SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I7P117

Volume 12 Issue 7, 220-230, July 2025

Original Article

Social Spider Enhanced Multi-Layered ANN Routing Scheme for Wireless Sensor Networks Utilizing Internet of Things and Blockchain Technology

Jinsha Lawrence[1], Shaji K. A. Theodore[2], Dinesh Kumar Budagam[3], B. Rajalakshmi[4], K. Manojkumar[5], Srikanth Mylapalli[6]

[1]*Department of Computer Science and Engineering, Karpagam Academy of Higher Education, Coimbatore, India.*
[2]*Faculty of IT (Networking), College of Computing and Information Science, University of Technology and Applied Sciences, Sultanate of Oman.*
[3]*Sr cybersecurity engineer at VISA, Inc., Foster City, CA, United States.*
[4]*Department of Computer Science and Engineering, New Horizon College of Engineering, Bengaluru, India.*
[5]*Department of Computer Science and Engineering, Government College of Engineering, Sengipatti, Thanjavur, Tamil Nadu, India.*
[6]*Department of Computer Science and Engineering, Tirumala Engineering College, Jonnalagadda, Narasaraopet, Andhra Pradesh, India.*

[1]*Corresponding Author : jinshalarence@gmail.com*

Received: 09 May 2025 Revised: 10 June 2025 Accepted: 11 July 2025 Published: 31 July 2025

Abstract *- Wireless Sensor Network (WSN) is prone to various attacks during data transmission and also faces difficulties including reduced energy efficiency, minimized security and less network lifetime. For this reason, appropriate security measures and routing approaches need to be implemented. Henceforth, this paper presents a secure and energy-efficient routing scheme for WSN to address these difficulties. The proposed work consists of a Social Spider enhanced Multi-layered Artificial Neural Network (ANN) based routing scheme for attaining improved WSN management with reduced complexity. The deployment of an SSO-multi-layered ANN routing scheme acquires adaptive and dynamic routing with energy efficiency and increased robustness. Moreover, conventional IoT platforms struggle with various limitations, including cyberattacks; thus, to enhance data access with improved data privacy and security, IoT is integrated with Blockchain technology to ensure data integrity and protection. In spite of this, achieving a dependable routing scheme is crucial for assuring the security and efficiency of WSN. As a result, the proposed SSO-multi-layered ANN routing scheme is combined with IoT and Blockchain technology, enhancing WSN efficacy and Reliability. The proposed system is validated using NS-2. The results show reduced packet loss and energy consumption with increased PDR, network lifetime and throughput, indicating highly secure and protected WSN performance.*

Keywords *- Wireless Sensor Network (WSN), SSO-multi-layered ANN routing, IoT and Blockchain technology.*

1. Introduction

At present, WSN is utilized for real-time applications, depicts various advantages such as size, cost efficiency and easy implementation, thereby making WSN a promising technology [1]. WSNs are an ensemble of smart sensor nodes, which gather data and take relevant decisions [2]. It also loads data into cloud applications, which are further accessed by end users for processing [3]. WSN is generally applicable to various aspects, including forest fire tracking, real-time monitoring of natural hazards, and environmental tracking [4]. Significantly, IoT is a rapidly developing communication technology that is widely employed in a variety of methods [5]. Thus, a large amount of sensing networks, such as WSN, utilizes IoT for monitoring [6]. Consequently, in recent times, WSN plays a crucial part in communication due to its easy connection and mobility [7]. Despite this, WSN faces various limitations including reduced energy sources, computational complexity, memory and minimized communication bandwidth, which leads to decreased WSN efficiency and performance [8]. However, designing different algorithms for a particular purpose is quite difficult [9]. The developed WSN design in specific must prioritize several problems like data aggregation, clustering, routing, fault detection and tracking, various challenges associated with WSN is depicted in Figure 1.

Amidst, all these stated limitations, routing is regarded as the most vital task, as majority of the energy consumption occurs during routing data from sender node to the receiver node [10].

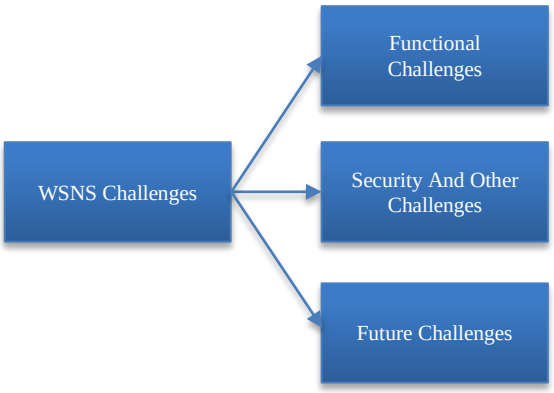


Fig. 1 WSN's challenges

Thus, Machine Learning (ML) based routing algorithms are widely considered, which are capable of improving the network reliability by handling a dynamic routing mechanism [11]. Thus, conventional ML-based routing models are analyzed for determining the optimum routing model, Deep Belief Network (DBN) deployed in [12] for attaining an efficient routing protocol that enables improved information transmission via a selected path with enhanced Packet Delivery Ratio (PDR). However, DBN struggles with certain difficulties like training time, hyperparameter tuning, overfitting, data sensitivity, and the inability to handle varying circumstances. Similarly, in [13], the authors developed a WSN system using energy-efficient routing using Fuzzy Neural Network (FNN) to reduce energy consumption during the routing process. FNN is capable of handling dynamic network environments such as varying network conditions or uncertainty. In spite of this, FNN is computationally expensive with scalability issues and reduced decision-making ability. Thus, the authors in [14] introduce the Gradient Boosted Decision Tree Algorithm (GBDT) for achieving an effective routing process. The implementation of GBDT enables increased flexibility and adaptability towards handling complex data relationships.

Nevertheless, GBDT highly depends on the data quality and quantity for effective routing. Henceforth, this paper proposes a routing scheme that attains increased robustness towards dynamic network conditions, enhanced energy-efficient routing with improved adaptability in handling complex data relationships. Furthermore, tuning a base model is considered essential for acquiring better routing. The various conventional routing optimization algorithms are evaluated in Table 1.

