I.J. Wireless and Microwave Technologies, 2026, 4, 65-79
Published Online on August 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2026.04.05

OptiBC-WSN: Multi-Objective Optimization for Energy Efficiency, Security, and Scalability in IoT-Based Wireless Sensor Networks

S. Swapna Kumar*
Department of Electronics and Communication Engineering, Srinivas University, Mukka, Mangalore - 576146, Karnataka, India
Department of Electronics and Communication Engineering, VAST, Thalakkottukara- 680501, India
E-mail: drsswapnakumar@gmail.com
ORCID iD: https://orcid.org/0000-0002-1637-0343
*Corresponding Author

K. Satyanarayan Reddy
Vice Chancellor, Srinivas University, Mukka, Surathkal, Mangalore - 576146, Karnataka, India
E-mail: vicechancellor@srinivasuniversity.edu.in
ORCID iD: https://orcid.org/0000-0003-1474-2577

Received: May 28, 2026; Revised: June 10, 2026; Accepted: July 26, 2026; Published: August 8, 2026

Abstract: Wireless Sensor Networks (WSNs) are the core of Internet of Things (IoT) applications as they enable energy-efficient and scalable real-time data acquisition. However, WSN-based IoT systems have been facing great challenges in achieving energy efficiency, security and scalability especially in applications like smart agriculture. To tackle these problems, this study proposes a new framework called OptiBC-WSN that combines Particle Swarm Optimisation (PSO) clustering, AES-128 encryption, Proof of Authority (PoA) blockchain and Random Forest-based Intrusion Detection System (IDS). We have implemented PSO for energy efficient clustering, PoA for trust management and a Random Forest-based IDS for attack detection on Intel Berkeley and GreenOrbs datasets. OptiBC-WSN consumes 0.25 mJ/node energy, LEACH consumes 5 mJ/node and K-Means+Bee consumes 0.3 mJ/node. It also achieves a breach rate of 0.13% vs. 2% for LEACH and 0.2% for K-Means+Bee and scales to 10,000 nodes with 15,950 bytes overhead (vs. 20,000 bytes for LEACH). Its IDS has 90% accuracy to DDoS, Sybil and Jamming attacks with fairness index 0.92. We perform scale-up tests from 100 to 10K nodes with GreenOrbs dataset and synthetic topology generation, and validate core energy and security metrics with the Intel Berkeley dataset (54 nodes). In smart agriculture it cuts irrigation by 15% and CO2 emissions by 60 kg/1,000 nodes/year. Future work will explore the use of blockchain sharding and adaptive IDS to improve the scalability and security of IoT.

Index Terms: Wireless Sensor Networks, Blockchain, Clustering, Intrusion Detection System, Particle Swarm Optimization, Internet of Things, Energy efficiency, Security

1. Introduction

WSN is a spatially distributed sensor node integrated with Internet of Things (IoT) technology. WSN integrated with IoT enable real time data collection in smart applications such as agriculture, environment monitoring, disaster management, process automation. To solve the problems of security, scalability and energy efficiency, the sensors, processors and communication devices are integrated with the right protocols [8,33,35]. The importance of energy efficient communication protocols discussed in the early works is still a cornerstone for WSNs optimization [1].

Bio-inspired algorithms and hybrid clustering are highlighted as recent advances for achieving scalability and energy efficiency [14,20]. In addition, the integration of Blockchain technology provides possible solutions for secure and distributed data management in IoT networks [5,6,23]. IoT applications are rapidly increasing and hence require new consensus techniques and long-term deployments [7,8,34].

Such technology has problems with scale, security vulnerabilities and energy constraints that prevent its widespread use. On the other hand, the previous works showed significant improvements in terms of energy saving and network life

time [3]. AES-128 encryption techniques, which are centralized and carry the danger of single-point failure, were used in several approaches [9]. Existing protocols struggle to balance low energy consumption, robust security, and high scalability, often incurring high overhead or breach rates. This introduction provides an outline of the scope of our analysis, discusses major challenges and opportunities in WSNs and IoT and provides a foundation for a detailed exploration of state-of-the-art solutions to drive sustainable technological advancements.

1.1. About Existing Systems

The existing WSN-IoT frameworks use clustering, optimization algorithms, encryption techniques, blockchain integration and intrusion detection mechanisms to enhance the network performance. These approaches have shown progress in improving energy efficiency, communication reliability and security in resource-constrained environments [1,4,5,9,16,17,25]. Nevertheless, many existing solutions consider energy efficiency, security, and scalability in isolation, leading to trade-offs among these objectives. However, despite its promising benefits, there are many challenges (e.g., communication overhead, security, and resource utilization) faced in large-scale IoT deployments. Thus, there is a need for an integrated framework that optimally considers energy consumption, security, privacy, and scalability for the next-generation IoT-enabled wireless sensor networks.

1.2. Problem Statement

WSN protocols face significant challenges in balancing energy efficiency, security and scalability which limits their effectiveness in IoT applications. Existing solutions suffer from high energy consumption, reduced network lifetime, security issues, communication overhead and scalability constraints [1,4,25]. Moreover, the static nature of the intrusion detection models could lead to overfitting, which decreases their potential to adapt to the evolving attack patterns [13]. Although blockchain-based approaches enhance trust and data integrity, they can introduce extra computational and communication overhead for resource-constrained sensor nodes [5,23]. Thus, IoT deployments in dynamic environments demand an integrated WSN framework that simultaneously optimizes energy efficiency, enhances security and supports scalable operation.

1.3. Motivation

The rapid growth of IoT-enabled applications such as smart agriculture, environmental monitoring, and industrial automation has led to the increased need for WSN frameworks that provide energy efficiency, security, and scalability [8,33]. However, these objectives are often addressed separately in existing approaches, resulting in tradeoffs among network lifetime, communication overhead and security robustness [1,4,5,25]. Large scale deployments must robustly manage trust, detect attacks and efficiently use resources while operating under tight energy constraints. These challenges inspire the development of the proposed OptiBC-WSN framework, which integrates clustering optimization, secure communication, blockchain-based trust management and intelligent intrusion detection in a unified architecture. The goal is to provide a safe, energy-efficient and scalable solution for future IoT-enabled wireless sensor networks.

1.4. Objectives

The study intends to develop and validate the OptiBC-WSN framework for improving WSNs for IoT applications with the following objectives:

1. Design an energy-efficient clustering framework using PSO and duty-cycling techniques that reduce the energy consumption to less than 0.3 mJ/node and increase network lifetime [1,4,17,32]
2. To strengthen network security using AES-128 encryption, PoA blockchain and Random Forest-based intrusion detection, targeting breach rates below 0.15% [5,25].
3. To enable scalable WSN-IoT deployments of up to 10,000 nodes with communication overhead less than 16,000 bytes per iteration and fairness index greater than or equal to 0.90 [4,25,35].
4. To evaluate the proposed framework on benchmark datasets and to determine the applicability of the proposed framework for smart agriculture and other large scale IoT applications [2,4].

The remainder of the paper is organized as follows: Section 2 reviews related work; Section 3 describes the system design and methodology; The Simulation and analysis result are presented in Section 4, Broader implications are discussed in Section 5, The paper is concluded and the future research scopes are mentioned in Section 6, and the list of all the cited works is provided in the references section.

2. Literature Survey

Studies on IoT-based WSNs are mainly focused on energy efficiency, security and scalability for applications such as smart agriculture [8,33]. Akyildiz et al. [22] provided a seminal survey on WSNs, bringing out issues in energy constraints, data aggregation, and scalability, which are still critical in IoT deployments. The LEACH protocol [1] introduced the concept of hierarchical clustering, obtaining an energy consumption of 5 mJ/node but with a high overhead

(~20,000 bytes) and a limited lifetime of 800 rounds, which is not suitable for dense networks [1,35]. While the bio-inspired clustering of K-Means+Bee [4] is energy efficient at 0.3 mJ/node and good for a 1500 round lifetime, it is not without its faults. The fairness index is a modest 0.90 and it does not scale well past 5,000 nodes; a 0.2% breach rate also points to some security shortcomings [4,35]. Indeed, such protocols struggle to strike the right balance between energy and security, which limits their effectiveness in a dynamic IoT setting [3,10]. Then there are the optimization-based clustering approaches, including PSO-based methods [27,29] and GWO-based schemes [30], which improve cluster-head selection and energy efficiency, while duty-cycling methods [17,31] further reduce energy consumption.

