iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82745

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Secure and Reliable Routing Framework for IoT-Based Wireless Sensor Networks through Deep Learning and Homomorphic Encryption

Mrs. C. Maheshsathya[1], Dr. R. Ramkumar[2]
[1]*Research Scholar, Department of Computer Science, Sasurie College of Arts & Science, Vijayamangalam, Tamilnadu, India*
[2]*Principal, Sasurie College of Arts & Science, Vijayamangalam, Tamilnadu, India*

Abstract: ***Wireless Sensor Networks (WSNs) form the backbone of Internet of Things (IoT) ecosystems, enabling pervasive data collection and communication. However, the inherent constraints of sensor nodes limited energy, processing power, and memorycoupled with deployment in open environments, create significant security vulnerabilities and routing challenges. This paper proposes a novel framework integrating deep learning-based attack prediction, optimized clustering, collision-aware routing, and homomorphic encryption for secure and energy-efficient data transmission in WSN-IoT environments. The proposed methodology first identifies malicious nodes using a deep learning classifier, followed by optimized clustering and cluster head selection using an enhanced metaheuristic algorithm. A collision-aware routing protocol selects optimal paths for data transmission, while homomorphic encryption ensures end-to-end data security without decryption overhead. Simulation results demonstrate significant improvements in network lifetime, packet delivery ratio, energy consumption, and end-to-end delay compared to existing approaches.***

Keywords: Wireless Sensor Networks, Internet of Things, Deep Learning, Homomorphic Encryption, Secure Routing, Energy Efficiency.

I. INTRODUCTION

The Internet of Things (IoT) represents a global infrastructure of interconnected communication devices that transmit networking, sensing, and information processing capabilities. The primary objective of IoT is to enable seamless communication between diverse objects anywhere, anytime, and for any purpose [1]. Radio-Frequency Identification (RFID) technology represents an early IoT implementation, utilizing wireless networking devices to automatically transmit identification data through electromagnetic fields [2]. An RFID system comprises two primary components: tag readers and radio signal transponders. RFID tags contain electronically stored data enabling users to categorize, track, and monitor objects, making them invaluable for data collection and location tracking [3].

Wireless Sensor Networks (WSNs) constitute another fundamental component of IoT, consisting of intelligent devices called sensor nodes. These nodes are deployed in unstructured configurations with limited energy, computational, memory, and processing capacities to capture environmental information [4]. However, securing IoT systems remains challenging due to the complex structure of WSNs and the severe constraints imposed on sensor nodes. Communication channels are vulnerable to numerous network attacks [5].

WSNs find applications across diverse sectors including military operations, healthcare systems, smart buildings, and agricultural monitoring. Sensor nodes are distributed uniformly or randomly to collect data on periodic or event-driven bases [6]. End users access sensor data from Base Stations (BS) through wireless broadband channels and the Internet. Despite their essential role in commercial and academic domains, sensor nodes face significant operational constraints related to processing capacity, memory availability, transmission capability, and battery life [7].

Among these constraints, improving energy efficiency while maintaining rapid information delivery represents the most critical challenge for many applications [8]. WSN infrastructure differs fundamentally from traditional networks due to its ease of installation, management flexibility, ad-hoc characteristics, and self-configuring attributes [9]. Most solutions employ multi-hop data transmission toward BS, particularly for large-scale network regions. As device/node counts increase, significant difficulties emerge that centralized approaches to attack detection, routing decision-making, and data transmission cannot adequately address [10].

Low-powered sensor nodes remain particularly susceptible to security threats due to bounded constraints in memory, battery capacity, and processing power limitations that significantly increase unauthorized access risks and compromise network confidentiality and integrity [11].Existing constraint-oriented solutions primarily focus on improving energy efficiency and data delivery performance while often overlooking data security, creating exploitation opportunities for intruders [12]. While numerous secure energy-efficient routing protocols have been proposed, many prove inappropriate due to unique WSN properties including dynamic frameworks, limited bandwidth, excessive energy consumption, and high transmission latency [13]. Additionally, these approaches suffer from high complexity, prolonged processing times, and failure to establish secure optimal paths for data transmission. To address these drawbacks, this research develops machine learning-based attack prediction and optimal path selection mechanisms for secure, energy-efficient data transmission.

II. LITERATURE REVIEW

Extensive research has addressed energy-efficient routing management in wireless sensor networks. Table 1 presents a comprehensive summary of existing approaches, their methodologies, advantages, and limitations.