Table 1. Conventional optimization algorithm

Optimization Algorithm	Advantages	Disadvantages
[15] Multi-Objective Improved Seagull Algorithm (MOISA)	• Effective Exploration • Flexibility • Adaptability • Improved Global Search	• High Computational Expenses • Increased Convergence Time • Increased Sensitivity
[16] Termite Hill Algorithm (THA)	• Adaptable to varying network conditions • Improved Energy Efficiency • Scalability	• Computational Overhead • Slow convergence time • Increased parameter sensitivity • incapable of handling larger networks
[12] Mantaray Foraging Optimization (MRFO) Algorithm	• Scalability • Robustness • Simple and Easy Implementation	• Computational Complexity • Sensitivity • Possibilities of being stuck in local optima

To overcome the above disadvantages, this paper integrates a Social Spider enhanced Multi-layered ANN routing scheme. In addition to this, regardless of these advantages, WSN still comprises various security issues, attacks and intruders. For this reason, security measures need to be implemented to ensure data security and privacy. Thus, Blockchain technology is introduced in WSN [17]. The initiation of Blockchain in WSN ensures an enhanced authentication process, thereby paving the way for a secure routing process. Therefore, the overall system utilizing SSO-multi-layered ANN routing with IoT and Blockchain technology achieves enhanced WSN performance with increased Reliability and efficiency. Overall outline of proposed work is depicted as follows,

- To achieve an enhanced and energy-efficient routing process, an SSO-multi-layered ANN routing scheme is utilized in WSN, ensuring optimized routing with increased Reliability and optimum decision-making capabilities.
- To ensure improved data security and protection, Blockchain technology is deployed, which enables effective and secure data transmission with increased data privacy and integrity.
- The integration of both SSO-multi-layered ANN routing scheme and Blockchain technology acquires overall enhanced network performance in terms of security, scalability and Reliability.

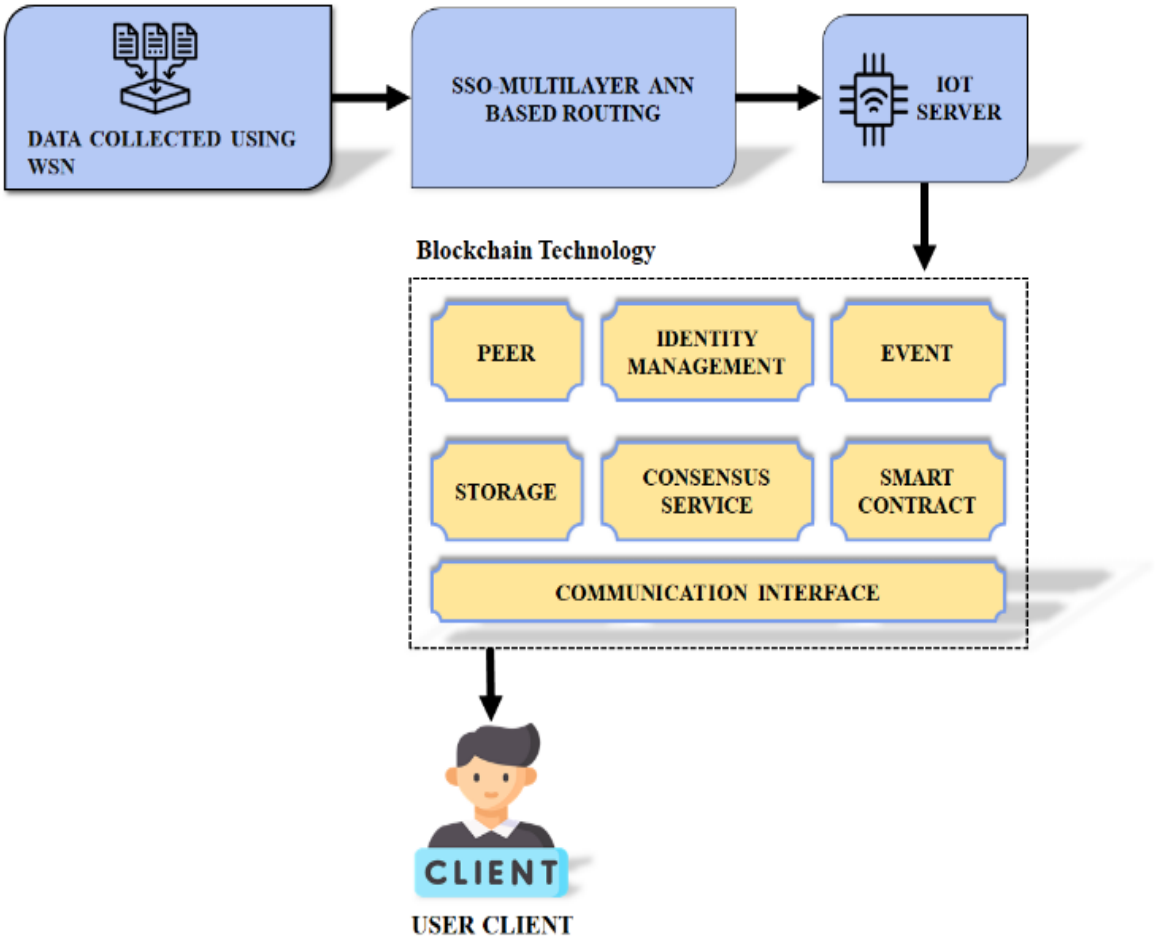


Fig. 2 Proposed system block diagram

2. Proposed Modelling

Figure 2 showcases the proposed system block diagram, consisting of an SSO-multi-layered ANN routing scheme with IoT and Blockchain technology for WSN. At first, data is collected through WSN, which is later fed to the SSO-multi-layered ANN routing scheme to achieve the optimum routing path, thus reducing energy consumption and providing effective communication. The utilization of a routing algorithm attains efficient and enhanced data handling, before proceeding it to the IoT server.

The data in the IoT cloud server is then passed to Blockchain technology for acquiring secured and protected data transactions, comprising various components including PEER, identity management, Event, storage, consensus service and smart contract. The PEER component manages network interactions for secure data transmission, identity management deals with authentication and authorization processes, and Event tracks. It monitors the network process, storage enables secure and reliable data storage, and the consensus service assures settlement between all the distributed nodes. Finally, a smart contract enacts pre-defined conditions for an improved transmission process. Furthermore, all these components are connected using the communication interface, which enables smooth transmission of data. Conclusively, the final processed data is made accessible to the user client. Thus, the whole structure of the proposed system ensures secure, reliable and protected data transmission within the WSN system.