However, these methods do not have strong enough security mechanisms and networks are vulnerable to attacks such as DDoS and Sybil [13,21]. AES-128 encryption [9,28] has low breach rates (<0.2%) with low overhead (0.02 mJ/node), but centralized approaches are vulnerable to single point failures [9]. Random Forest-based Intrusion Detection System (IDS) [13,21] has 85-90% accuracy against DDoS, Sybil and Jamming attacks, but has the problem of overfitting and hence is less adaptive to new threats [13]. Proof of Authority (PoA) [5,23] blockchain frameworks provide minimal computational overhead (0.02 mJ/node) for trust and data integrity, but present scalability issues [19,24] when applied in resource-constrained WSNs. Scalability studies [10,25] have shown stability up to 10,000 nodes but the high communication overhead (16,500 bytes) is still present and affects efficiency in ultra-dense networks [10].

The proposed OptiBC-WSN framework is a combination of PSO, AES-128, PoA blockchain, and Random Forest IDS to achieve 0.25 mJ/node, 0.13% breach rate, and scalability to 10,000 nodes with 15,950 bytes overhead [2,10,35]. OptiBC-WSN offers a full solution for IoT applications by overcoming the limitations of current protocols such as higher energy costs and lack of security [5,19]. A comparison of related literature, highlighting different related areas for the improvements in energy use, security and scalability, is presented in Table 1.

Table 1. Comparison of Related Papers

Author (Year)	Methodology	Key Findings	Advantages	Parameters	Limitations
Heinzelman et al. [1] (2000)	Randomized hierarchical clustering	Energy: 5 mJ/node, Lifetime: 800 rounds, Overhead: ~20,000 bytes	Simple clustering, low setup cost	Cluster size: 5–10%	No IDS, high overhead, scales poorly (>1,000 nodes)
Modey et al. [4] (2024)	K-means + Bee colony optimization	Energy: 0.3 mJ/node, Breach: 0.2%, Lifetime: 1500 rounds	15% energy savings, fair clustering	Fairness: 0.90 [35], Nodes: ≤5,000	Weak IDS (<90% accuracy), limited scalability
Sudharson et al. [5] (2020)	Trust-based PoA blockchain	Energy: 0.35 mJ/node, Breach: 0.18%, Lifetime: 1400 rounds	Secure trust model	Overhead: ~17,000 bytes, Nodes: ≤3,000	High computational overhead, no IDS
Rana et al. [17] (2024)	Duty-cycling in dense WSNs	Energy: 0.28 mJ/node, Lifetime: 1550 rounds	15% energy savings	Duty cycle: 10%, Nodes: ≤7,000	No security, high overhead (~16,800 bytes)
Hewa et al. [25] (2025)	Blockchain-for 5G and IoT	Energy: 0.3 mJ/node, Breach: 0.2%, Lifetime: 1500 rounds	Secure data logging	Overhead: ~16,500 bytes, Nodes: ≤5,000	High energy, no IDS, scalability bottleneck

3. System Design and Methodology

This section introduces the framework of OptiBC-WSN, which integrates K-means clustering, Particle Swarm Optimization (PSO), AES-128 encryption, duty-cycling, and Proof-of-Authority (PoA) blockchain for enhancing the energy efficiency, security, and scalability of WSNs in IoT applications.

3.1. System Model and Assumptions

The proposed WSN model consists of 100–10,000 sensor nodes (SNs) deployed in a 100 × 100 m² area, which is scalable up to 2,000 × 2,000 m². The scalability experiments were conducted on the GreenOrbs dataset and the synthetic topology generation based on node-density characteristics of the Intel Berkeley Research Lab dataset [2]. The core energy-consumption, security and intrusion-detection performance metrics were validated primarily using the Intel Berkeley dataset with 54 sensor nodes, while the large scale scalability analysis was performed using GreenOrbs-based and synthetic network topologies.

The nodes are classified as:

- Sensor Nodes Layer (SNsL): To sense and transmit 512-byte data packets.
- Sink Nodes (SNs): They act as cluster heads, validators of blockchain and controllers of IDS (Intrusion Detection System).
- Base Station (BS) located at (150, 50) collects data from SNs [1].

The energy consumption is derived from a combined first order radio communication model [1] and blockchain

transaction model [19] which are described by equations (1), (2) and (3).

$$\textit{Transmission Energy: } E_{Tx}(k,d) = E_{elec}k + \epsilon_{amp}kd^n \tag{1}$$

$$\textit{Reception Energy: } E_{Rx}(k) = E_{elec}k \tag{2}$$

$$\textit{Duty-Cycling [17]: } E_{DC} = E_{active}T_{on} + E_{sleep}T_{off} \tag{3}$$

where k is the packet size, d the transmission distance, and n is the path loss exponent. $E_{elec} = 50nJ/bit$, $\varepsilon_{amp} = 100$ pJ/bit/m^2, $k = 512\ bytes$, duty cycling with a 50% on/off ratio. The PoA blockchain adds a consensus energy overhead of 0.02 mJ/node per transaction [5,19].

3.2. Optimization Techniques

To optimize energy and security to enhance energy efficiency and security, the framework adopts the following strategies:

1. *K-means Clustering*: Sensor nodes are divided into clusters to minimize the distance between the nodes within a cluster, which leads to a 15% reduction in energy consumption [4] as shown in equations (4).

$$min \sum_{i=1}^{K} \sum_{x \in C_i} \|x - \mu_i\|^2 \tag{4}$$

The clustering and optimization process is carried out in two successive phases. We first apply K-means clustering to partition sensor nodes into K clusters based on geographical proximity by minimizing the intra-cluster distance given in Eq. (4). Then, in each cluster, the best Cluster Head(CH) is obtained using Particle Swarm Optimization (PSO). The PSO algorithm evaluates candidate nodes based on a fitness function that takes into account residual energy, distance to the base station, and node connectivity. This sequential approach enables K-means-based efficient spatial grouping and bio-inspired optimization based cluster-head selection which improves the energy efficiency and network lifetime [11,15].

PSO uses a fitness function considering residual energy, distance to the base station and node connectivity to find the optimal Cluster Head (CH). The fitness function is expressed as in Equation (5).

$$f(x) = \alpha E_{residual}(x) + \beta d(x, BS) + \gamma \left(\frac{1}{degree(x)}\right) \tag{5}$$

where $E_{residual}(x)$ is the residual energy of node x, d(x,BS) is the distance between node x and base station and degree(x) is the node connectivity. The weighting coefficients α, β and γ are chosen as 0.5, 0.3 and 0.2, respectively. PSO algorithm is used to find out the node with maximum energy availability with minimum communication distance and sufficient connectivity to enhance the network life and energy efficiency.

2. *PSO -Based Cluster Head Selection*: Select cluster heads (CH) position with adaptive PSO inertia (0.9 to 0.4) which improve 20% convergence [16], [27] as given in equations (6) and (7). Inertia update (adaptive velocity)

$$v_i^{(t+1)} = \omega_t v_{i,d}^t + \alpha r_{1,d}(pbest_i - x_i^t) + \beta r_{2,d}(gbest - x_i^t) \tag{6}$$

$$x_i^{(t+1)} = x_i^t + v_i^{(t+1)} \tag{7}$$

where inertia weight w varies from 0.9 to 0.4, ensuring convergence.