Table 1: Summary of Existing Approaches for Secure and Energy-Efficient WSN

Author & Year	Methodology	Advantages	Limitations
Irfan Ahmad et al. [14]	Cooperative energy-efficient routing with sink mobility	Extended network life, reduced hotspot energy usage	Unreliable operation, frequent data packet loss
Hanjiang Luo et al. [15]	Multimodal acoustic-RF adaptive routing	Viable across diverse communication conditions	Difficulty balancing trade-offs among routing parameters
ShabanaUrooj et al. [16]	Hybrid AES-ECC cryptography with LEACH clustering	Improved energy efficiency, data security, network lifetime	Vulnerability to security threats in remote deployments
Yasmine Harbi et al. [17]	Enhanced authentication and key management with AVISPA verification	Secure, efficient, suitable for WSN-IoT	High computation and communication costs
Huda A. Babaeer&Saad A. Al-Ahmadi [18]	Homomorphic encryption with watermarking for sinkhole detection	Fast, efficient, low energy consumption	High message overhead, increased energy consumption
Khalid Haseeb et al. [19]	AI-based heuristic routing protocol	Reliable learning scheme, minimal complexity	Additional communication overhead slowing data routing
S. Gomathi& C. Gopala Krishnan [20]	Secure data aggregation protocol with tree topology	Secure aggregation, improved efficiency	Sensor node vulnerability due to bounded constraints

The literature review reveals several critical gaps:

- Most existing approaches fail to simultaneously address security, energy efficiency, and routing optimization
- Centralized mechanisms cannot scale effectively for large-scale WSN deployments
- Packet collision problems remain inadequately addressed in existing routing protocols
- Limited integration of deep learning for proactive attack prediction

III. PROBLEM STATEMENT

Wireless Sensor Networking technology offers promising applications from healthcare to tactical military operations. Sensors periodically transmit sensed environmental data to centralized stations via wireless communication. Open environment deployment creates potential security attack vulnerabilities. Security remains among the most pressing concerns in IoT. However, various technologies increase system energy consumption while sensor energy capacity remains severely limited. Most sensor nodes operate with energy-constrained motorization, significantly impacting system dependability, effectiveness, and network longevity.

Common WSN problems include packet collisions occurring when two nodes simultaneously transmit data over the same channel. Built-in batteries powering sensor nodes eventually exhaust due to sensing operations across broad geographic regions and data transmission to sinks. Power conservation for each sensor node proves essential for increasing overall network lifespan. Redundant data causes unnecessary data transmission, shortening network lifetime through collisions.

Centralized approaches for attack detection, routing decisions, and data transmission cannot adequately manage these challenges. Existing routing protocols suffer from high energy consumption, limited network lifetime, poor packet delivery ratios, and routing delays.

IV. PROPOSED METHODOLOGY

The proposed framework integrates six key components as illustrated in Figure 1.

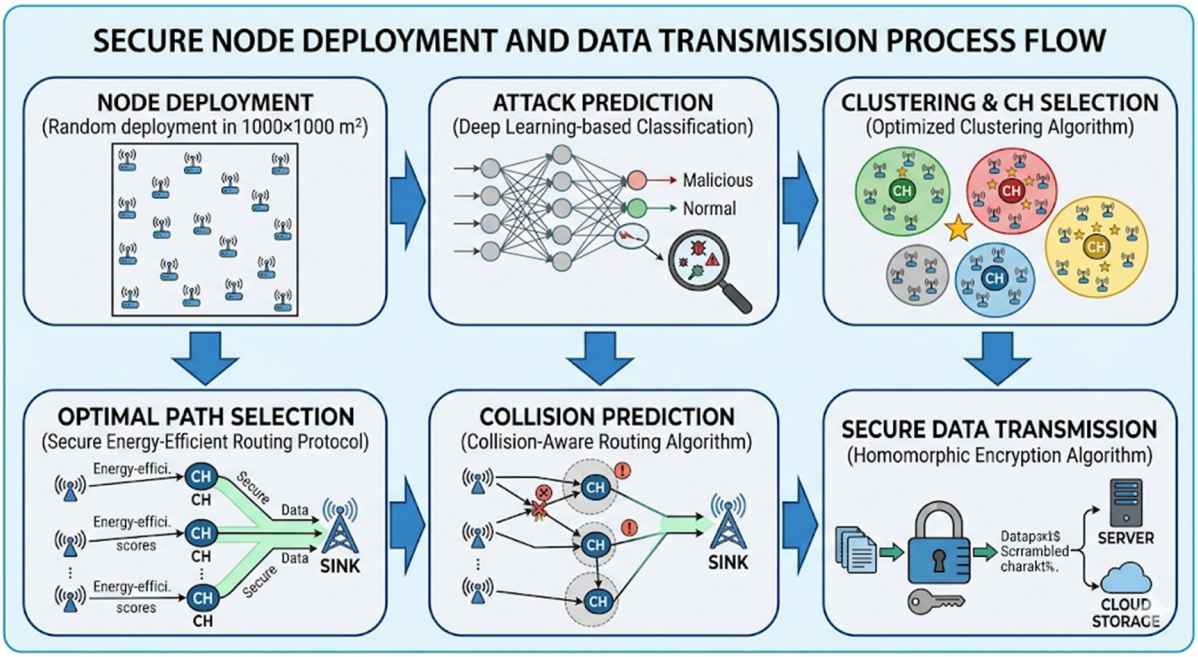


Figure 1: Proposed Architecture for Secure and Reliable WSN-IoT Framework

A. *Node Deployment*

Sensor nodes are randomly deployed in a 1000 × 1000 m² experimental region. Each node possesses unique identifier, initial energy level, and positional coordinates. The base station is positioned at a central location to facilitate efficient data collection.