2.1. Modelling of SSO-Multi-Layered ANN Routing Scheme

Figure 3 represents the ANN architecture with multiple hidden layers, which deals with forward and backwards propagation of the ANN. The initial layer is known as the input layer, which gathers the incoming information for routing in the WSN. ANN atleast consists of one hidden layer; here, ANN is deployed with two hidden layers comprising various neurons. Significantly, the Final layer is known as the output layer. In Figure 1, summation $\vec{y}^{(k)}$ and activation $\overrightarrow{\hat{y}^{(k)}}$ Parts of all the neurons are separated within the hidden layers. The data transmits from one layer to another until it reaches the output layer.

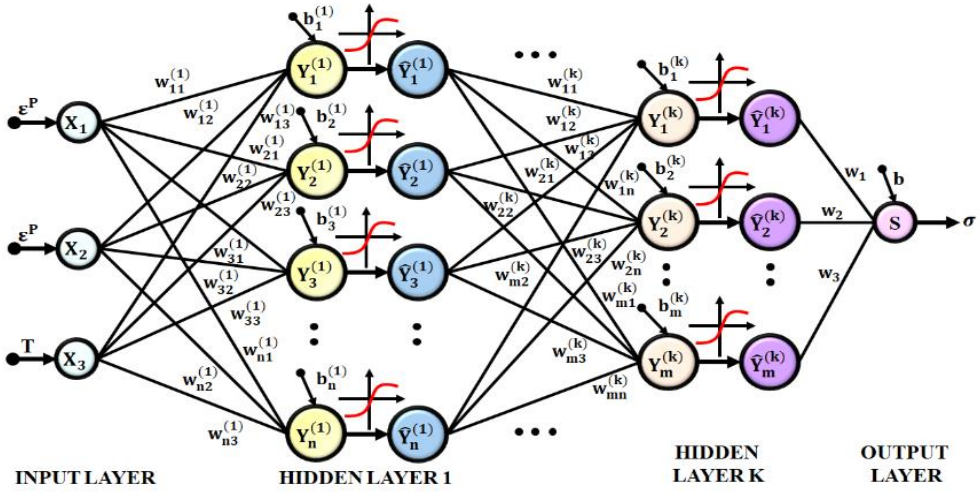


Fig. 3 Multi-layered ANN architecture

2.1.1. Input Layer

The input layer is expressed as $\vec{x} = [x_1, x_2, x_3]^T$, where $\vec{x}$ Consists of three components that depict the attributes of the routing problems.

2.1.2. Hidden Layer

Each input node is connected to the node in the next layer for a fully connected neural network. Hidden layer k, consisting of n neurons, occupies the weights of the output $\vec{x}$ Sum from the previous layer $(k-1)$ comprising m neurons, which is expressed as,

$$y_i^{(k)} = \sum_{j=1}^{m} w_{ij}^{(k)} x_j + b_i^{(k)} \quad (1)$$

Where, $y_i^{(k)}$ refers to the value of i^{th} neuron of k layer, $w_{ij}^{(k)}$ indicates the weight attained between i^{th} neuron of k layer and j^{th} neuron of $(k-1)$ layer and $b_i^{(k)}$ implies the bias of i^{th} neuron of k layer respectively. The obtained weights and biases are the training parameters of the ANN. The matrix representation of (1) is rewritten as,

$$\vec{y}^{(k)} = w^{(k)}.\vec{x} + \vec{b}^{(k)} \quad (2)$$

Where, $\vec{y}^{(k)} = [\, y_1^{(k)}, y_2^{(k)}, \ldots\ldots, y_n^{(k)}\,]^T$ Which depicts the node values obtained from the summation operation in k layer, whereas, $\vec{b}^{(k)}$ indicates the node value of bias in k layer and $w^{(k)}$ Denotes weight parameters $[n \times m]$ of k layer, which is further given as,

$$w^{(k)} = \begin{bmatrix} w_{11}^{(k)} & w_{12}^{(k)} & \cdots & w_{1m}^{(k)} \\ w_{21}^{(k)} & w_{22}^{(k)} & \cdots & w_{2m}^{(k)} \\ \vdots & \vdots & \ddots & \vdots \\ w_{n1}^{(k)} & w_{n2}^{(k)} & \cdots & w_{nm}^{(k)} \end{bmatrix} \quad (3)$$

Where the sum of the weight parameters and bias parameters of k layer is the total number of training parameters N for any hidden layer k, that is, $N = n(m+1)$. The output value $\vec{y}^{(k)}$ Is provided via neurons in the hidden layer after the summation operation, which is given as,

$$\overrightarrow{\hat{y}}^{(k)} = f^{(k)}\left(\vec{y}^{(k)}\right) \text{ or } \hat{y}_i^{(k)} = f^{(k)}\,(y_i^{(k)} \quad (4)$$

2.1.3. Output Layer

The output layer consists of the output values attained from the hidden layers, which are given as,

$$s = \sum_{j=1}^{m} w_j\, \hat{y}_j^{(l)} + b \quad (5)$$

Where b refers to the bias of the output neuron, w_j Represents the weight parameter between the previous hidden layer and the output neuron s. To further tune the ANN parameter, optimization algorithm plays an essential part; thus, the SSO algorithm is integrated with a multi-layered ANN architecture.

2.2. ANN Optimization using SSO Algorithm

Based on the behavioural aspects, spiders are classified into two types, namely, solitary spiders and social spiders. Social spiders prefer zero contact or reduced contact with other spiders and live in their own spider web. These spiders live in a collective web. This algorithm is developed based on the social spider behavioural traits. Both male and female social spiders live together in a collective web, where the number of female spiders is higher by 70% than that of the male spiders. Hence, dominant male spiders mate with female spiders located at a specific space range, illustrated in Figure 4. Meanwhile, the non-dominant males persist fixed in their current point near new male spiders of the web. Besides mating, these spiders communicate via vibrations; the intensity of the vibrations depends on two parameters, that is, the weight of the spider and the distance between them.