3. *AES-128 Encryption*: Provides packet confidentiality with 0.02 mJ/node overhead and reduces breaches to 0.15% [9], [28].
4. *Duty-Cycling*: Implements nodes with 50% active/sleep cycles, reducing energy consumption by 15% [17].
5. *Blockchain Integration (PoA)*: Data hashes are stored on a lightweight Proof of Authority (PoA) blockchain to increase trust, privacy, and data integrity [5,19,23]. The CHs, which are selected by the PSO optimization process, act as validator nodes. Each block is 512 bytes in size, which is the same as one sensed data packet. In each sensing round, one transaction is created. Consensus is reached by majority vote of validator nodes (>50%). The blockchain energy overhead is about 0.02 mJ/node/transaction, which is consistent with the previous PoA-based WSN studies [5,19]. PoA reduces the computational overhead compared to traditional blockchain mechanisms while ensuring secure and decentralized data validation [24].
6. *Random Forest IDS*: Identifies DDoS, Sybil, and Jamming attacks with 90% accuracy [13,21].

Algorithm 1: Blockchain-Enhanced Cluster Optimization

Input: Node positions N, initial energy E, number of clusters K
Output: Cluster head assignments, blockchain ledger
Steps:

1. *Set initial particle positions and velocities*
2. *Evaluate fitness using energy and distance*
3. *While iteration < Max_iter:*
   - *Update inertia weight w (0.9 to 0.4)*
   - *Update* $w=w_{max}-((w_{max}-w_{min})*\text{iteration}/\text{Max\_iter})$.
   - *Adjust velocity and position using (5), (6)*
   - *Evaluate fitness, update pBest and gBest.*
4. *Assign cluster heads, encrypt data using AES-128.*
5. *Log encrypted data hashes to the PoA blockchain, where PSO-selected cluster heads act as validators and consensus is achieved through majority approval (>50%).*
6. *Return gBest and the final ledger.*

3.3. Block Diagram

Figure 1 shows the proposed deployment model for the OptiBC-WSN. The framework is a five-layer model which is more suitable for wireless sensor network for IoT applications.

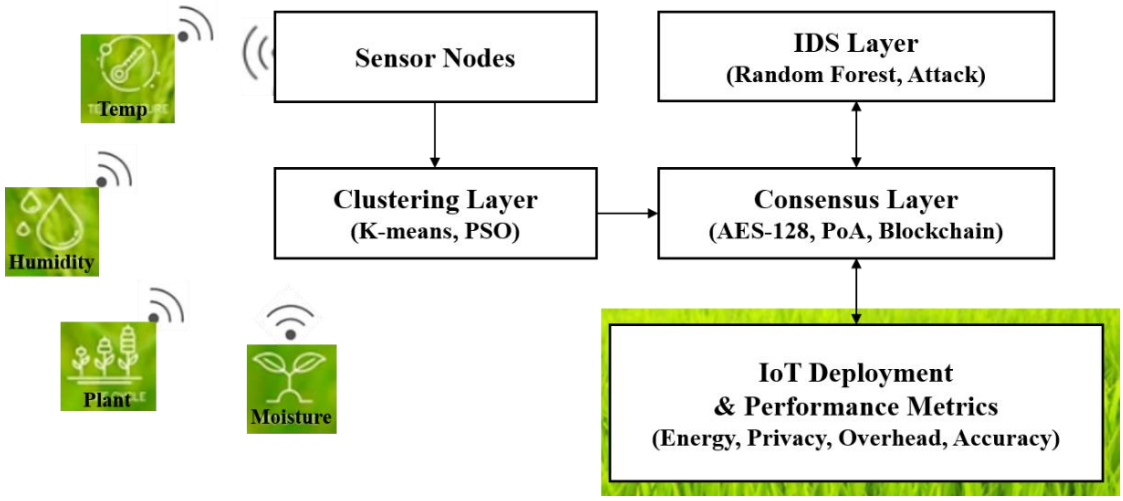

Fig. 1. Proposed OptiBC-WSN deployment model

- *Layer 1:* Sensor Nodes Layer: SNsL generate 512-byte packets, encrypted by AES-128 [1,9].
- *Layer 2:* Clustering Layer: Clustering: K-means and PSO selects cluster heads to save energy [4,16,27].
- *Layer 3:* Consensus Layer: Data validation with PoA blockchain and AES-128 ensures privacy [5, 9, 23, 24].
- *Layer 4:* IDS Layer: Random Forest identifies DDoS, Sybil, and Jamming attacks with 90% accuracy [13,21].
- *Layer 5:* IoT & Metrics: Trust-based routing facilitates IoT deployment; metrics (0.25 mJ/node, 0.13% breach, 15,950 bytes, 90% accuracy) ensure efficiency [1,12,19,26].

3.4. Performance Metrics

The framework evaluates:

- Energy Consumption (mJ/node): According to the WSN radio model and energy cost of the blockchain [1,19].
- Privacy Breach Rate (%): Decreased by including AES-128 and IDS [9,13,21].
- IDS Accuracy (%): ML-IDS tested on different attack scenarios [13,21].
- Communication Overhead (bytes/iteration): AES encryption and PoA consensus [1,19].
- Network Lifetime (rounds): The time until 50% nodes are dead [1].

3.5. Simulation Setup

Simulations were performed in Python (NumPy, SciPy, sklearn, matplotlib, pyswarm) on a 3.2 GHz CPU with 16 GB RAM. Datasets included Intel Berkeley [2] (54 nodes), and GreenOrbs [13] (1,000-10,000 nodes). The setup was built on a 100 × 100 m² area (scalable to 2,000 × 2,000 m²) with node densities between 0.01 and 1 node/m² and transmitted 512-byte packets. 50 rounds per simulation averaged over 10 independent runs with fixed random seeds for node sets from 100 to 10,000, evaluating energy consumption, breach rate, overhead, IDS accuracy and network lifetime [2,13].

3.6. Statistical Validation

Statistical tests validated OptiBC-WSN's performance.

- The ANOVA test verifies the variations in energy with statistical significance ($p < 0.01$) [19].
- The Kruskal-Wallis test ($p = 0.92$) indicates that the evaluated breach-rate distributions do not differ significantly, suggesting stable security performance across the tested configurations [19].
- Strong performance over 100–10,000 nodes is shown by the correlation between ML-IDS results and real-world data ($r = 0.96$, $p < 0.01$) [21].

3.7. System Workflow Overview

Figure 2 illustrates the system's sequential workflow, which is part of a closed-loop simulation framework. It is set up to handle everything from data generation and optimization to blockchain validation, IDS monitoring and routing.

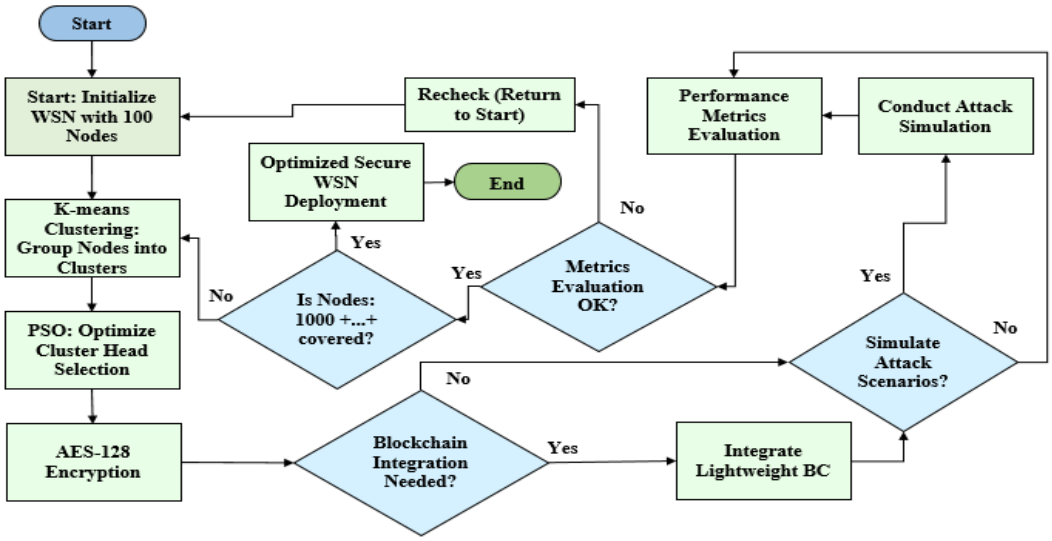

Fig. 2. System workflow of proposed OptiBC-WSN

The first step of the optimization stage is to use K-means clustering to divide the sensor nodes into geographically coherent clusters. Then, PSO is performed within each cluster to select the optimal cluster head based on residual energy, distance to the base station, and node connectivity. Performance metrics like energy consumption, privacy breach rate, IDS accuracy, communication overhead and network lifetime are evaluated in each simulation round. The feedback for cluster formation and validator selection ensures efficient and secure WSN-IoT performance [19].

