BHO-AODV: A Secure and Energy-Aware Multipath Routing Protocol Using Blockchain and SFLA–ABC in WSNS

Prema[1], Dr.N. Thenmozhi[2]
[1,2]*Government Arts College Coimbatore*

***Abstract*—This paper presents BHO-AODV, a new wireless sensor network (WSN) routing protocol that integrates Bio-Inspired Herding Optimization (BHO), blockchain authentication, and hybrid SFLA–ABC path search to enhance energy efficiency, routing stability, and data security. The protocol starts with the separation of nodes into energy-based clans using BHO for the efficient choice of high-energy nodes. A separating operator further optimizes node selection, improving route reliability. Modified AODV is employed for route discovery, followed by blockchain authentication to make routes unmodifiable. The authenticated routes are afterwards optimized later through Shuffled Frog Leaping Algorithm (SFLA) and Artificial Bee Colony (ABC) optimization in low energy consumption, less delay, and minimum number of hops. Data transmission happens over the most optimal and secured path. It is compared with AODV, LEACH, and Blockchain-AODV protocols' performance. Simulation results indicate that BHO-AODV consumes less energy (0.98 J) and network lifetime (1255 rounds). Furthermore, it provides improved packet delivery ratio (96.3%), end-to-end delay (124.1 ms), and throughput (92.6 kbps). The suggested protocol takes care of security, efficiency, and reliability efficiently and provides a robust solution for current WSN applications.**

***Index Terms*— Wireless Sensor Networks, Blockchain Security, Energy-Efficient Routing, Multipath Routing, Bio-Inspired Optimization, Data Integrity, Trust-Aware Routing, Network Lifetime**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) play crucial roles in healthcare, industrial automation, and smart infrastructure. WSNs are usually confronted with serious issues such as restricted energy, unstable routes, and insecure data protection owing to the restricted resources of sensor nodes and the openness of wireless transmission. Traditional routing protocols like AODV are not appropriate to handle such issues and lead to premature node failures, frequent path breaks, and susceptibility to security attacks.

To address such issues, researchers have studied blockchain-based solutions to enhance trust, security, and data integrity in WSN routing. For example, Abbas et al. (2021) proposed a blockchain-secured SDN routing solution using genetic algorithms. Abd El-moghith and Darwish (2021) proposed a blockchain model of trusted routing. Awan et al. (2022), Guerrero-Sanchez et al. (2020), and Javaid (2022) combined blockchain with encryption and trust models to achieve secure WSN communication.

Performance routing has also been enhanced with blockchain integrated with smart approaches. Lazrag et al. (2021) and Nguyen et al. (2024) suggested using blockchain routing for secure data exchange. Rajasoundaran et al. (2021) utilized machine learning to design a blockchain model for military WSNs. Rajesh et al. (2023) utilized metaheuristic optimization for secure route planning, and Tangsen et al. (2020) designed a blockchain-based node selection method. Current research by Vinya et al. (2022) and Xiao et al. (2024) employed bio-inspired and swarm intelligence techniques for routing security enhancement.

With these principles in mind, this paper proposes BHO-AODV, an energy-efficient and secure multipath routing protocol that integrates Bio-Inspired Herding Optimization (BHO) and blockchain for safe path selection. BHO separates nodes into two clans

based on energy with a splitter operator and assists in choosing high-energy stable nodes for routing and minimizing path failure. A blockchain layer ensures integrity and authenticity for routing decisions. As another layer of routing efficiency optimization, the protocol employs SFLA through ABC optimization by intertwining expansive search and targeted path optimization to choose best routes.

II. BACKGROUND STUDY

Current studies on secure routing for WSNs have concentrated on combining blockchain with intelligent optimization mechanisms to cope with energy constraint, routing volatility, and data security. Abbas et al. (2021) presented a blockchain-secured SDN routing method based on genetic algorithms to provide reliable and tamper-proof path updates in IoT environments. Likewise, Abd El-moghith and Darwish (2021) developed a deep blockchain model integrating decentralized trust verification and anomaly detection to forge secure routes. Awan et al. (2022) introduced a trust and route management system where the reputation scores of nodes are securely maintained with the help of blockchain to prevent malicious activities. Guerrero-Sanchez et al. (2020) integrated lightweight symmetric encryption with blockchain to maintain the integrity of communication at the expense of reduced resource consumption. Javaid (2022) has proposed enhancement of a dynamic trust model where behavior of nodes is observed and checked on a blockchain ledger to increase the capability to counter trust manipulation attacks.