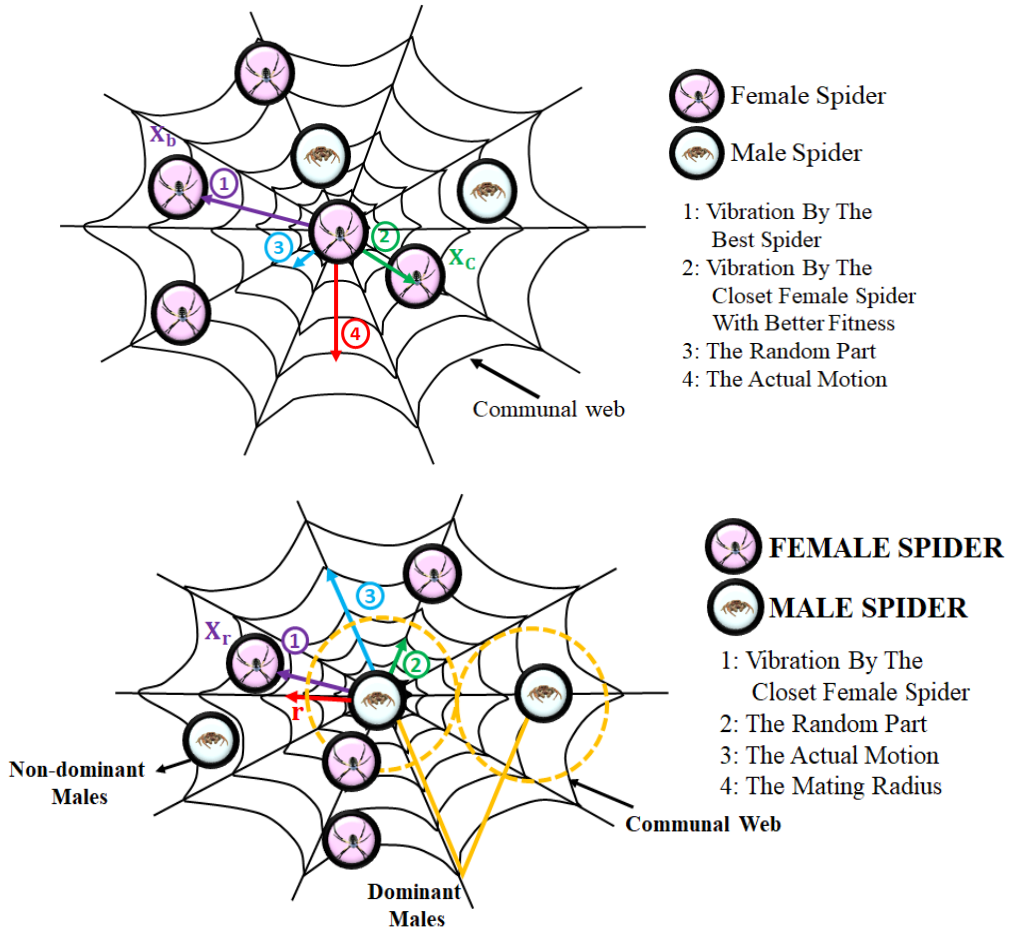


Fig. 4 Social spider optimization structure

SSO functions based on the characteristics of social spiders. Search agents comprise both spiders, which are expressed as,

$$N_f = \lfloor (0.9 - rand * 0.25) * N \rfloor \quad (6)$$

$$N_m = N - N_f \quad (7)$$

Where N, N_f and N_m Refers to the total population of the spiders, including males and females within their web. The weight of each spider is i and w_i calculated using,

$$w_i = \frac{fitness_i - worst}{best - worst} \quad 0 \leq i \leq N \quad (8)$$

Where, $fitness_i best$ and $worst$ indicate the objective functions, respectively, and the vibrations used for interaction by the spiders in the communal web are evaluated as,

$$V_{i,j} = w_j * e^{-d_{i,j}^2} \quad (9)$$

Where, w_j implies the weight of the spider and $d_{i,j}$ Refers to the Euclidean distance between them. Figure 5 depicts the flowchart of the SSO algorithm.

Algorithm:1 SSO algorithm

Input: N- total number of spiders, N_f- Number of females, N_m – Number of male spiders.
First point of both spiders
N_{iter} – Number of iterations
Output: Ideal point of social spiders and their fitness value.
Process: While $i <= N_{iter}$ do
Evaluate the radius of male and female spiders
Evaluate the weight of spiders
Calculate the motion of both spiders on the basis of their cooperative operations.
Perform mating among the prevailing males and females
Update the solutions when spider offspring are weightier
End

However, data transmission over WSN is prone to cyber threats; hence, to enable secure and protected data transmission, Blockchain technology is integrated within the system to achieve highly protected data transmission.