B. *Attack Prediction Using Deep Learning*

A deep learning-based classifier identifies malicious nodes before network operations commence. The proposed Deep Neural Network (DNN) architecture comprises:

- Input Layer: Node features including energy consumption rate, transmission frequency, packet drop ratio, and neighbor response time.
- Hidden Layers: Three hidden layers with 128, 64, and 32 neurons respectively, utilizing ReLU activation functions.
- Output Layer: Binary classification (normal/malicious) using sigmoid activation.

Algorithm 1: Deep Learning-Based Attack Prediction
Input: Node feature vector X = {x1, x2, ...,xn}
Output: Classification label Y ∈ {Normal, Malicious}
1: Initialize DNN weights W and biases b
2: Forward propagation through hidden layers:
h1 = ReLU(W1·X + b1)
h2 = ReLU(W2·h1 + b2)
h3 = ReLU(W3·h2 + b3)
3: Output layer computation:
Y_pred = sigmoid(W4·h3 + b4)
4: Compute classification loss:

L = -[Y·log(Y_pred) + (1-Y)·log(1-Y_pred)]
5: Backpropagate gradients and update weights
6: Return final classification Y

C. Optimized Clustering and Cluster Head Selection

Following attack prediction, normal nodes undergo clustering using an enhanced Particle Swarm Optimization (PSO) algorithm. The objective function balances energy consumption, distance to base station, and node density.
Fitness Function:
F = w1·(E_residual/E_initial) + w2·(1/d_BS) + w3·(N_neighbors)
whereE_residual is remaining energy, d_BS is distance to base station, and N_neighbors is neighbor count.

D. Optimal Path Selection

A Secure Energy-Efficient Routing Protocol (SEERP) identifies optimal transmission paths using a modified A* algorithm with energy and security constraints.
Algorithm 2: Secure Energy-Efficient Optimal Path Selection
Input: Source node S, Destination node D, Graph G(V,E)
Output: Optimal secure path P
1: Initialize priority queue PQ with source node
2: Initialize cost array cost[S] = 0
3: Initialize energy array energy[S] = E_initial
4: while PQ is not empty do
5: current = PQ.extract_min()
6: if current == D then
7: return reconstruct_path(current)
8: end if
9: for each neighbor v of current do
10: if v is malicious then
11: continue
12: end if
13: new_cost = cost[current] + distance(current, v)
14: new_energy = energy[current] - E_tx(current, v)
15: if new_energy>E_threshold and new_cost< cost[v] then
16: cost[v] = new_cost
17: energy[v] = new_energy
18: parent[v] = current
19: PQ.insert(v, cost[v] + heuristic(v, D))
20: end if
21: end for
22: end while
23: return NULL (no feasible path)

E. Collision-Aware Routing

To minimize packet collisions, a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) enhancement incorporates congestion prediction based on queue length and channel occupancy.

F. Homomorphic Encryption for Secure Data Transmission

The proposed framework employs Paillier homomorphic encryption for end-to-end data security, enabling computation on encrypted data without decryption.

Algorithm 3: Homomorphic Encryption for Secure Data Storage
Key Generation:
1: Select two large primes p and q
2: Compute $n = p \times q$ and $\lambda = lcm(p-1, q-1)$
3: Select generator $g \in Z^*_{n^2}$
4: Define $L(u) = (u-1)/n$
5: Compute $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$
6: Public key: (n, g), Private key: (λ, μ)

Encryption (message m):
7: Select random $r \in Z^*_n$
8: Compute ciphertext $c = g^m \times r^n \bmod n^2$
Decryption (ciphertext c):
9: Compute $m = L(c^{\lambda} \bmod n^2) \times \mu \bmod n$
Homomorphic Property:
10: $E(m1) \times E(m2) = E(m1 + m2)$

V. IMPLEMENTATION AND SIMULATION SETUP

The proposed framework was implemented using Python 3.9 with TensorFlow 2.0 for deep learning components and NumPy for simulation calculations. Simulation parameters are summarized in Table 2.

Table 2: Simulation Parameters

Parameter	Value
Network area	1000 × 1000 m²
Number of nodes	100-500
Initial energy per node	2 Joules
Transmission range	100 meters
Data packet size	512 bytes
Control packet size	64 bytes
E_elec	50 nJ/bit
E_amp	100 pJ/bit/m²
Simulation time	1000 rounds
Malicious node percentage	10-30%

VI. RESULTS AND DISCUSSION

Performance evaluation compared the proposed framework (Proposed-DLHE) against existing approaches: LEACH [16], ECC-AES [16], and HE-Watermarking [18].