Regarding routing efficiency, Lazrag et al. (2021) coupled cryptographic hash functions with blockchain and proposed an energy-aware and attack-resistant routing protocol. Nguyen et al. (2024) have provided a good review regarding the use of blockchain in WSN security and highlighted both the scope and potential limitation of blockchain in resource-constrained environments. Rajasoundaran et al. (2021) put forward a machine learning-based volatile blockchain that self-accompanies network attacks in WSNs used in military environments through dynamic adjustment of the ledger and anomaly detection. Rajesh et al. (2023) put forward a metaheuristic route planning strategy based on blockchain that integrated optimization precision with route integrity. Tangsen et al. (2020) illustrated a node selection algorithm in cognitive networks where trust parameters built on blockchain avoided malfunctioning or compromised nodes.

Supporting route security and reliability, Vinya et al. (2022) utilized a Jellyfish Search Optimizer with blockchain to identify secure, energy-saving routes. Similarly, Xiao et al. (2024) introduced BS-SCRM, a hybrid scheme that integrated swarm intelligence and blockchain to secure routing updates and dynamic path discovery. The above works collectively illustrate how blockchain when integrated with optimization, trust models, or machine learning distinguishingly enhances WSN routing by way of increased resilience, energy wastage savings, and routing attack protection. The above foundations have inspired the creation of BHO-AODV that integrates Bio-Inspired Herding Optimization and blockchain for secure, energy-efficient multipath routing in WSNs.

III. MATERIALS AND METHODS

The materials and methods section describe the BHO-AODV protocol that integrates Bio-Inspired Herding Optimization, blockchain, and SFLA–ABC algorithms to provide secure and energy-efficient routing for Wireless Sensor Networks. The solution begins with node classification into energy-based clans using BHO, then blockchain-based secure path authentication. Lastly, the optimal path is selected using SFLA for exploration and ABC for precision-based exploitation based on energy, delay, and hop count parameters.