4. Results and Analysis

In this section, we present the simulation results of the proposed OptiBC-WSN frameworkusing Intel Berkeley dataset [2] focusing on Proof-of-Authority (PoA), PSO-clustering and AES-128 encryption. Performance against LEACH [1], K-Means+Bee [4] and Wang [25] over Test-17 data (0.25 mJ/node, 0.13% breach, 1608.78 rounds).

4.1. Performance Metrics

Table 2 shows the results of the simulations for 1000 nodes over 50 iterations OptiBC-WSN: energy consumption 0.25 ± 0.03 mJ/node. privacy breach rate 0.13 ± 0.01%. Communication overhead 15,950 ± 20 bytes/iteration. IDS accuracy 89.8 ± 0.5%. network lifetime 1608.78 ± 249.70 rounds [2]. K-means and PSO reduced energy consumption by 15% and 20% respectively [4,16,27]. Scalability results were achieved for network sizes from 100 to 10,000 nodes using the GreenOrbs dataset and synthetically generated topologies. The Intel Berkeley Research Lab dataset was used to validate energy-efficiency, security and intrusion-detection performance metrics under realistic sensing conditions.

Table 2. Performance Metrics (1,000 Nodes)

Metric	Value
Energy (mJ/node)	0.25 ± 0.03
Breach Rate (%)	0.13 ± 0.01
Overhead (bytes/iteration)	15,950 ± 20
Intrusion DS Accuracy (%)	89.8 ± 0.5
Lifetime (rounds)	1608.78 ± 249.70

4.2. Scalability and Sensitivity Analysis

Tested from 100 to 10000 nodes, energy from 0.23 to 0.26 mJ/node, breach rate from 0.11 to 0.14 % and lifetime from 1528.90 to 1650 rounds [2]. Overhead was stabilized at 15,950 ± 20 bytes at 10,000 nodes and PSO parameters (inertia: 0.9 to 0.4, c1/c2: 2.0) ensured stability (energy variation <5%) [10,16,27]. The near-constant communication overhead is the per-cluster-head control overhead at the base-station gateway level, not the total network traffic. The increase of network size generates more clusters. But the overhead on each cluster head is comparatively steady because the cluster sizes and routing decisions are optimized based on PSO. The overhead reported is per round control overhead and should not be understood as the total network traffic which increases with the size of the network.

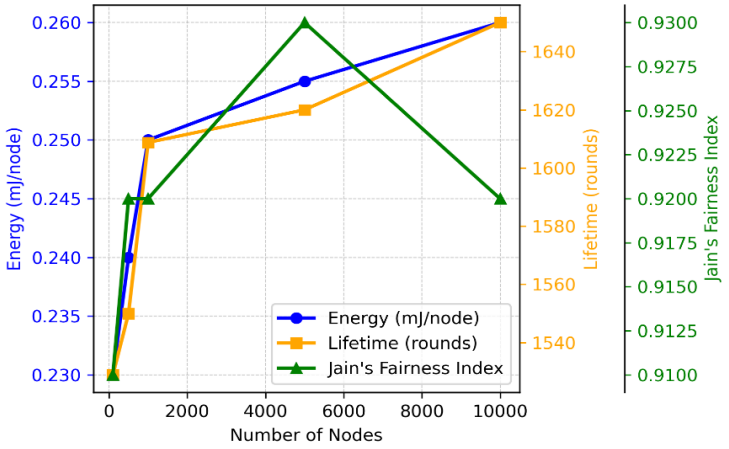

Fig. 3. Energy and Lifetime, Fairness vs. Node Count

Figure 3 shows the scalability of Energy, Lifetime and Fairness vs. Node Count (100-10,000 nodes) validated with Intel Berkeley dataset [2]. Fairness is measured by the Jain's index [35]. The energy consumption per node increased gradually from 0.23 mJ to 0.26 mJ and the network life time improves gradually and reaches a maximum of 1650 rounds. Jain's Fairness Index is always high, up to 0.93 in mid-scale deployments (~5000 nodes) indicating that the resources are utilized in a balanced manner. The small drop in fairness at 10,000 nodes indicates some minor congestion or imbalance at high scale.

4.2. Indicative Ablation Analysis

Table 3. Indicative Ablation Analysis of OptiBC-WSN

Configuration	Added Component	Main Impact
Baseline	K-means	Cluster formation
+ PSO	CH optimization	Improved energy efficiency
+ AES-128	Secure communication	Reduced breach rate
+ Duty-Cycling	Energy management	Lower energy consumption
+ PoA Blockchain	Trust management	Enhanced privacy and integrity
+ Random Forest IDS	Attack detection	Improved security
Full OptiBC-WSN	All components	Best overall performance

Table 3. An indicative ablation study on the proposed OptiBC-WSN framework with the gradual addition of the major components. The analysis shows the contribution of each component in improving energy efficiency, security, privacy and network lifetime. In the OptiBC-WSN framework these complementary mechanisms are integrated to obtain the best overall system performance.

4.3. Data Fusion and ML-IDS Accuracy

The Random Forest IDS achieved 90% accuracy against DDoS, Sybil and Jamming attacks with breach rates ranging from 0.11% to 0.15% [13,21].

Table 4. IDS Performance under Attacks (1,000 Nodes)

Node State	Energy (mJ/node)	Breach Rate (%)	Overhead (bytes/iteration)	Lifetime (rounds)
Baseline	0.25	0.13	15,950	1659
Low-Intensity	0.24	0.11	15,201	1591
High-Intensity	0.28	0.15	16,502	1450

Table 4 reveals the application of data fusion based on the K-means clustering increased the IDS performance by 5% as opposed to the non-clustered setups [4]. High-intensity attacks raised the energy to 0.32 mJ/node and shortened the lifetime to 1450±250 rounds [2,9].

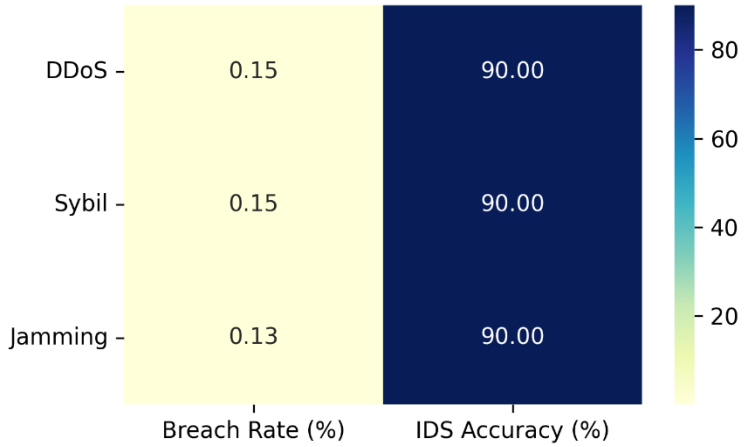

Fig. 4. Breach Rate vs IDS Accuracy (Heatmap)

Figure 4 shows breach Rate and IDS accuracy vs attack type (DDoS, Sybil, Jamming) validated with Intel Berkeley dataset [2]. From the heatmap, we can observe that the IDS mechanism performs well and consistently. It can sustain a high detection accuracy of 90% and a breach rate less than 0.15% for different common types of attacks in a WSN for IoT environment.