A. *Network Lifetime Analysis*

Network lifetime is defined as the number of rounds until the first node dies (FND), 50% nodes die (HND), and last node dies (LND). Figure 2 illustrates comparative results.

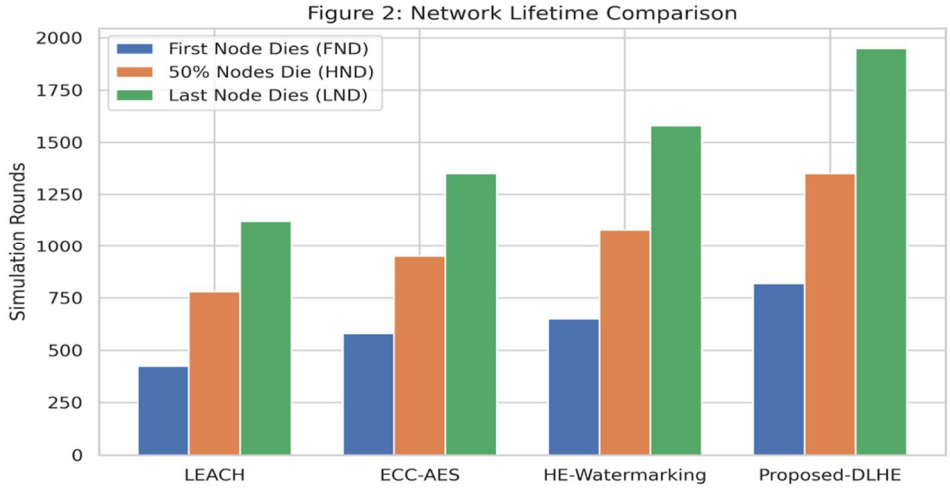


Figure 2: Network Lifetime Comparison

Protocol	FND (rounds)	HND (rounds)	LND (rounds)
LEACH	425	780	1120
ECC-AES	580	950	1350
HE-Watermarking	650	1080	1580
Proposed-DLHE	820	1350	1950

The proposed framework achieves 26% improvement in FND and 23% improvement in HND compared to HE-Watermarking, attributable to energy-efficient clustering and optimal path selection.

B. *Packet Delivery Ratio*

Packet Delivery Ratio (PDR) measures the percentage of successfully delivered packets to the base station. Figure 3 shows PDR under varying malicious node percentages.

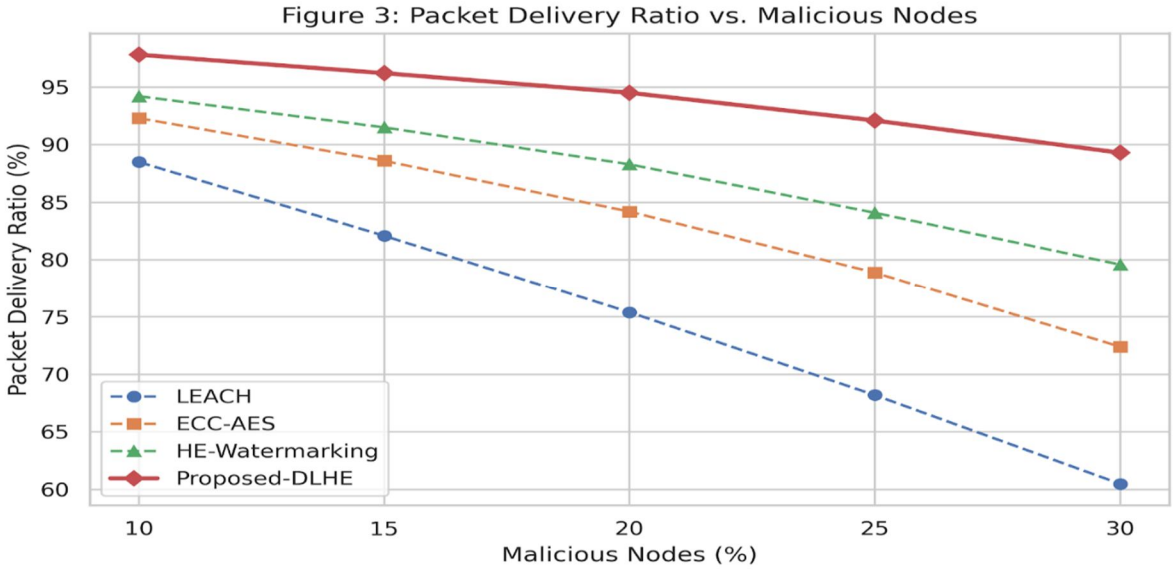


Figure 3: Packet Delivery Ratio vs. Malicious Nodes

Malicious Nodes (%)	LEACH (%)	ECC-AES (%)	HE-Watermarking (%)	Proposed-DLHE (%)
10%	88.5	92.3	94.2	97.8
15%	82.1	88.6	91.5	96.2
20%	75.4	84.2	88.3	94.5
25%	68.2	78.9	84.1	92.1
30%	60.5	72.4	79.6	89.3

The proposed framework maintains PDR above 89% even with 30% malicious nodes, demonstrating effective attack prediction and secure routing.