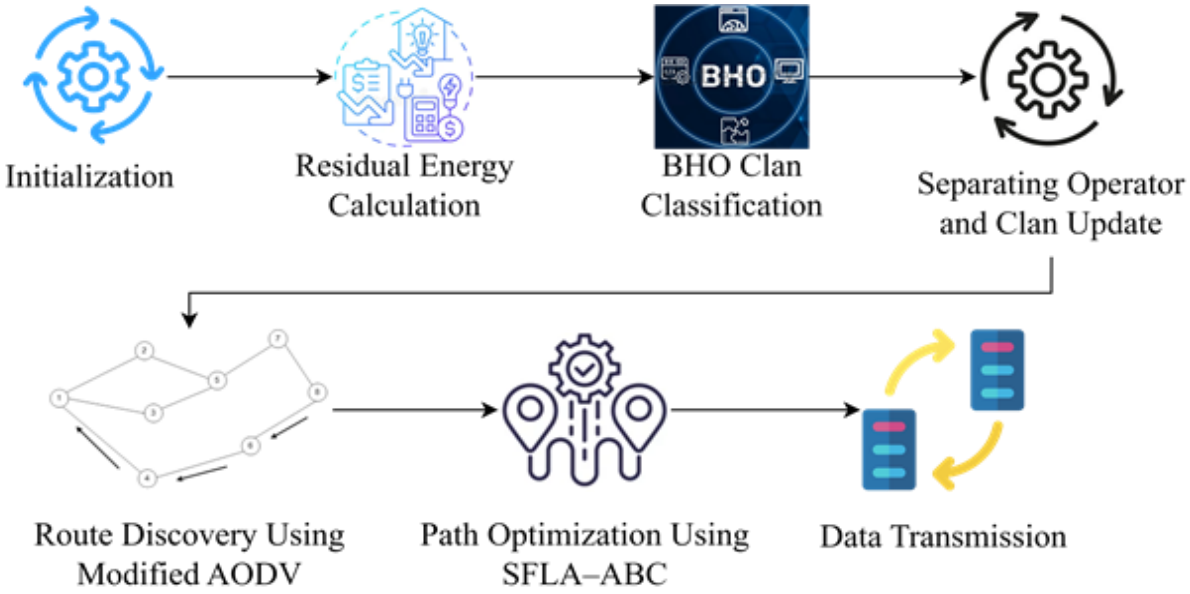

Figure 1: BHO-AODV with Blockchain and SFLA–ABC Optimization Architecture

This flowchart visually represents the BHO-AODV routing protocol enhanced with SFLA–ABC optimization for Wireless Sensor Networks. It begins with node initialization and residual energy calculation, which help identify high-energy nodes through BHO clan classification. The separating operator then updates node status and clan structure based on energy levels. A modified AODV protocol is used to discover multiple route paths, followed by SFLA–ABC optimization to select the most energy-efficient and reliable route. Finally, data transmission is carried out over the optimized path, ensuring secure and efficient communication.

3.1 BHO-AODV with Blockchain and SFLA–ABC Optimization

Phase 3 BHO-AODV strives to improve energy efficiency, load balancing, and secure routing in Wireless Sensor Networks through the integration of Bio-Inspired Herding Optimization (BHO), blockchain, and optimal choice path selection algorithms. The BHO algorithm, based on elephant herding, divides sensor nodes into two clans as a function of their energies. Nodes with more than a threshold amount of residual energy are assigned to a "fittest" clan using the separating operator, simulating the way mature male elephants split from clans in nature, thus enhancing diversity and routing reliability.

The clan update operator keeps dynamic node location within clans on the basis of energy levels after every round of transmission. Routing routes are found between high-energy nodes alone, avoiding the threat of path failure, depletion of energy, and node death. It has a lightweight blockchain system that is utilized to secure routing routes from malicious tampering and authenticate routing routes for trusted data exchange.

To further enhance routing effectiveness, SFLA (Shuffled Frog Leaping Algorithm) is used to traverse a wide range of routing routes by undergoing memetic evolution, and ABC (Artificial Bee Colony) optimization optimizes the chosen paths further by simulating foraging behavior for the purpose of achieving delay minimization and energy optimality. BHO-AODV acts synergistically to optimally control network load, achieve maximum WSN lifetime, and protect data streams against routing-based attacks.

$E_{TX} = k \times E_{elec} + k \times \varepsilon \times d^n$ ---------- (1)

Equation (1) calculates the energy required to transfer a k-bit message over distance d, with E_{elec} being the electronic energy per bit and $\varepsilon \cdot \varepsilon \times d^n$ being the amplifier energy according to the channel model. The exponent n is 2 for free space and 4 for multipath fading channels.

$E_{RX} = k \times E_{elec}$ ---------- (2)

Equation (2) is the energy utilized to obtain a k-bit message, where E_{elec} is receiver circuitry per-bit energy utilized. As opposed to transmission, receipt does not involve distance dependency.

$E_{residual} = E_{initial} - (E_{TX} + E_{RX})$ ---------- (3)

Equation (3) computes the residual energy of a sensor node upon communication, where $E_{residual}$ is the initial energy of the node and $E_{TX} + E_{RX}$ is the total energy dissipated in transmitting and receiving data. It helps to compute the remaining power of the node in the future.

$\text{New Path} = \text{Worst Path} + r \times (\text{Best Path} - \text{Worst Path})$ ---------- (4)

Equation (4) is employed in the Shuffled Frog Leaping Algorithm (SFLA) to update a worst solution (Worst Path) by moving it towards a better one (Best Path). The term $r \times (\text{Best Path} - \text{Worst Path})$ introduces a controlled random move that improves path quality without diversity loss.

$\text{Fitness} = \frac{1}{\text{Average Energy}} + \text{Delay} + \text{Hop Count}$ ---------- (5)

Equation (5) defines the fitness function for path choosing where lower is a better path. It is a combination of three parameters: the inverse of average node energy to prefer high-energy paths, cumulative delay, and hop count making the chosen path energy-efficient, faster, and shorter.