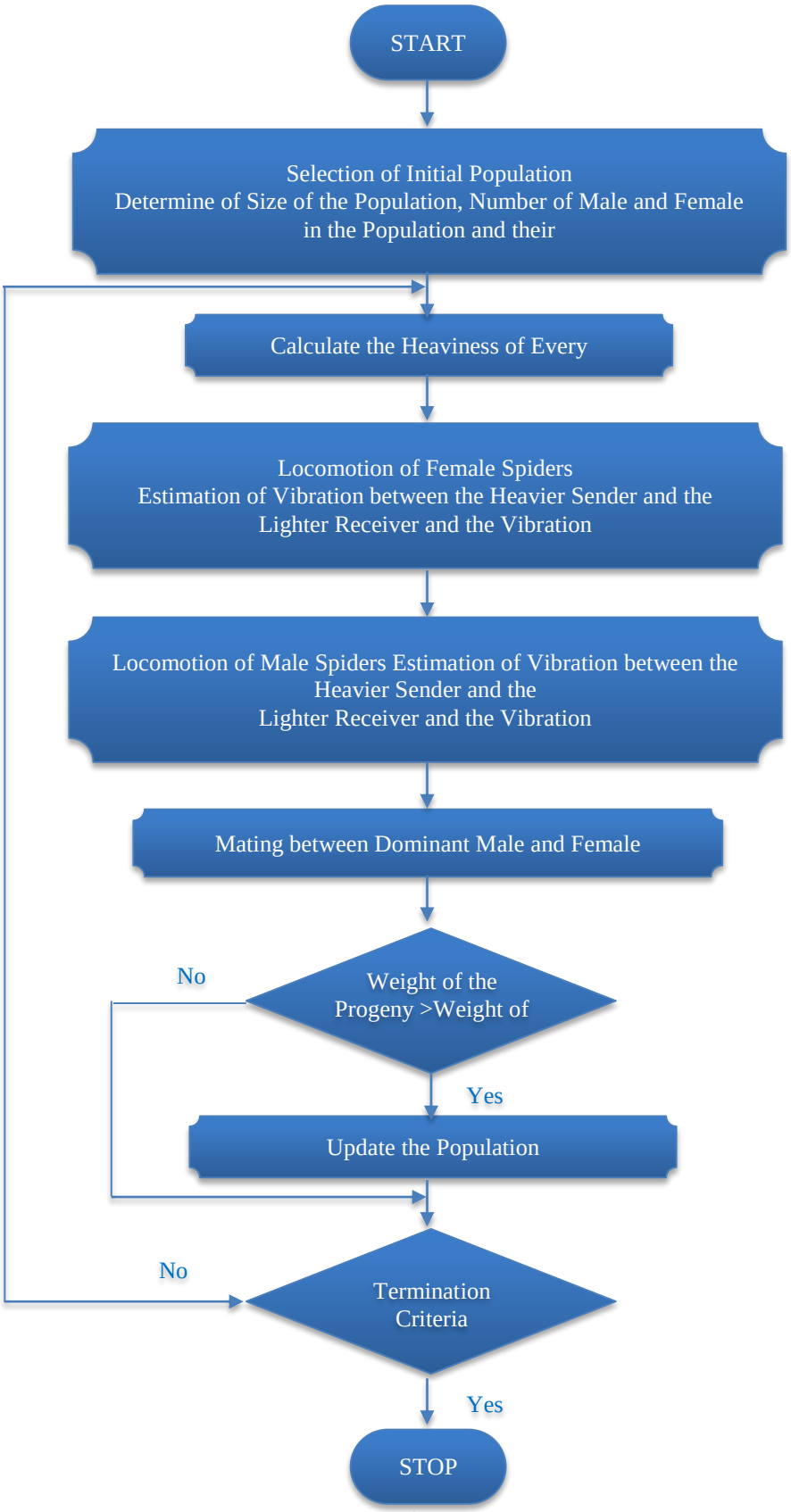


Fig. 5 Flowchart of SSO algorithm

2.3. Modelling of Blockchain Technology

Blockchain is a distributed form of data storage technology, as depicted in Figure 6, in which data is fed to special constructions termed blocks. Every block comprises two parts, namely, head and body, in which the head part consists of block number, timestamp, hash value of prior block and its own hash value. Whereas the body part contains data and the block number denotes the number of blocks, the nonce value represents "Number Only Used Once". Nonce is generally utilized for authentication and cryptographic hash functions, which refers to a pseudo-random number and finally, timestamp refers to the block creation time.

Moreover, every block comprises its individual hash value and the prior block, carrying information about the previous block. Each and every block is connected via chain components, hence the name Blockchain; thus, once the data is stored in Blockchain, it is quite difficult to erase it. Blockchain technology functions based on a mining process using hash algorithms. A hash algorithm receives input of any size and delivers output of the same size. The obtained output is known as "hash" and consists of 64 characteristics. It is a one-way function, making it unfeasible to determine the input from the output.

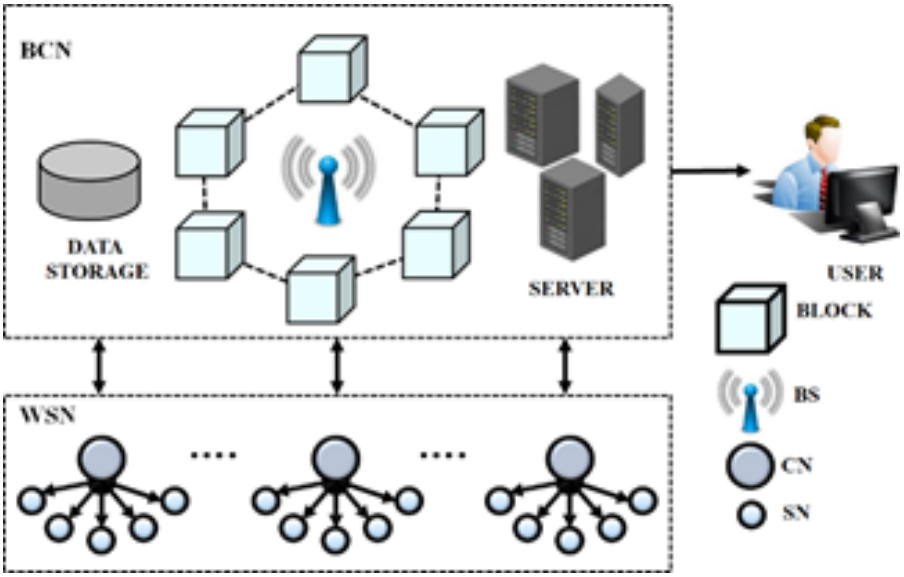


Fig. 6 Blockchain architecture

Algorithm 2: Blockchain Technology

Input: Peer nodes P_i and IoT nodes M_j In a blockchain network, N" are chosen as minor nodes based on their validity.
Output: IoT devices are trusted or malicious
Main ()
{

1. IoT node records are saved in both Blockchain and traditional databases, allowing users and managers to track and monitor their activities.
2. If (IoT device authorized on Blockchain)
   Then
   The device is enabled to deliver service to users
3. A record of every action of all devices is collected in the Blockchain network based on various trust factors.
4. If (IoT device rating $>$ 7)
   Then
   The device is kept in extreme alert, and significantly, its record is checked.
   Else
   Block IoT device from Blockchain

Various components of Blockchain are Peer, Identity management, Event, Storage, Consensus Service, Smart Contract and communication interface.

a) Peer-to-Peer: This technology is a vital component of Blockchain architecture, which allows users to communicate with each other and enables transactions without the need for intermediaries. Peer-to-Peer comprises interconnected nodes that allow interaction with each other, enabling the storage and recording of transactions.

b) Identity Management: This technology ensures that only the authorized user has access to the data, information or resources, thus allowing access to only authorized users, thereby achieving a highly trusted and secure system.

c) Event: This component enables tracking and monitoring of the changes that occur within the smart contract.

d) Storage: Blockchain storage enables reliable and secure data storage, where the data is encrypted with a private key, making it impossible for unauthorized users to access.

e) Consensus Service: The consensus service is a technology that validates the transactions between users and makes them authentic.
f) Smart Contract: Programs that execute automatically when two users agree to the terms and conditions.
g) Communication Interface: This mechanism allows nodes to communicate with each other while maintaining the data integrity of the network. The communication interface is regarded as the crucial component, as it enables nodes to interact without the requirement of a central authority.