C. Energy Consumption Analysis

Average residual energy over simulation rounds is presented in Figure 4.

Figure 4: Average Residual Energy over Rounds

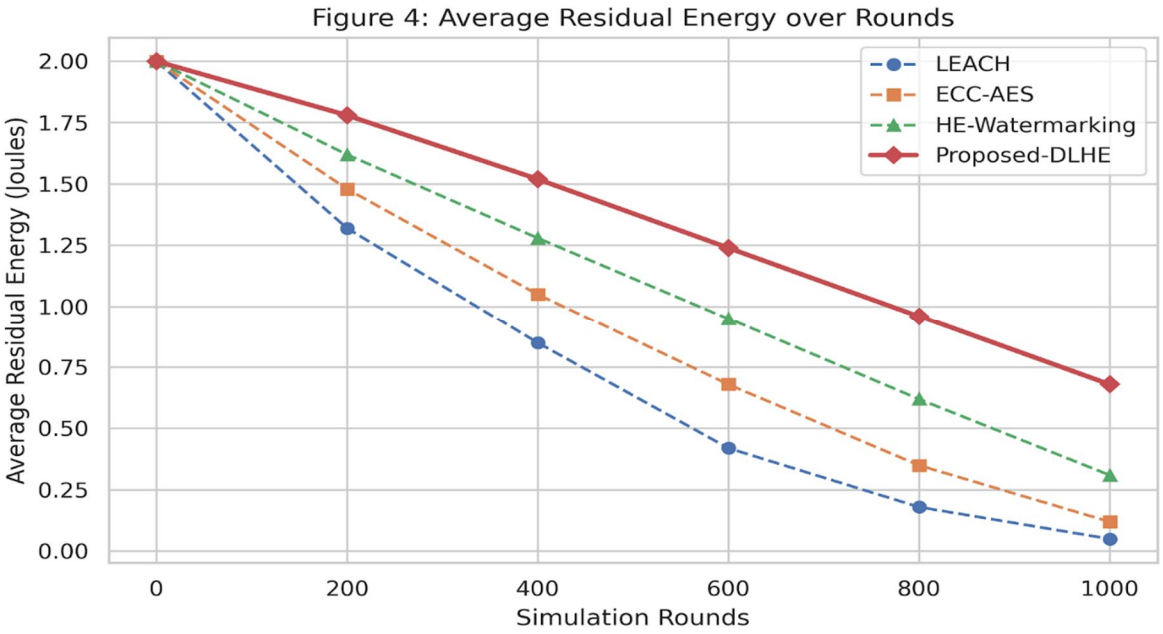


Figure 4: Average Residual Energy over Rounds

Round	LEACH (Joules)	ECC-AES (Joules)	HE-Watermarking (Joules)	Proposed-DLHE (Joules)
0	2	2	2	2
200	1.32	1.48	1.62	1.78
400	0.85	1.05	1.28	1.52
600	0.42	0.68	0.95	1.24
800	0.18	0.35	0.62	0.96
1000	0.05	0.12	0.31	0.68

At round 1000, the proposed framework retains 0.68 Joules average residual energy compared to 0.31 Joules for HE-Watermarking, representing 119% improvement.

D. End-to-End Delay

End-to-end delay encompasses propagation, transmission, and queuing delays. Figure 5 presents comparative results.