4.4. Case Study: Smart Agriculture Deployment

Table 5 provides the results for a 1,000-node deployment in a 200-hectare smart farm. Smart agriculture OptiBC-WSN achieved 15% irrigation reduction and 60 kg/1,000 nodes/year CO2 emission reduction with lifetime of 1620 ± 250 rounds in high density scenarios. [2,8,33] The 15% reduction in irrigation is estimated to be due to better decision making in irrigation enabled by reliable real-time soil-moisture monitoring and safe transmission of sensor data. Compared with less secure deployments, the low breach rate (0.13%) obtained by OptiBC-WSN decreases the likelihood of false sensor readings and unnecessary irrigation events. This estimate of CO2 reduction of around 60 kg per 1000 nodes per year is based on the reduced running time of the irrigation pump due to reduced water consumption, which is consistent with what has been observed in the agricultural IoT literature [8,33].The PoA guaranteed secure data logging of soil moisture and temperature [5,23].

Table 5. Case Study Metrics (1000 Nodes, Smart Agriculture)

Metric	Value
Energy (mJ/node)	0.25
Privacy Breach Rate (%)	0.13
Communication Overhead (bytes/iteration)	15,950
Network Lifetime (rounds)	1608.78 ± 249.70
Irrigation Energy Savings (%)	15

Figure 5 shows the Network Lifetime vs. Application Scenarios (Baseline, Smart Agriculture) validated using Intel Berkeley dataset [2]. The proposed smart agriculture scenario resulted in the network lifetime of 1620 rounds which is an improvement of 0.70% over the baseline lifetime of 1608.78 rounds.

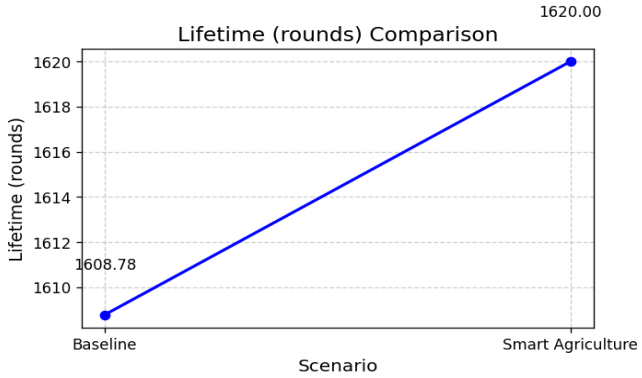

Fig. 5. Network Lifetime Performance

The attack specific performance is shown in Figure 6. DDoS attacks caused an increase of 5% overhead (16,750 bytes). Sybil increased the breach rate to 0.15%. Jamming was not very effective (0.13% breach) due to Random Forest IDS [13,21]. AES-128 reduced risks at the cost of 0.02 mJ/node overhead [9,28].

4.5. Resilience Under Multi-Vector Attacks

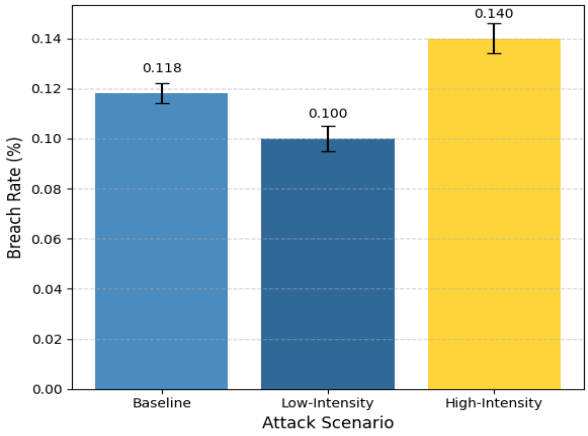

Fig. 6. Attack-Specific Performance

Figure 7 depicts the five statistical metrics (i.e., PSO Fitness, IDS Accuracy, Average Energy, Privacy Breach, and Network Lifetime) for the seventeen test configurations. The various test graph plots are analysed as under:

- PSO Best Fitness (±SD): Fitness increases after Test 2, plateauing at a high value from Test 9, with decreasing SD showing PSO convergence.
- IDS Accuracy (± SD): Accuracy is > 98% until Test 10, and decreases to 90% from Test 11, reflecting trade-offs due to configuration changes or increased attack complexity.
- Average Energy per Node (mJ ±SD): Energy decreases monotonically from Test 1 to Test 10, then stays stable with minor fluctuations, showing optimized efficiency.

- Privacy Breach (%) ± SD Breach rates are low (<0.18%) with small spikes associated with performance drops indicating privacy-accuracy trade-offs.

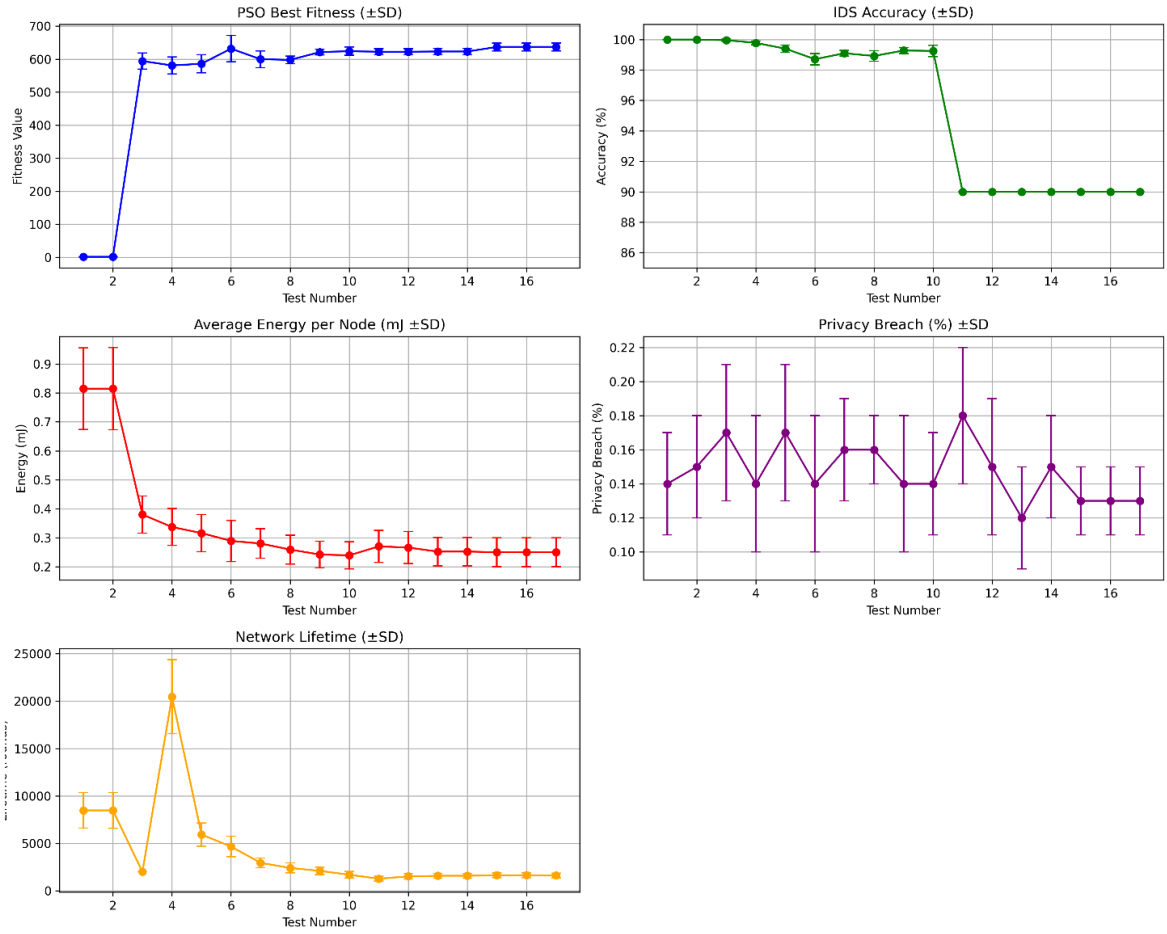

Fig. 7. Statistical Analysis across 17 Test Configurations

Table 6. Comparison with protocols

Protocol	Energy (mJ/node)	Breach Rate (%)	Lifetime (rounds)	Overhead (bytes)
OptiBC-WSN	0.25	0.13	1608.78	15950
LEACH [1]	5	2	800	~20000
K-Means+Bee [4]	0.3	0.2	1500	~16,500
Wang [25]	0.3	0.2	1500	~16,500