Henceforth, the overall proposed system ensures enhanced data transmission with an optimum routing strategy and secured protection against cyber threats.

3. Results and Discussion

The proposed model has been evaluated by NS2 software to establish the effectiveness and efficiency of the proposed approach, and their comparative analysis is also elaborated in this section.

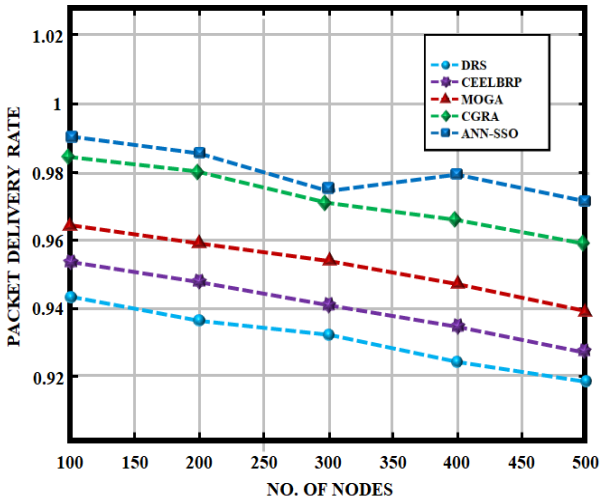


Fig. 7 PDR

Figure 7 represents the PDR graph attained by various routing algorithm such as DRS [18], CEELBRP [19], MOGA [20] and CGRA [21] from which it is visible that proposed ANN_SSO based routing algorithm attained highest PDR of 0.99, while [18-20, 21] depicts slightly reduced PDR value, indicating efficient delivery of packets to the receiver with reduced losses, thus attaining increased network stability.

Figure 8 indicates throughput performance depicted by different routing algorithms, achieving the highest enhances the overall system efficiency, enabling a large quantity of data to be communicated over a network effectively. It is evident from the above chart that ANN-SSO attained the highest throughput value compared to the other conventional routing algorithms, referring to improved data transmission with enhanced utilization of available resources.

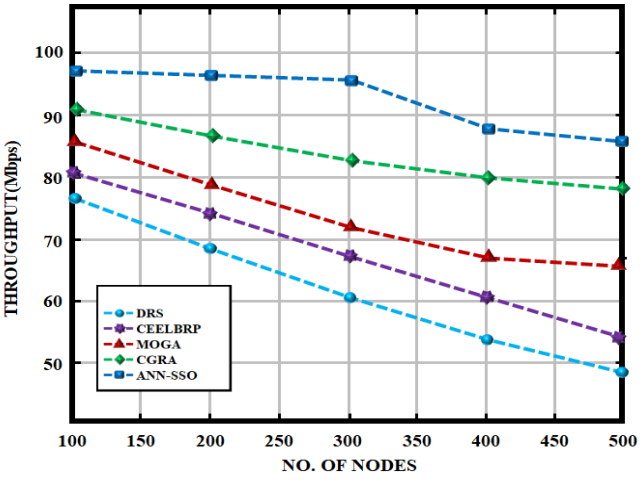


Fig. 8 Throughput

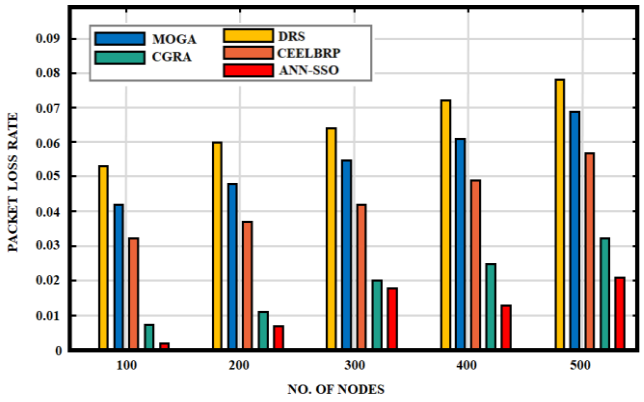


Fig. 9 Packet loss rate

A comparison of packet loss rate is showcased in Figure 9; reduced packet loss rate refers to increased system reliability, as a minimal number of packets are lost during packet transmission. Reduced packet loss generally means the system's ability to adapt to various network conditions, indicating optimum path selection by the routing algorithm. The reduced packet loss rate attained by the proposed routing algorithm showcases its efficient performance, ensuring reliable packet delivery.

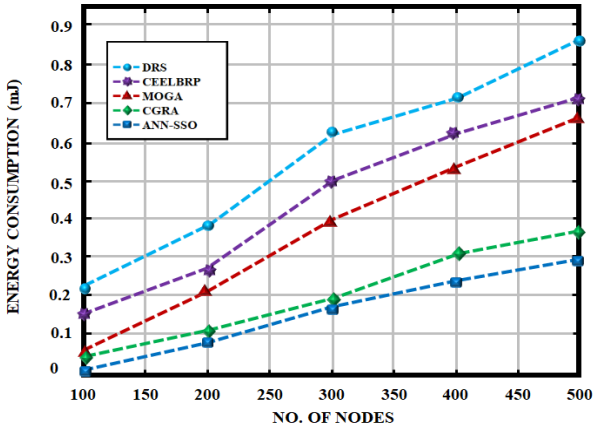


Fig. 10 Energy consumption

Figure 10 showcases the energy consumption characterized by ANN-SSO and other conventional algorithms. ANN-SSO achieves efficient utilization of energy resources, which is evident from the energy consumption rate acquired. Minimized energy consumption indicates optimum management of energy resources without compromising the network's functioning ability. When compared to other conventional algorithms, which attained slightly higher energy consumption rates, ANN-SSO shows improved performance with reduced energy consumption.

The network lifetime performed by ANN-SSO is analized and compared with other conventional algorithms in Figure 11. The above chart demonstrates that ANN-SSO attained increased network lifetime when compared without compromising the network stability. Meanwhile, other routing algorithms obtained slightly reduced network lifetime, referring to ANN-SSO performance efficiency, which is comparatively higher.