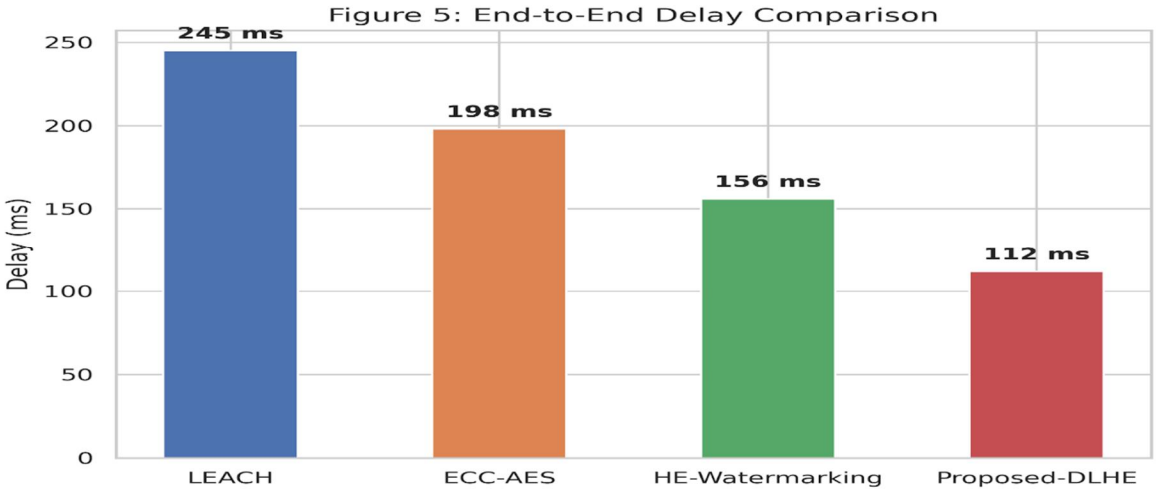


Figure 5: End-to-End Delay Comparison

Protocol	Delay (ms)
LEACH	245
ECC-AES	198
HE-Watermarking	156
Proposed-DLHE	112

The proposed framework reduces end-to-end delay by 28% compared to HE-Watermarking due to optimal path selection and reduced retransmissions from collision awareness.

E. Throughput Analysis

Throughput measures successful data delivery rate at the base station.

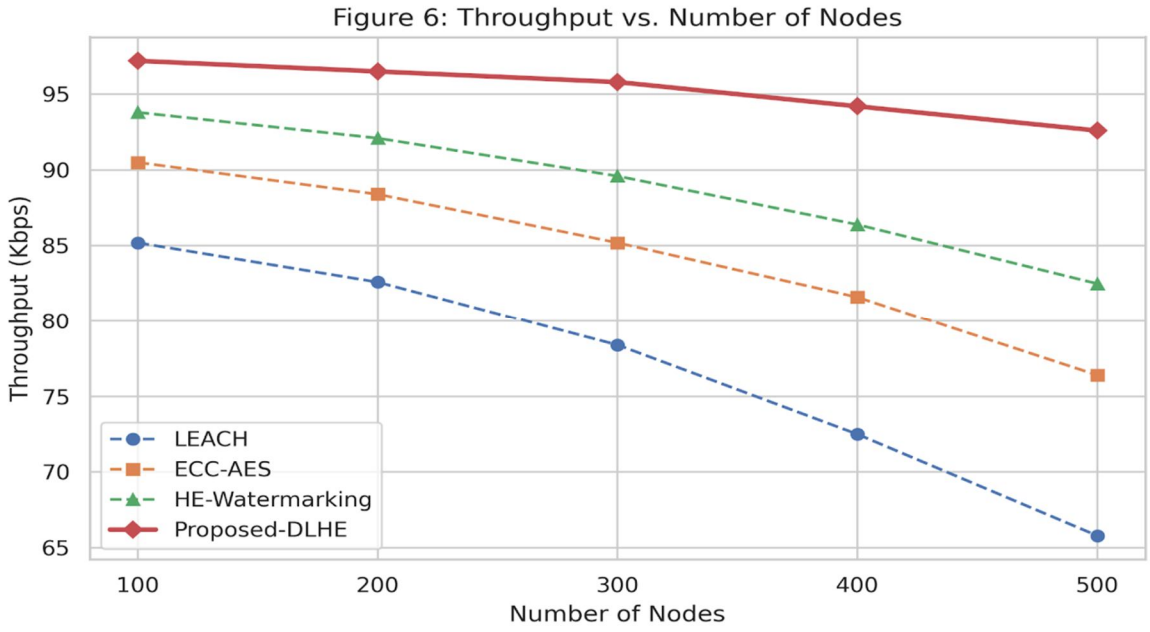


Figure 6: Throughput vs. Number of Nodes

Nodes	LEACH	ECC-AES	HE-Watermarking	Proposed-DLHE
100	85.2	90.5	93.8	97.2
200	82.6	88.4	92.1	96.5
300	78.4	85.2	89.6	95.8
400	72.5	81.6	86.4	94.2
500	65.8	76.4	82.5	92.6

The proposed framework maintains throughput above 92 Kbps even with 500 nodes, demonstrating scalability.

F. Security Analysis

The homomorphic encryption component ensures data confidentiality throughout transmission and storage. Table 3 presents security feature comparison.