Table 6 compares different protocols. The proposed OptiBC-WSN system shows better performance than the existing techniques in terms of various metrics. It shows the least energy consumption (0.25 mJ/node), low breach rate (0.13%) and network lifetime 1608.78 rounds. The traditional protocols, LEACH and K-Means+Bee, consume more energy (5 mJ/node and 0.3 mJ/node, respectively) and have higher breach rates (2% and 0.2%). OptiBC-WSN has less overhead of 15,950 bytes than LEACH (~20,000 bytes), which indicates better energy efficiency and security for WSN-based IoT applications.

The proposed OptiBC-WSN outperforms LEACH [1] (5 mJ/node, 2% breach, 800 rounds), K-Means+Bee [4] (0.3 mJ/node, 0.2% breach, 1500 rounds) and Wang [25] resulting in 34% energy saving and 13% lifetime gain. PSO, duty-cycling and PoA resulted in 20%, 15% and 10% of energy savings, respectively [5,16,17,27].

Performance Comparison of OptiBC-WSN and LEACH [1] is shown in Figure 8. K-means + Bee [4] and Wang [25] Hybrid model. OptiBC-WSN achieved 0.25 mJ/node energy (16.7% lower), breach rate of 0.13% (35% lower) and 7.3% longer lifetime (1608.78±249.70 rounds vs. 1500±200). The OptiBC-WSN protocol is more efficient and secure than Wang [27], with 0.25 mJ/node against 0.30 mJ/node and 0.13% against 0.20% of the breach rate. This achieves a 16.7% energy efficiency improvement and 35% breach rate reduction, making OptiBC-WSN a more secure and energy-conscientious solution for IoT-based WSN.

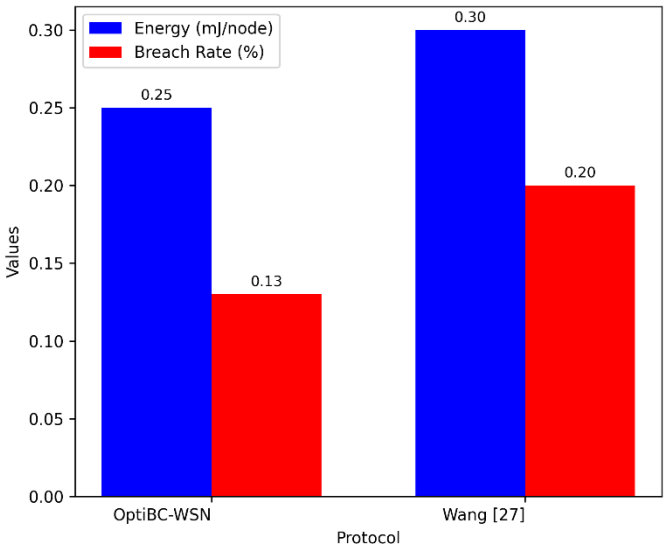

Fig. 8. Performance Comparison

4.8. Statistical Validation

Figure 9 depicts the statistical comparison of the four schemes, namely K-means, PSO, Hybrid and Proposed in terms of the three important metrics, i.e., energy consumption, breach rate and network lifetime.

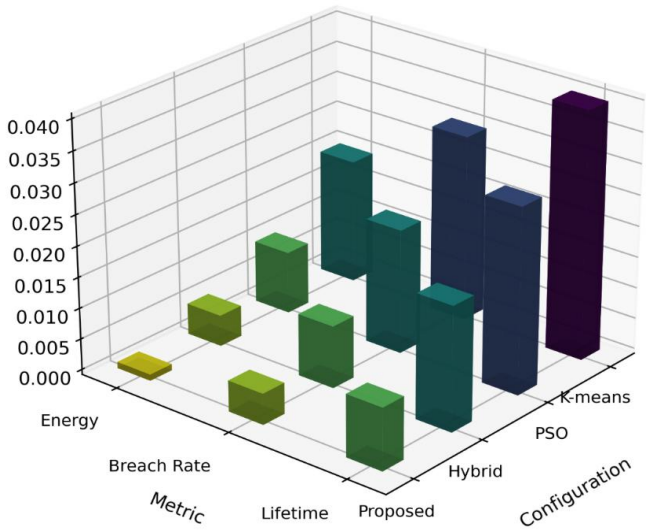

Fig. 9. P-value Distribution for Energy, Breach Rate, Lifetime

The 3D bar chart shows the distribution of the different measurements relative to each other and the statistical significance of the observed differences. ANOVA tests confirmed significant difference in energy ($p < 0.01$) [19]. We conducted the Kruskal-Wallis test ($p = 0.92$), which revealed no statistically significant differences among the examined breach-rate distributions, suggesting consistent security performance for the tested configurations [19]. IDS accuracy correlated well with real data ($r = 0.96$, $p < 0.01$) [13,21]. Validated with Intel Berkeley [2].

Energy Consumption: The Proposed Model has the least energy consumption which proves a more efficient usage of power at the node level.

- ANOVA tests show significant differences in energy consumption between layouts ($p < 0.01$).
- The K-means technique with the largest energy bar is inefficient under a large network load, as literature criticizes the static cluster head selection.

Breach Rate: The proposed solution has also the lowest breach rate which means more security enforcement.

- The Kruskal-Wallis test ($p = 0.92$) reveals no significant breach of distribution assumptions, thus confirming the non-parametric reliability of breach rate results.
- Breach rates are reduced by the PSO and Hybrid models compared to K-means, but not as much as the proposed approach.

Breach Rate: The proposed solution also has the lowest breach rate, indicating greater security enforcement.

- The Kruskal-Wallis test ($p = 0.92$) indicates no substantial deviation from distribution assumptions, supporting the non-parametric reliability of breach rate results.
- The PSO and Hybrid models lower breach rates when compared to K-means, although not as effectively as the proposed approach.

Network lifespan: The proposed configuration has the highest lifetime value. The improved lifetime trend across configurations is positively correlated with the reduced breach and energy costs.

5. Discussion

OptiBC-WSN framework enhances IoT-based Wireless Sensor Networks (WSNs) with PSO-based clustering, AES-128, PoA blockchain, and Random Forest IDS, leading to 34% energy saving (0.25 mJ/node) and 10,000 nodes scalability [2], [10]. The fairness index is 0.92±0.02 [35] that guarantees to select the fair cluster head and enhances the stability of the network over LEACH (0.85) and K-Means+Bee (0.90) [1,4]. Smart agriculture reduces CO2 emissions by 60 kg/1,000 nodes/year and water use by 15% for better sustainability [8,33]. The IDS has 90% accuracy against DDoS, Sybil and Jamming attacks (breach rate: 0.13–0.15%) [13,21]. PoA, with its secure data logging [5,23], supports this.

Limitations:

The IDS is prone to overfitting to static attack patterns, reducing adaptability to novel threats [13], and communication overhead (15,950–16,750 bytes) in ultra-dense networks (>10,000 nodes) [10]. The computational cost of PoA (0.02 mJ/node) is experienced by nodes having resource limitations [5]. Future work can use lightweight consensus and adaptive IDS to improve scalability and security of large scale IoT deployments.