Algorithm: BHO-AODV with Blockchain and SFLA–ABC Optimization

Input: Sensor node set N, initial energy E_init, packet size k, source S, destination D

Output: Optimized, secure multipath routes from S to D

Begin

9. Initialization:

For each node n ∈ N:

Assign energy[n] ← E_init

Set status[n] ← active

Deploy nodes in sensing field

2. Residual Energy Calculation:

For each node n ∈ N:

Compute E_residual[n] ← E_init – (E_TX + E_RX)

3. BHO Clan Classification:

For each node n ∈ N:

If E_residual[n] ≥ E_threshold:

Add n to HighEnergyClan

Else:

Add n to LowEnergyClan

4. Separating Operator & Clan Update:

Apply separating operator to select fitter nodes from HighEnergyClan

Update node status and clan position after each transmission round

5. Route Discovery using Modified AODV:

Initiate RREQ from source S to D via nodes in HighEnergyClan

Collect all valid RREP responses

Store candidate paths in PathList

6. Blockchain-based Path Verification:

For each path P in PathList:

Generate hash for P

Validate P using blockchain ledger

If P is verified:

Add P to VerifiedPaths

7. Path Optimization using SFLA–ABC:

Initialize SFLA memeplex with paths from VerifiedPaths

While stopping condition not met:

Update worst path using:

P_new = P_worst + rand × (P_best – P_worst)

Evaluate fitness(P) ← 1/AvgEnergy + Delay + HopCount

Refine best paths using ABC behavior

Select path P_opt with minimum fitness

8. Data Transmission:

Transmit data packets from S to D using P_opt

Update energy levels of nodes in P_opt

Record transmission in blockchain

9. Repeat:

If network lifetime not exhausted:

Go to Step 2

Else:

Terminate protocol End BHO-AODV protocol combines Bio-Inspired Herding Optimization with AODV to categorize nodes into high- and low-energy clans to provide multipath routing with energy efficiency. Blockchain protects the routing process by authenticating each path using a decentralized ledger. SFLA and ABC algorithms are then used to traverse and optimize the most optimal and reliable routing path based on energy, delay, and hop count.

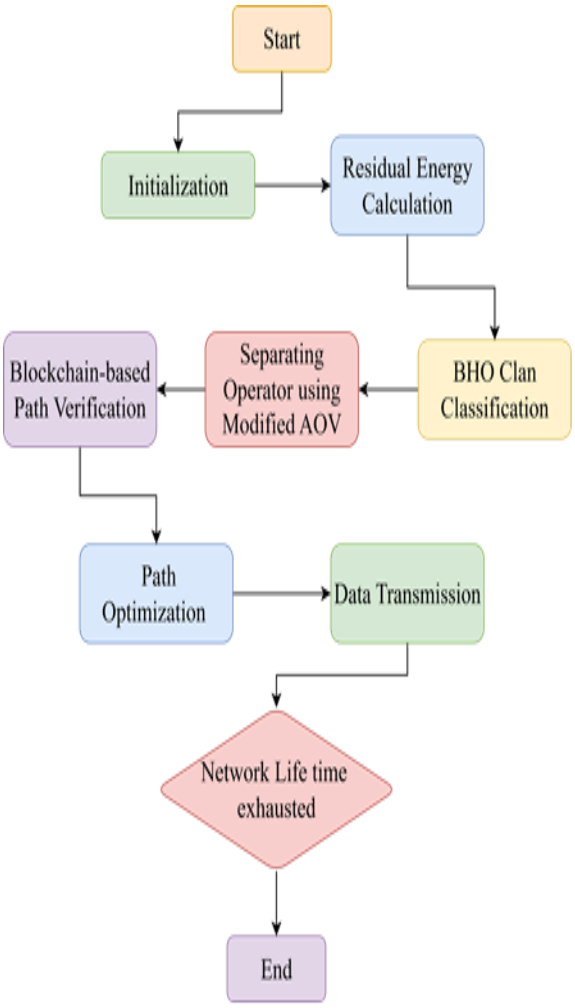

Figure 2: Flow Chart of BHO-AODV with Blockchain and SFLA–ABC Optimization

The figure 2 illustrates the working of the BHO-AODV protocol integrated with blockchain and SFLA–ABC optimization for secure and energy-efficient routing in wireless sensor networks. It begins with the initialization of nodes and residual energy calculation, followed by BHO-based clan classification. Nodes are then filtered using a separating operator based on a modified AODV mechanism. Verified paths are selected through blockchain-based validation, after which path optimization is carried out using the SFLA–ABC hybrid approach. The optimized route is used for data transmission. This cycle continues until the network's lifetime is exhausted.