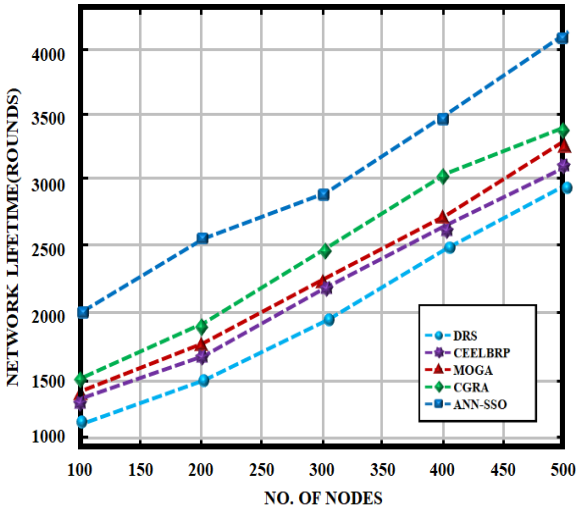
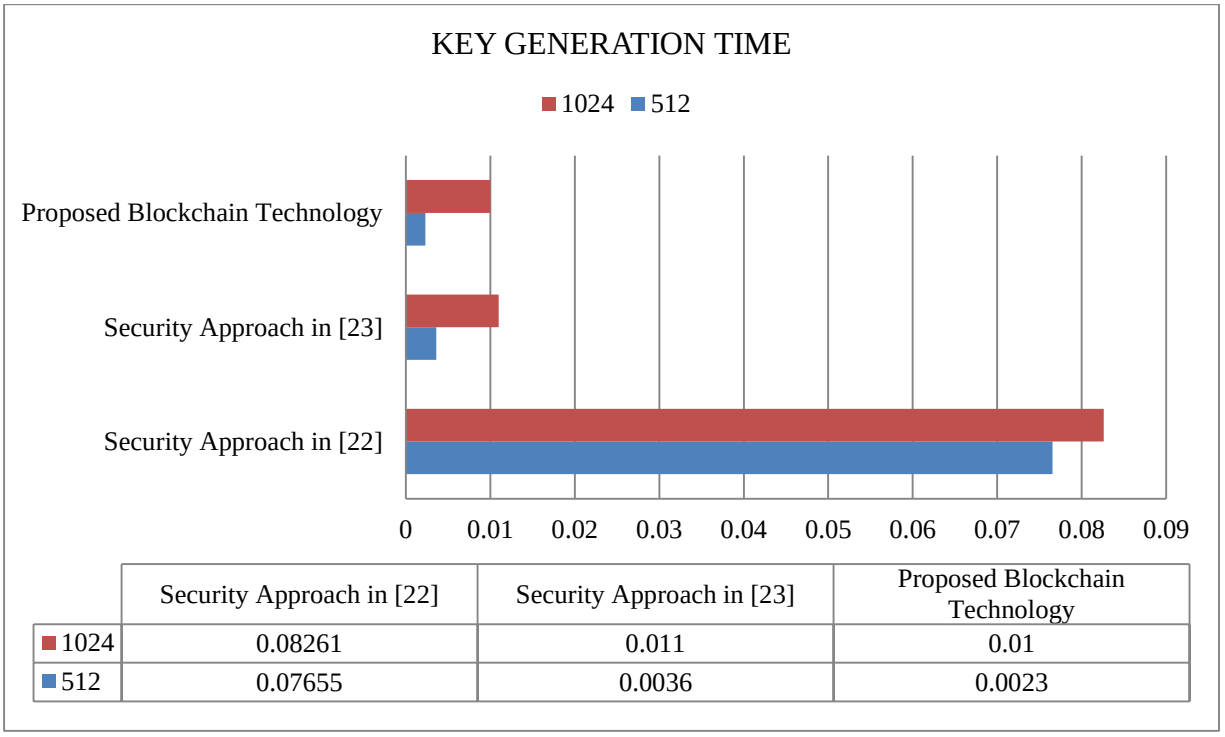


Fig. 11 Network lifetime



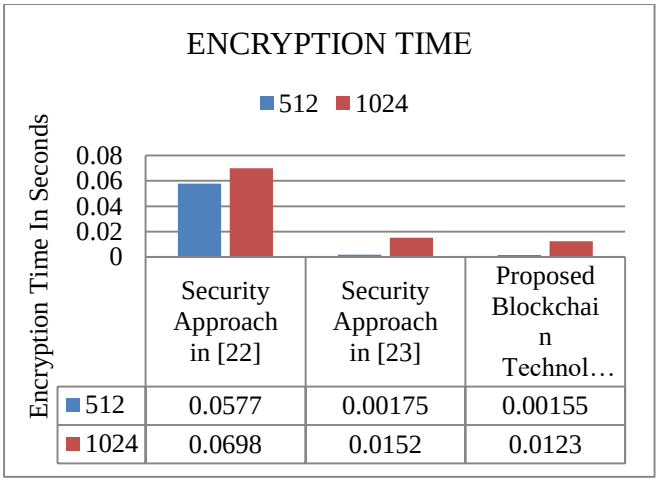
	Security Approach in [22]	Security Approach in [23]	Proposed Blockchain Technology
1024	0.08261	0.011	0.01
512	0.07655	0.0036	0.0023

Fig. 12 Key generation time

Figure 12 represents the key generation time acquired by various security approaches with proposed Blockchain technology, from the graph, it is evident that proposed Blockchain technology required reduced time of 0.0023 s for 512 data size and 0.01 s for 1024 data size, thereby ensuring rapid generation of security keys and improving the system secuirty with enhanced key management process. Meanwhile, the other two approaches proposed in [22, 23] required slightly higher time durations for key generation.

Figure 13 showcases the encryption and decryption times performed by various security approaches. From the chart, it is notable that both the encryption and decryption times required for the proposed blockchain technology are much less than those of the other existing approaches.

The minimal time required for encryption and decryption signifies faster security operations, thus leading to increased system security and protection.