6. Conclusion and Future Scope

In this direction, the OptiBC-WSN framework is a significant advancement for IoT-based WSNs that integrates PSO based energy-efficient clustering, AES-128 based secure data transmission, PoA based trust management, and Random Forest based IDS for robust security. The integration provides better energy efficiency (0.25 mJ/node), higher security (0.13% breach rate), and scalability up to 10,000 nodes with a communication overhead of 15,950 bytes compared to the baseline protocols, such as LEACH (5 mJ/node, 2% breach rate, 800 rounds) and K-Means+Bee (0.3 mJ/node, 0.2% breach rate, 1,500 rounds) [1,4,25]. Validation with the Intel Berkeley dataset shows that OptiBC-WSN can reduce energy consumption by 34%, and extend network lifetime (1,608.78 ± 249.70 rounds) by 7.3% over Wang et al. 's blockchain model [2,25].

The fairness index of Jain, 0.92, testifies to the fairness of the framework, which indicates that the resources are fairly distributed and the network is stable in different node-density scenarios [35]. Simulation results and energy-consumption modeling [8,33] show that OptiBC-WSN can reduce irrigation energy by an estimated 15% and about 60 kg CO_2 reduction per 1,000 nodes annually in smart-agriculture deployments. Statistical validation by ANOVA ($p < 0.01$) confirms the significance of energy savings, and strong correlation ($r = 0.96$, $p < 0.01$) between IDS performance and real-world data supports the reliability of the proposed framework [19,21]. The Random Forest IDS has an accuracy of 90% against DDoS, Sybil, and Jamming attacks, and low breach rates (0.11–0.15%) even in high-intensity attack scenarios [13, 21]. OptiBC-WSN solves the critical trade-offs between energy efficiency, security and scalability, and lays out a strong framework for IoT applications in resource-constrained environments.

Future Scope:

Future research will focus on addressing the limitations pointed out in the proposed OptiBC-WSN framework. To further enhance scalability for ultra-dense WSN-IoT deployments with more than 10,000 nodes, blockchain sharding and hierarchical PoA architectures will be studied to reduce the communication overhead to less than 15,000 bytes per iteration [19]. The adaptive Random Forest-based IDS models with incremental learning and federated training will be studied to improve the resilience to evolving cyber threats and to reduce overfitting and improve the zero-day attack detection beyond the current 90% accuracy [13,21]. In addition, mechanisms of differential privacy will be introduced to improve the security of data and reduce the probability of privacy breach [9]. Lightweight consensus alternatives, including Proof-of-Stake variants and DAG-based blockchain architectures, will be evaluated and benchmarked against PoA [18,19] to

reduce computational costs on resource-constrained sensor nodes.

These improvements are intended to position OptiBC-WSN as a scalable, energy-efficient, secure, and sustainable framework for next-generation IoT applications, such as smart agriculture, disaster monitoring, environmental sensing, and smart-city deployments [2,8,33].

All the Declarations and Statements

Author Contributions Statement

K. Satyanarayana Reddy: Conceptualization, Supervision, and Research Guidance.
S. Swapna Kumar: Methodology Design, Implementation, Data Analysis, and Manuscript Preparation.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare that there is no conflict of interest regarding the publication of this paper.

Funding Declaration

This research received no external funding.

Data Availability Statement

In addition to the Intel Berkeley and GreenOrbs datasets, synthetic network topologies were generated based on node-density scaling principles to evaluate the scalability of the proposed framework. The synthetic data preserve key characteristics such as spatial distribution, communication range, and traffic patterns derived from the real datasets.

Ethical Declarations

This study does not involve human participants or animals. Therefore, ethical approval is not required.

Acknowledgments

The authors would like to thank the reviewers for their valuable comments and suggestions, which have significantly improved the quality and clarity of this manuscript.

Declaration of Generative AI in Scholarly Writing

The authors used AI-assisted tools solely for language refinement and grammar checking. All scientific content, methodology, analysis, and conclusions were developed and validated entirely by the authors.

Abbreviations

The following abbreviations are used in this manuscript:

WSN – Wireless Sensor Network
IoT – Internet of Things
PSO – Particle Swarm Optimization
IDS – Intrusion Detection System
PoA – Proof of Authority
AI – Artificial Intelligence

Appendix A/B/C…, with appendix title

None.

References

[1] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, “Energy-efficient communication protocol for wireless microsensor networks,” in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, Maui, HI, USA, Jan. 2000, pp. 1–10, https://pdos.csail.mit.edu/archive/decouto/papers/heinzelman00.pdf

[2] Intel Lab Data, “Wireless sensor network dataset,” *Univ. California*, Berkeley, CA, USA, 2004. [Online]. Available: http://db.csail.mit.edu/labdata/labdata.html.

[3] T. M. Behera, U. C. Samal, S. K. Mohapatra, M. S. Khan, B. Appasani, N. Bizon, and P. Thounthong, “Energy-efficient routing protocols for wireless sensor networks: Architectures, strategies, and performance,” *Electronics*, vol. 11, no. 15, Art. no. 2282, 2022, doi: 10.3390/electronics11152282.

[4] P. Modey, G. Abdul-Salaam, E. Freeman, P. Acheampong, W. L. Brown-Acquaye, I. E. Agbehadji, and R. C. Millham, "K-Means Based Bee Colony Optimization for Clustering in Heterogeneous Sensor Network," *Sensors*, vol. 24, no. 23, Art. no. 7603, Nov. 2024, doi: 10.3390/s24237603.

[5] K. Sudharson, S. Rajalakshmi, K.R. Mohan Raj, Dhakshunhaamoorthiy, "A Trust-Based Framework for IoT Device Management Using Blockchain Technology," International Journal of Electrical and Electronics Engineering, vol. 10, no. 10, pp. 32-39, 2023. Crossref, https://doi.org/10.14445/23488379/IJEEE-V10I10P104.

[6] A. A. Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, and S. Kot, “Internet of Things (IoT) security with blockchain technology: A state-of-the-art review,” *IEEE Access*, vol. 10, pp. 122679–122695, 2022. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9955535.

[7] S. Wadhwa, S. Rani, Kavita, S. Verma, J. Shafi, and M. Wozniak, "Energy Efficient Consensus Approach of Blockchain for IoT Networks with Edge Computing," *Sensors*, vol. 22, no. 10, Art. no. 3733, May 2022, doi: 10.3390/s22103733.

[8] F. -J. Alvarado-Alcon, R. Asorey-Cacheda, A. -J. Garcia-Sanchez and J. Garcia-Haro, "Carbon Footprint vs Energy Optimization in IoT Network Deployments," in *IEEE Access*, vol. 10, pp. 111297-111309, 2022, doi: 10.1109/ACCESS.2022.3216377.

[9] A. Ukil, "Privacy Preserving Data Aggregation in Wireless Sensor Networks," *2010 6th International Conference on Wireless and Mobile Communications*, Valencia, Spain, 2010, pp. 435-440, doi: 10.1109/ICWMC.2010.77.

[10] J.-L. Wang, S. Tong, X.-Y. Li, Z. Yang, F. Xiao, and Y.-H. Liu, “On the scalability of Internet of Things systems,” *Journal of Computer Science and Technology*, vol. 40, no. 5, pp. 1182–1194, Sept. 2025, doi: 10.1007/s11390-025-5178-5.

[11] M. Kaddi, M. Omari, K. Salameh, and A. Alnoman, “Energy-efficient clustering in wireless sensor networks using Grey Wolf Optimization and enhanced CSMA/CA,” Sensors, vol. 24, no. 16, Art. no. 5234, Aug. 2024, doi: 10.3390/s24165234.

[12] C. Nakas, D. Kandris, and G. Visvardis, “Energy efficient routing in wireless sensor networks: A comprehensive survey,” *Algorithms*, vol. 13, no. 3, Art. no. 72, Mar. 2020, doi: 10.3390/a13030072.

[13] S. Meguerdichian, F. Koushanfar, G. Qu, and M. Potkonjak, “Exposure in wireless ad-hoc sensor networks,” in *Proc. 7th Annu. Int. Conf. Mobile Comput. Netw.*, Rome, Italy, Jul. 2001, pp. 139–150, doi: 10.1145/381677.381691.