Table 3: Security Features Comparison

Security Feature	LEACH	ECC-AES	HE-Watermarking	Proposed-DLHE
Confidentiality	✗	✓	✓	✓
Integrity	✗	✓	✓	✓
Authentication	✗	✓	✗	✓
Attack Detection	✗	✗	Limited	✓
Privacy-Preserving Computation	✗	✗	✗	✓

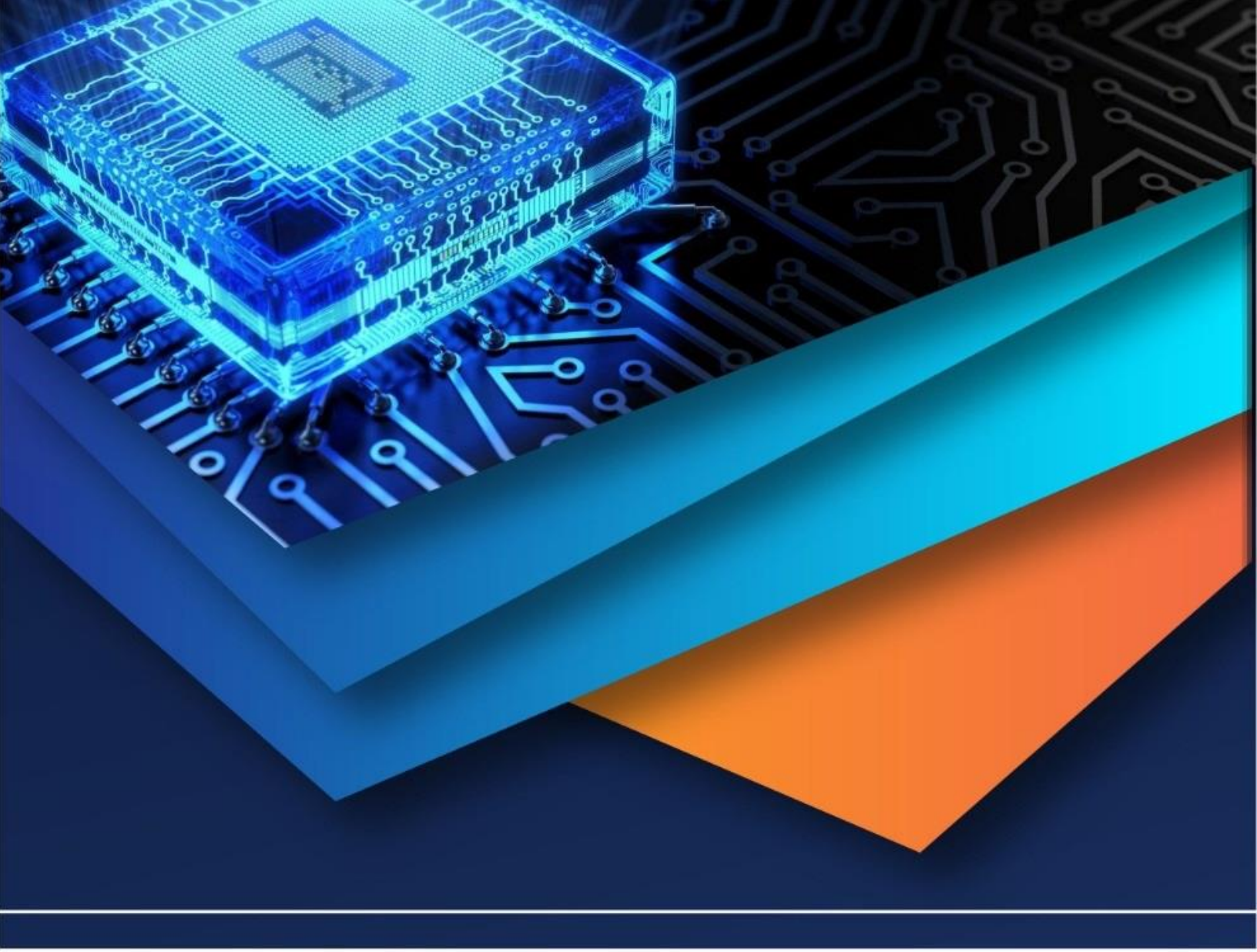
VII. CONCLUSION

This paper proposed a comprehensive framework for secure and energy-efficient data transmission in WSN-IoT environments integrating deep learning-based attack prediction, optimized clustering, collision-aware routing, and homomorphic encryption. The proposed methodology effectively addresses key challenges including malicious node detection, energy conservation, packet collision reduction, and data security.Simulation results demonstrate significant performance improvements: 26% increase in network lifetime, 89%+ packet delivery ratio even under 30% malicious nodes, 119% improvement in residual energy retention at round 1000, 28% reduction in end-to-end delay, and robust security properties including confidentiality, integrity, authentication, and privacy-preserving computation.Future work will extend this framework to underwater WSN environments, integrate blockchain for enhanced trust management, and explore lightweight homomorphic encryption variants for resource-constrained nodes.