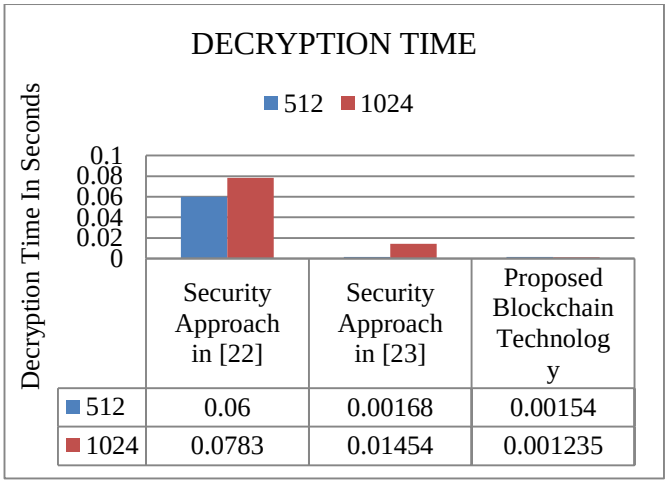


Fig. 13 Encryption time and decryption Time

4. Conclusion

The proposed system utilizing a highly efficient and secure routing algorithm for WSN, effectively improving overall system performance by addressing energy consumption rate, security issues and limited network lifetime. The implementation of a multi-layered ANN-SSO-based routing algorithm effectively achieves optimum routing path selection by adapting to various network conditions, thus increasing the overall system efficiency. Similarly, deploying Blockchain technology into IoT networks provides enhanced data security, protection, privacy and integrity. Blockchain technology assures secure data transmission with increased protection against cyber threats, hence increasing the overall Reliability of the model. The proposed system is validated through NS-2 software. The results demonstrate that the proposed model attained reduced energy consumption and packet loss rates with increased PDR, network lifetime, and throughput. In conclusion, the proposed system effectively enhances the WSN performance efficiency with increased Reliability.

References

[1] Ibrahim A. Abd El-Moghith, and Saad M. Darwish, "Towards Designing a Trusted Routing Scheme in Wireless Sensor Networks: A New Deep Blockchain Approach," *IEEE Access*, vol. 9, pp. 103822-103834, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Saba Awan et al., "Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks," *Sensors*, vol. 22, no. 2, pp. 1-24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] K.H. Vijayendra Prasad, and Sasikumar Periyasamy, "Secure-Energy Efficient Bio-Inspired Clustering and Deep Learning-Based Routing Using Blockchain for Edge Assisted WSN Environment," *IEEE Access*, vol. 11, pp. 145421-145440, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Azath Mubarakali, "An Efficient Authentication Scheme Using Blockchain Technology for Wireless Sensor Networks," *Wireless Personal Communications*, vol. 127, pp. 255-269, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Rahul Nawkhare, and Daljeet Singh, "Machine Learning Approach on Efficient Routing Efficient Techniques in Wireless Sensor Network," *2022 IEEE International Conference on Current Development in Engineering and Technology*, Bhopal, India, pp. 1-6, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Abdul Rehman et al., "Ensuring Security and Energy Efficiency of Wireless Sensor Network by Using Blockchain," *Applied Sciences*, vol. 12, no. 21, pp. 1-22, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Zahoor Ali Khan et al., "A Blockchain-Based Deep-Learning-Driven Architecture for Quality Routing in Wireless Sensor Networks," *IEEE Access*, vol. 11, pp. 31036-31051, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Gebrekiros Gebreyesus Gebremariam, J. Panda, and S. Indu, "Secure Localization Techniques in Wireless Sensor Networks against Routing Attacks Based on Hybrid Machine Learning Models," *Alexandria Engineering Journal*, vol. 82, pp. 82-100, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] S. Harihara Gopalan et al., "An Energy Efficient Routing Protocol with Fuzzy Neural Networks in Wireless Sensor Network," *Ain Shams Engineering Journal*, vol. 15, no. 10, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Lei Hang, and Do-Hyeun Kim, "Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity," *Sensors*, vol. 19, no. 10, pp. 1-26, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[11] Awatef Salem Balobaid et al., "Neural Network Clustering and Swarm Intelligence-Based Routing Protocol for Wireless Sensor Networks: A Machine Learning Perspective," *Computational Intelligence and Neuroscience*, vol. 2023, no. 1, pp. 1-10, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Greeshma Arya, Ashish Bagwari, and Durg Singh Chauhan, "Performance Analysis of Deep Learning-Based Routing Protocol for an Efficient Data Transmission in 5G WSN Communication," *IEEE Access*, vol. 10, pp. 9340-9356, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Rajesh Kumar Varun et al., "Energy-Efficient Routing Using Fuzzy Neural Network in Wireless Sensor Networks," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, pp. 1-13, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Carlos Lester Duenas Santos et al., "ML-RPL: Machine Learning-Based Routing Protocol for Wireless Smart Grid Networks," *IEEE Access*, vol. 11, pp. 57401-57414, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] H.L. Gururaj et al., "Collaborative Energy-Efficient Routing Protocol for Sustainable Communication in 5G/6G Wireless Sensor Networks," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 2050-2061, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Kegomoditswe Boikanyo et al., "Performance Optimization for Mobile Wireless Sensor Networks Routing Protocol Using Adaptive Boosting With Sensitivity Analysis," *IEEE Access*, vol. 12, pp. 146494-146512, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Geetanjali Rathee et al., "A Secure IoT Sensors Communication in Industry 4.0 Using Blockchain Technology," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 533-545, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Sunil Kumar et al., "Division Algorithm Based Energy-Efficient Routing in Wireless Sensor Networks," *Wireless Personal Communications*, vol. 122, pp. 2335-2354, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Saleh A. Alghamdi, "Cuckoo Energy-Efficient Load-Balancing On-Demand Multipath Routing Protocol," *Arabian Journal for Science and Engineering*, vol. 47, pp. 1321-1335, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Mohammed Al Mazaideh, and Janos Levendovszky, "A Multi-Hop Routing Algorithm for WSNs Based on Compressive Sensing and Multiple Objective Genetic Algorithm," *Journal of Communications and Networks*, vol. 23, no. 2, pp. 138-147, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Munuswamy Selvi et al., "An Energy Efficient Clustered Gravitational and Fuzzy Based Routing Algorithm in WSNs," *Wireless Personal Communications*, vol. 116, pp. 61-90, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Chunfu Zhang et al., "An Improved Public Key Cryptographic Algorithm Based on Chebyshev Polynomials and RSA," *Symmetry*, vol. 16, no. 3, pp. 1-15, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Kevin Hendy, and Arya Wicaksana, "Post-Quantum Hybrid Encryption Scheme for Blockchain Application," *International Journal of Innovative Computing, Information and Control*, vol. 18, no. 6, pp. 1701-1717, 2022. [CrossRef] [Google Scholar] [Publisher Link]