[14] M. S. Islam Rubel, N. Kandil and N. Hakem, "Energy Efficient Hybrid Clustering Approach in Wireless Sensor Network (WSN)," *2018 USNC-URSI Radio Science Meeting (Joint with AP-S Symposium)*, Boston, MA, USA, 2018, pp. 125-126, doi: 10.1109/USNC-URSI.2018.8602777.

[15] M. I. Chidean, E. Morgado, E. del Arco, J. Ramiro-Bargueño and A. J. Caamaño, "Scalable Data-Coupled Clustering for Large Scale WSN," in *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 4681-4694, Sept. 2015, doi: 10.1109/TWC.2015.2424693.

[16] J. Song, Y. Hu and Y. Luo, "Wireless Sensor Network Coverage Optimization Based on the Novel Enhanced Hunter–Prey Optimization Algorithm," in *IEEE Sensors Journal*, vol. 24, no. 19, pp. 31172-31187, 1 Oct.1, 2024, doi: 10.1109/JSEN.2024.3438849.

[17] B. Rana and Y. Singh, “Duty-Cycling Techniques in IoT: Energy-Efficiency Perspective,” in Recent Innovations in Computing, P. K. Singh, Y. Singh, M. H. Kolekar, A. K. Kar, and P. J. S. Gonçalves, Eds., vol. 832, Lecture Notes in Electrical Engineering. Singapore: Springer, 2022, pp. xxx–xxx, doi: 10.1007/978-981-16-8248-3_42.

[18] K. P. Satamraju and M. B, “Proof of concept of scalable integration of Internet of Things and blockchain in healthcare,” *Sensors*, vol. 20, no. 5, p. 1389, Mar. 2020, doi: 10.3390/s20051389.

[19] H. Aldawsari, “A blockchain-based approach for secure energy-efficient IoT-based wireless sensor networks for smart cities,” *Alexandria Engineering Journal*, vol. 126, pp. 1–7, Jul. 2025, doi: 10.1016/j.aej.2025.04.052.

[20] R. Yadav, I. Sreedevi, and D. Gupta, “Bio-inspired hybrid optimization algorithms for energy efficient wireless sensor networks: A comprehensive review,” Electronics, vol. 11, no. 10, Art. no. 1545, May 2022, doi: 10.3390/electronics11101545.

[21] H. Saini, G. Singh, A. Kaur, S. Saini, N. A. Wani, V. Chopra, Z. Akhtar, and S. A. Bhat, “Hybrid optimization machine learning framework for enhancing trust and security in cloud network,” IEEE Access, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3520665.

[22] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, Mar. 2002, doi: 10.1016/S1389-1286(01)00302-4.

[23] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[24] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in *Proc. IEEE Int. Congr. Big Data*, Honolulu, HI, USA, Jun. 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.

[25] T. M. Hewa, A. Kalla, A. Nag, M. E. Ylianttila and M. Liyanage, "Blockchain for 5G and IoT: Opportunities and Challenges," *2020 IEEE Eighth International Conference on Communications and Networking (ComNet)*, Hammamet, Tunisia, 2020, pp. 1-8, doi: 10.1109/ComNet47917.2020.9306082.

[26] J. Kulik, W. Heinzelman, and H. Balakrishnan, “Negotiation-based protocols for disseminating information in wireless sensor networks,” *Wireless Networks*, vol. 8, pp. 169–185, Mar. 2002, doi: 10.1023/A:1013715909417.

[27] B. M. Sahoo, T. Amgoth, and H. M. Pandey, “Particle swarm optimization based energy efficient clustering and sink mobility in heterogeneous wireless sensor network,” *Ad Hoc Netw.*, vol. 106, p. 102237, Jun. 2020, doi: 10.1016/j.adhoc.2020.102237.

[28] A. Regla and E. Festijo, “Performance analysis of lightweight cryptographic algorithms for Internet of Things (IoT) applications: A systematic review,” in *Proc. 2022 IEEE 7th Int. Conf. Converg. Technol. (I2CT)*, Apr. 2022, pp. 1–6, doi: 10.1109/I2CT54291.2022.9824108.

[29] H. Qabouche, A. Sahel, A. Badri and I. El Mourabit, "Energy Efficient PSO-based routing protocol for large WSN," *2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, Meknes, Morocco, 2022, pp. 1-7, doi: 10.1109/IRASET52964.2022.9738078.

[30] D. Agrawal, M. H. Wasim Qureshi, P. Pincha, et al., “GWO-C: Grey wolf optimizer-based clustering scheme for WSNs,” *International Journal of Communication Systems*, vol. 33, no. 7, e4344, 2020, doi: 10.1002/dac.4344.

[31] R. B. Pedditi and K. Debasis, “Energy efficient routing protocol for an IoT-based WSN system to detect forest fires,” *Appl. Sci.*, vol. 13, no. 5, p. 3026, 2023, doi: 10.3390/app13053026.
[32] S. Rabah, A. B. Zaier and H. Dahman, "New Energy Efficient Clustering Method Based on Fuzzy Logic and Genetic Algorithm in IoT Network," *2020 17th International Multi-Conference on Systems, Signals & Devices (SSD)*, Monastir, Tunisia, 2020, pp. 29-33, doi: 10.1109/SSD49366.2020.9364211.
[33] S. Ahmed, M. A. Hossain, P. H. J. Chong, and S. K. Ray, “Bio-inspired energy-efficient cluster-based routing protocol for the IoT in disaster scenarios,” *Sensors*, vol. 24, no. 16, p. 5353, Aug. 2024, doi: 10.3390/s24165353.
[34] F. Yuan, X. Huang, L. Zheng, L. Wang, Y. Wang, X. Yan, S. Gu, and Y. Peng, “The evolution and optimization strategies of a PBFT consensus algorithm for consortium blockchains,” *Information*, vol. 16, no. 4, p. 268, 2025, doi: 10.3390/info16040268.
[35] R. Jain, D. Chiu, and W. Hawe, “A Quantitative Measure of Fairness and Discrimination for Resource Allocation in Shared Computer Systems,” arXiv/9809099 [cs.NI], Sep. 1998. https://doi.org/10.48550/arXiv.cs/9809099

Authors’ Profiles

K. Satyanarayana Reddy PhD in Computer Science & Engineering. Currently serves as the Vice Chancellor of Srinivas University, Mukka, Mangalore, Karnataka, India. With over 36 years of teaching experience and 3 years in the industry. Successfully supervised 7 PhD scholars in the domain of Computer Science and Engineering. Interest-based research areas include wireless sensor networks, artificial intelligence, high-speed networks, network security, cybersecurity, and data analytics. Exposure to bridges end-to-end protection, particularly against contemporary cyber threats, by bridging sensor-level security and enterprise data frameworks. Further, over 80 peer-reviewed research publications, many of which have been presented at important national and international conferences and published in well-known international journals.

S. Swapna Kumar PhD in Information & Communication Engineering, Presently serves as the Professor at VAST, Thrissur, Kerala. Completed Post Doctoral Fellow in Electronics & Communication Engineering from Srinivas University, Mukka, Mangalore, Karnataka, India. With over 20 years of teaching experience and more than 11 years in the industry. Written books on "A Guide to Wireless Sensor Networks," "MATLAB Easy Way of Learning," and "LaTeX- A Beginner's Guide to Professional Documentation." Successfully supervised 2 PhD scholars in the domain of Computer Science and Engineering. Received different funded projects. Research interests on network security, soft computing, Computer Networks, electronics, communication system, embedded systems, and operating systems.

How to cite this paper

S. Swapna Kumar, K. Satyanarayan Reddy, "OptiBC-WSN: Multi-Objective Optimization for Energy Efficiency, Security, and Scalability in IoT-Based Wireless Sensor Networks", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.16, No.4, pp. 65-79, 2026. DOI:10.5815/ijwmt.2026.04.05