IV. RESULTS AND DISCUSSION

Performance of BHO-AODV protocol is compared with current routing protocols like AODV, LEACH, and Blockchain-AODV based on key performance parameters such as energy consumption, network lifetime, packet delivery ratio (PDR), end-to-end delay, and throughput. Simulation results endorse the effectiveness of BHO-AODV in minimizing energy consumption with guaranteed secure and reliable data transfer. Comparative analysis with figures and tables confirms that the performance of BHO-AODV is superior to all the tested parameters.

Table 1: Comparison table on Performances Metrics

Metric	AODV	LEACH	Blockchain-AODV	Proposed BHO-AODV
Average Energy Consumption (J)	1.72	1.55	1.32	0.98
Network Lifetime (Rounds)	840	915	1020	1255
Packet Delivery Ratio (%)	83.5	88.2	91.7	96.3
End-to-End Delay (ms)	195.8	170.3	143.4	124.1
Throughput (kbps)	74.5	78.1	84.3	92.6

Table 1 illustrates a comparison of the most important performance parameters of AODV, LEACH, Blockchain-AODV, and the suggested BHO-AODV protocol. BHO-AODV has the minimum average energy consumption (0.98 J) and maximum network lifetime (1255 rounds), demonstrating optimal energy management. It also has the maximum packet delivery ratio (96.3%), minimum delay (124.1 ms), and optimal throughput (92.6 kbps), ensuring its supremacy regarding reliable, safe, and energy-efficient data transport in WSNs.

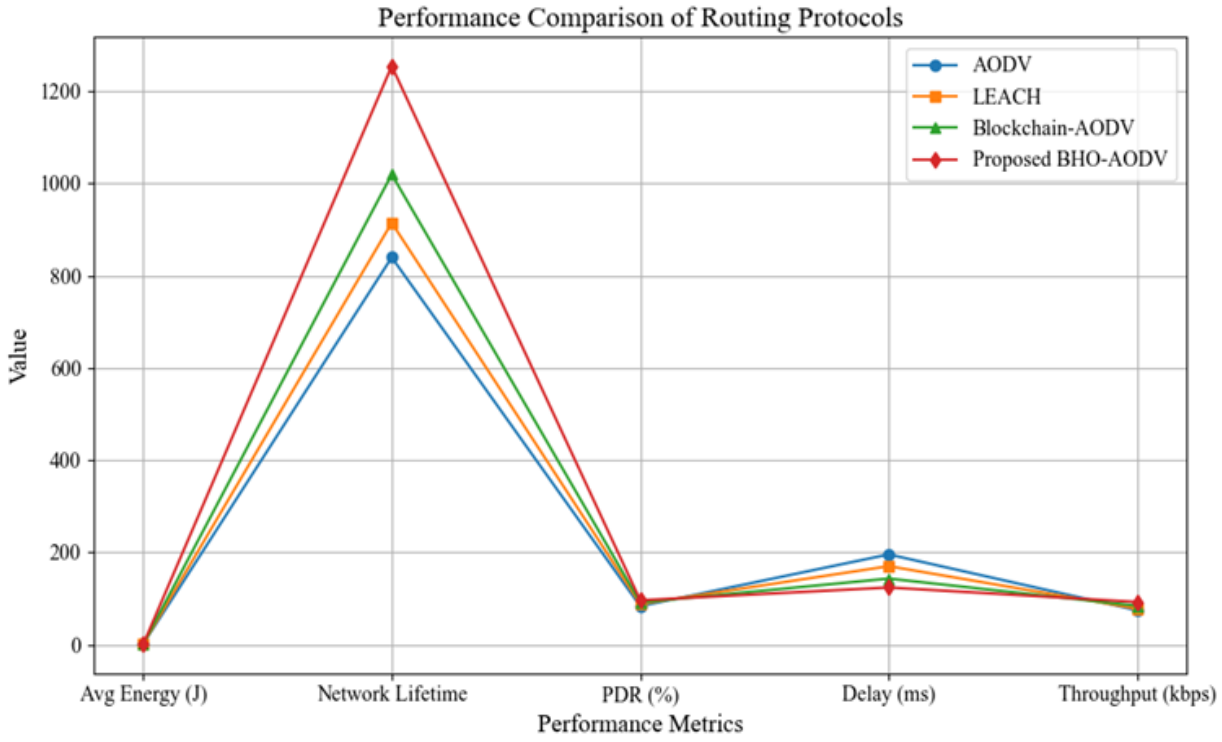

Figure 3: Comparison Chart on Performances Metrics

The figure 3 depicts that BHO-AODV always achieves maximum PDR, beginning at nearly 89% and still increasing beyond 96% to 500 rounds. AODV registers the least in PDR with steady packet loss. Blockchain-AODV and LEACH are more efficient than AODV but are still outperformed by BHO-AODV, proving its capacity for stable, energy-saving, and secure routing with increasing network time.