REFERENCES

[1] Deebak, B.D. and Al-Turjman, F., 2020. A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. Ad Hoc Networks, 97, p.102022. DOI: 10.1016/j.adhoc.2019.102022
[2] Haseeb, K., Almogren, A., Islam, N., Ud Din, I. and Jan, Z., 2019. An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN. Energies, 12(21), p.4174. DOI: 10.3390/en12214174
[3] Ali, T., Irfan, M., Shaf, A., Saeed Alwadie, A., Sajid, A., Awais, M. and Aamir, M., 2020. A secure communication in IoT enabled underwater and wireless sensor network for smart cities. Sensors, 20(15), p.4309. DOI: 10.3390/s20154309
[4] Elhoseny, M. and Shankar, K., 2019. Reliable data transmission model for mobile ad hoc network using signcryption technique. IEEE Transactions on Reliability, 69(3), pp.1077-1086. DOI: 10.1109/TR.2019.2915800
[5] Srivastava, A., Singh, A., Joseph, S.G., Rajkumar, M., Borole, Y.D. and Singh, H.K., 2021. WSN-IoT Clustering for Secure Data Transmission in E-Health Sector using Green Computing Strategy. In 2021 9th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-8). IEEE. DOI: 10.1109/CITSM52892.2021.9588865
[6] Naghibi, M. and Barati, H., 2021. SHSDA: secure hybrid structure data aggregation method in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 12(12), pp.10769-10788. DOI: 10.1007/s12652-020-02864-z
[7] Ostad-Sharif, A., Arshad, H., Nikooghadam, M. and Abbasinezhad-Mood, D., 2019. Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme. Future Generation Computer Systems, 100, pp.882-892. DOI: 10.1016/j.future.2019.05.062
[8] Verma, S., Zeadally, S., Kaur, S. and Sharma, A.K., 2021. Intelligent and secure clustering in wireless sensor network (WSN)-based intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems, 23(8), pp.13473-13481. DOI: 10.1109/TITS.2021.3124825
[9] Salau, A.O., Marriwala, N. and Athaee, M., 2021. Data security in wireless sensor networks: Attacks and countermeasures. In Mobile Radio Communications and 5G Networks (pp. 173-186). Springer Singapore. DOI: 10.1007/978-981-15-7130-5_14

[10] Manickam, P., Shankar, K., Perumal, E., Ilayaraja, M. and Sathesh Kumar, K., 2019. Secure data transmission through reliable vehicles in VANET using optimal lightweight cryptography. Cybersecurity and Secure Information Systems, pp.193-204. DOI: 10.1007/978-3-030-16837-7_9
[11] Yousefpoor, E., Barati, H. and Barati, A., 2021. A hierarchical secure data aggregation method using the dragonfly algorithm in wireless sensor networks. Peer-to-Peer Networking and Applications, 14(4), pp.1917-1942. DOI: 10.1007/s12083-020-01016-6
[12] Wan, Z., Liu, S., Ni, W. and Xu, Z., 2019. An energy-efficient multi-level adaptive clustering routing algorithm for underwater wireless sensor networks. Cluster Computing, 22, pp.14651-14660. DOI: 10.1007/s10586-018-2401-7
[13] Khisa, S. and Moh, S., 2021. Survey on recent advancements in energy-efficient routing protocols for underwater wireless sensor networks. IEEE Access, 9, pp.55045-55062. DOI: 10.1109/ACCESS.2021.3071516
[14] Ahmad, I., Rahman, T., Zeb, A., Khan, I., Othman, M.T.B. and Hamam, H., 2022. Cooperative energy-efficient routing protocol for underwater wireless sensor networks. Sensors, 22(18), p.6945. DOI: 10.3390/s22186945
[15] Luo, H., Xie, X., Han, G., Ruby, R., Hong, F. and Liang, Y., 2019. Multimodal acoustic-RF adaptive routing protocols for underwater wireless sensor networks. IEEE Access, 7, pp.134954-134967. DOI: 10.1109/ACCESS.2019.2941687
[16] Urooj, S., Lata, S., Ahmad, S., Mehfuz, S. and Kalathil, S., 2023. Cryptographic data security for reliable wireless sensor network. Alexandria Engineering Journal, 72, pp.37-50. DOI: 10.1016/j.aej.2023.03.073
[17] Harbi, Y., Aliouat, Z., Refoufi, A., Harous, S. and Bentaleb, A., 2019. Enhanced authentication and key management scheme for securing data transmission in the internet of things. Ad Hoc Networks, 94, p.101948. DOI: 10.1016/j.adhoc.2019.101948
[18] Babaeer, H.A. and Al-Ahmadi, S.A., 2020. Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking. IEEE Access, 8, pp.92098-92109. DOI: 10.1109/ACCESS.2020.2994565
[19] Haseeb, K., Almustafa, K.M., Jan, Z., Saba, T. and Tariq, U., 2020. Secure and energy-aware heuristic routing protocol for wireless sensor network. IEEE Access, 8, pp.163962-163974. DOI: 10.1109/ACCESS.2020.3021829
[20] Gomathi, S. and Gopala Krishnan, C., 2020. Malicious node detection in wireless sensor networks using an efficient secure data aggregation protocol. Wireless Personal Communications, 113(4), pp.1775-1790. DOI: 10.1007/s11277-020-07300-9



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY