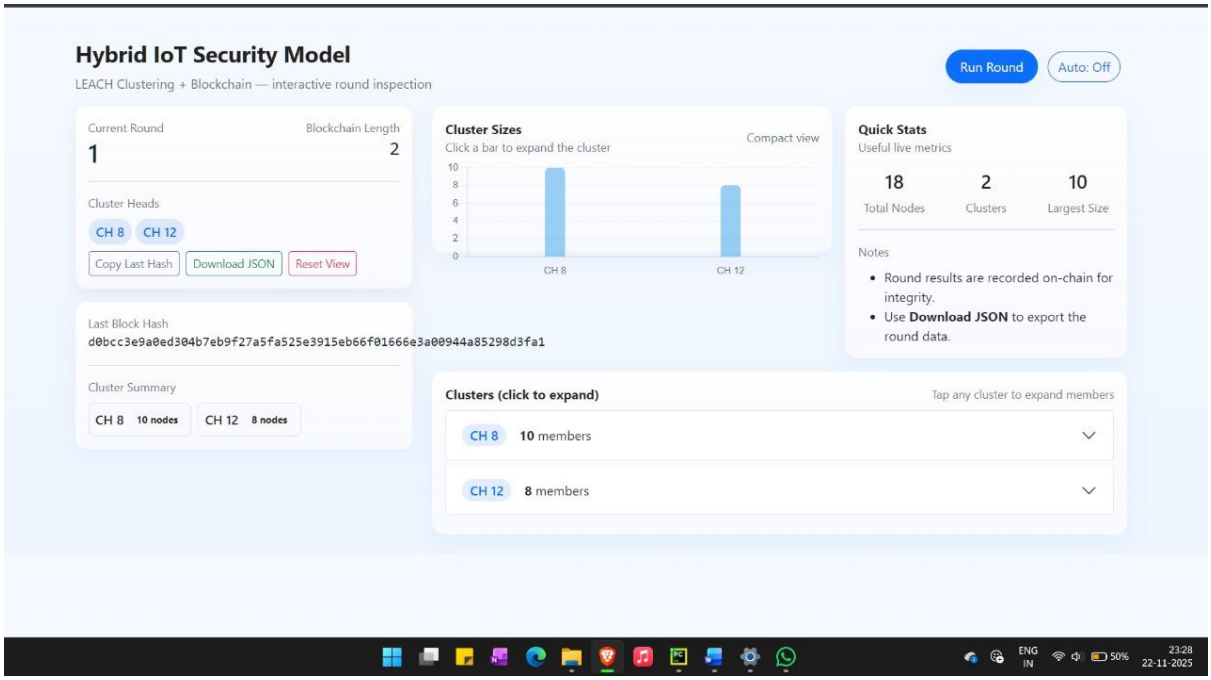


Fig 4: Hybrid LEACH–Blockchain IoT Model: Results of Blockchain Rounds and Cluster Formation with Multiple Cluster Heads

Let's begin with Figure 4. There are 16 IoT sensor nodes, which are grouped into 4 clusters. One of the clusters has 8 nodes, which is a lot, while the other three have 3, 4, or even 1 node. The cluster heads for this round are CH1, CH10, CH11, and CH16. The length of the blockchain is 2, which means the cluster heads are doing their job of checking the transactions. There are a lot of clusters, so the load is spread out rather evenly, which keeps energy use from getting too high. But you can tell that the shape of clusters changes a lot based on how near the nodes are to each other and how many of them are in one region.

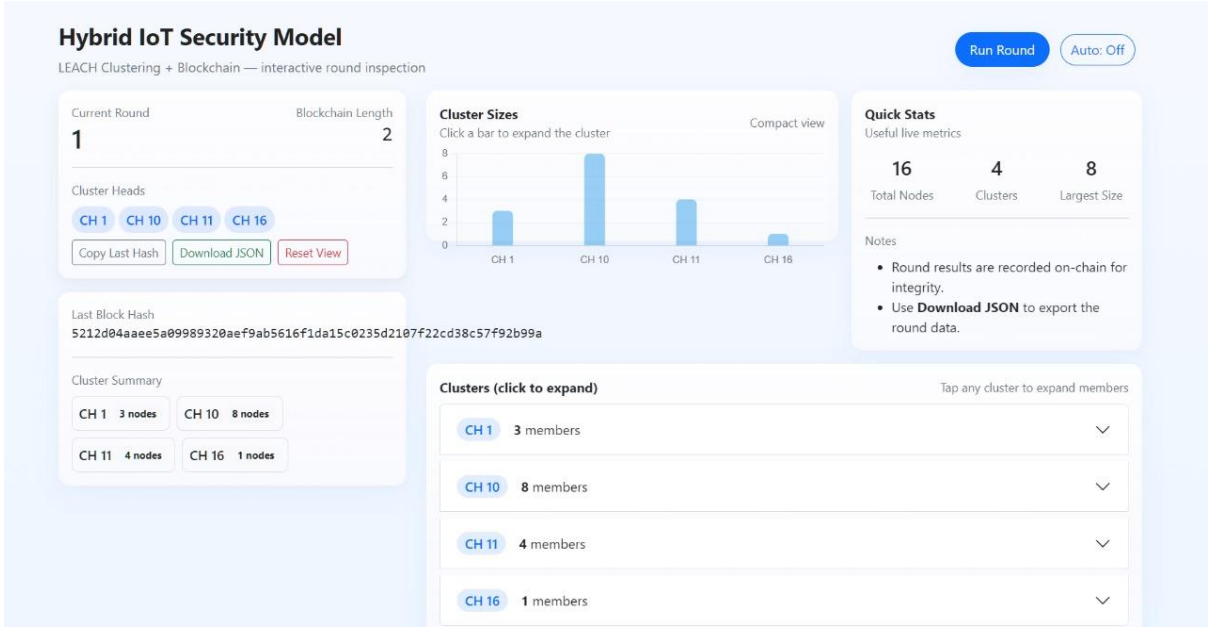


Fig 5: Hybrid LEACH–Blockchain IoT Model: Results of Cluster Formation and Blockchain Round with Two Cluster Heads

Take a look at Fig. 5 now. This time, the number of sensor nodes is 18, but they can all fit into two clusters, making the size of the clusters bigger. The number of heads of the cluster is just two, namely CH8 and CH12. They have the responsibility of managing 10 and 8 nodes respectively. The blockchain length is the same, remaining at 2.There are only two clusters now, so each cluster head needs to deal with more data than before. This makes their job harder. But the good news is that there isn't as much talking between clusters because there aren't as many of them.

So, what does all of this mean? The hybrid model is very versatile. The LEACH protocol determines how to cluster and regroup the clusters based on the position of the nodes and the remaining energy. The blockchain, on the other hand, secures the data regardless of the movement of the clusters. In both cases, you end up with a system where all the data is secure, energy is conserved, and the system moves around as desired. It doesn’t matter how you configure it; it just works.

DISCUSSION AND FUTURE WORK

This hybrid model shows how the combination of energy-efficient clustering and the decentralized blockchain technology can actually alleviate some of the difficulties faced in IoT networks. This is because only the cluster heads handle the blockchain. This is very good news. Of course, there is still some issues to deal with.

You can still have some lag in the system if it is very big, even if only the cluster heads handle the blockchain. This is especially true if there are constant transactions. Of course, the entire system is based on the selection of the right cluster heads. It gets unstable if the nodes are not evenly distributed or if some of the nodes have low energy. There is a lot you can do in the future. You can use artificial intelligence or machine learning to select the cluster heads.

This can potentially save even more energy. You can also add some nodes to the system to act as edge computing devices. This can potentially speed up the system and allow more devices to connect simultaneously. And, of course, to be honest, you can actually test the system in the real world and see how it performs.

CONCLUSION

This paper proposes a security approach that incorporates the LEACH clustering algorithm and blockchain to increase the efficiency and security of IoT devices. The clustering algorithm helps in the organization of devices, and the devices communicate in groups, reducing the number of device-to-device communications. The addition of blockchain properties to the cluster head increases the security of the network without compromising its efficiency.

From the simulation results, the proposed approach proves to be more efficient in terms of the amount of saved power, the longevity of the devices, and the security of the network compared to the conventional IoT network setup. The key to the success of the proposed approach is the confinement of the blockchain properties to the cluster head, ensuring the efficiency and security of the devices.

The proposed approach, based on the incorporation of the LEACH clustering algorithm and blockchain, seems to be appropriate for the conventional IoT network setup. However, there are plans to improve the approach to make it more efficient and capable of dealing with the more complex IoT network setup that may emerge in the future.

REFERENCES

[1] W. R. Heinzelman et al., “Energy-efficient communication protocol for wireless microsensor networks,” Proc. HICSS, 2000.

[2] I. F. Akyildiz et al., “A survey on sensor networks,” IEEE Commun. Mag., 2002.

[3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[4] M. Khan et al., “Blockchain-based security for IoT,” IEEE Access, 2021. S. Amjad, et al., “Blockchain based authentication and cluster head selection using DDR-LEACH in Internet of Sensor Things,” Sensors, vol. 22, no. 3, 2022.

[5] X. Xu, et al., “Blockchain for Internet of Things: A Survey,” IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6425-6448, 2020.

[6] Z. Nie, et al., “A lightweight blockchain consensus mechanism for IoT,” Applied Sciences, vol. 12, no. 24, 2022.

[7] H. H. A. Emira, “Blockchain-Enabled Security Framework for Enhancing IoT Networks,” The Science and Information (SAI) Conference,.

[8] M. A. Uddin, et al., “A comprehensive survey of blockchain for IoT applications,” Computer Networks, vol. 194, 2021.

[9] F. Comeau and Y. Liu, “Analysis of LEACH parameters for energy optimization in wireless sensor networks,” Procedia Computer Science, vol. 4, pp. 1172-1178, 2011.

[10] S. Amjad, et al., “Blockchain based authentication and cluster head selection using DDR-LEACH in Internet of Sensor Things,” Sensors, vol. 22, no. 3, 2022.

[11] K. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain: A distributed solution to automotive security and privacy,” IEEE Communications Magazine, vol. 55, no. 12, pp. 119-125, Dec. 2017.

[12] A. Reyna, C. Mart´ın, J. Chen, E. Soler, and M. D´ıaz, “On blockchain and its integration with IoT. Challenges and opportunities,” Future Generation Computer Systems, vol. 88, pp. 173-190, 2018.

[13] F. M. Al-Turjman, “Blockchain-based solutions for IoT security: A survey,” ICT Express, vol. 6, no. 4, pp. 221-229, Dec. 2020.

[14] S. Li, L. Da Xu, and S. Zhao, “5G internet of things: A survey,” Journal of Industrial Information Integration, vol. 10, pp. 1-9, Jun. 2018.