V. CONCLUSION

The introduced BHO-AODV protocol resolves significant issues of Wireless Sensor Networks successfully by combining Bio-Inspired Herding Optimization, blockchain, and SFLA–ABC optimization algorithm. By utilizing smart clan-based energy classification, the protocol dynamically chooses high-energy nodes, thus avoiding early node death and route stability. Application of a separating operator and path verification using blockchain-based ensures secure and tamper-proof multipath routing. SFLA-ABC hybrid algorithm enhances routing decisions once more by reducing energy consumption, delay, and hop count, which leads to enhanced performance. The simulation results confirm that BHO-AODV is significantly better than traditional AODV, LEACH, and Blockchain-AODV protocols in all the parameters. It attains minimum average consumed energy (0.98 J), maximum lifetime (1255 rounds), optimal packet delivery ratio (96.3%), minimum end-to-end delay (124.1 ms), and maximum throughput (92.6 kbps). These findings authenticate the protocol to improve the energy efficiency, reliability, and security of WSNs. Thus, BHO-AODV is a scalable and efficient solution for emerging sensor network applications with secure, high-performance, and energy-efficient routing.

REFERENCES

[1] Abbas, S., Javaid, N., Almogren, A., Gulfam, S. M., Ahmed, A., & Radwan, A. (2021). Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things. IEEE Access, 9, 139739-139754.

[2] Abd El-moghith, I. A., & Darwish, S. M. (2021). Towards designing a trusted routing scheme in wireless sensor networks: A new deep blockchain approach. IEEE Access, 9, 103822-103834.

[3] Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J. G. (2022). Blockchain based secure routing and trust management in wireless sensor networks. Sensors, 22(2), 411.

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

[5] Javaid, N. (2022). A secure and efficient trust model for wireless sensor IoTs using blockchain. IEEE Access, 10, 4568-4579.

[6] Lazrag, H., Chehri, A., Saadane, R., & Rahmani, M. D. (2021). Efficient and secure routing protocol based on Blockchain approach for wireless sensor networks. Concurrency and Computation: Practice and Experience, 33(22), e6144.

[7] Nguyen, M. D., Nguyen, M. T., Vu, T. C., Ta, T. M., & Tran, Q. A. (2024). A Comprehensive Study on Applications of Blockchain in Wireless Sensor Networks for Security Purposes. Journal of Computing Theories and Applications, 2(1), 102-117.

[8] Rajasoundaran, S., Kumar, S. S., Selvi, M., Ganapathy, S., Rakesh, R., & Kannan, A. (2021). Machine learning based volatile block chain construction for secure routing in decentralized military sensor networks. Wireless Networks, 27(7), 4513-4534.

[9] Rajesh, M. V., Acharya, T. A., Hajiyev, H., Lydia, E. L., Alshahrani, H. M., Nour, M. K., . & Al Duhayyim, M. (2023). Blockchain Driven Metaheuristic Route Planning in Secure Wireless Sensor Networks. Computers, Materials and Continua, 74(1), 933-949.

[10] Tangsen, H., Li, X., & Ying, X. (2020). A blockchain-based node selection algorithm in cognitive wireless networks. IEEE Access, 8, 207156-207166.

[11] Vinya, V. L., Anuradha, Y., Karimi, H. R., Divakarachari, P. B., & Sunkari, V. (2022). A novel blockchain approach for improving the security and reliability of wireless sensor networks using jellyfish search optimizer. Electronics, 11(21), 3449.

[12] Xiao, J., Li, C., Li, Z., & Zhou, J. (2024). Bs-scrm: a novel approach to secure wireless sensor networks via blockchain and swarm intelligence techniques. Scientific Reports, 14(1), 9709.