IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 2, April 2026, pp. 1275~1285
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i2.pp1275-1285

Energy-efficient and secure WSN clustering for IoT using particle swarm optimization and advanced encryption standard

S. Swapna Kumar[1,2], Kalli Satyanarayan Reddy[3]
[1]Department of Electronics and Communication Engineering, Srinivas University, Mangalore, India
[2]Department of Electronics and Communication Engineering, Vidya Academy of Science and Technology, Thalakkottukara, India
[3]Srinivas University, Mangalore, India

Article Info

Article history:

Received Sep 16, 2025
Revised Jan 6, 2026
Accepted Jan 22, 2026

Keywords:

AES-128
Internet of things
Secure data
Swarm optimization
Wireless sensor networks

ABSTRACT

Wireless sensor networks (WSNs) are made up of distributed sensor nodes that work together under energy and communication constraints. They support diverse internet of things (IoT) applications such as smart agriculture and environmental monitoring. This paper proposes a technique to optimize the WSN framework for secure and energy-efficient data transmission. To improve cluster formation and network energy consumption, the suggested model combines k-means clustering with particle swarm optimization (PSO). Inter-cluster data is encrypted by the cluster head (CH) using the advanced encryption standard (AES)-128. To protect data and save energy, the low-energy adaptive clustering hierarchy (LEACH) protocol uses a number of techniques. Energy efficiency, model accuracy, likelihood of privacy breaches, and network longevity are examples of performance metrics. The system is tested by Python simulations on the Intel Berkeley Research Lab (IBRL) real-world dataset, which includes 54 sensor nodes measuring temperature and humidity. The results demonstrate significant energy savings and a model accuracy of 96.50%, thereby reducing privacy breaches and extending network lifetime. The framework offers scalability, effective privacy monitoring, and adaptability to changing topologies.

Corresponding Author:

S. Swapna Kumar
Department of Electronics and Communication Engineering, Srinivas University
Mukka, Surathkal, Mangalore, Karnataka, India
Email: swapnakumar.s@vidyaacademy.ac.in

1. INTRODUCTION

Wireless sensor networks (WSN) are ad-hoc networks that support many modern smart applications like industrial automation, agriculture, healthcare, and smart cities [1]–[3]. A WSN consists of numerous tiny sensor nodes that gather information, aggregate it, and transmit it to a base station. These sensor nodes have low energy and computing capability. As a result, WSNs are faced with issues like high energy usage, insecure data transmission, communication overhead, and scalability, which lower the overall system performance [4], [5].

The main objectives of WSN design are to reduce energy usage, extend network lifetime, protect the transmitted data, and maintain reliable operation in various node densities and potential attack conditions. The following are the contributions of this research: i) development of an optimized clustering framework incorporating distance-based clustering, swarm intelligence, and duty cycling in order to minimize energy consumption; ii) incorporation of lightweight encryption at the cluster head (CH) level to increase security against common adversarial attacks; and iii) empirical validation of the framework using simulations with up to 10,000 nodes and real-world sensor data, along with statistical evaluation against known benchmarks. This

work addresses the gap between the scalability of theory and the deployment of practice. It is energy-efficient and secure architecture for next-generation sensor networks.

The rest of the paper is organized as follows. Section 2 presents a literature study. Section 3 discusses the methodology. Section 4 presents results and discussion. Lastly, section 5 contains conclusion.

2. RELATED WORK

Conventional clustering algorithms, especially the low-energy adaptive clustering hierarchy (LEACH), are usually applied to node energy management [6]. However, these protocols typically employ probabilistic CH selection and assume homogenous nodes, which leads to unequal energy consumption [7], [8]. Clustering efficiency is further limited by the fact that modern installations typically contain the levels of energy of mobile base stations and heterogeneous nodes [9], [10].

Recent research is aimed at approaches that maximize clustering, minimize energy consumption, and secure inter-cluster communication [11]–[15]. To fill this gap, a scalable framework using a combination of clustering optimization, swarm-based search, and lightweight encryption is proposed in the current study. Zhang and Li [15] examine the energy consumption of WSNs using a duty-cycle model, in which nodes switch between active and sleep modes in order to save energy. A machine learning-based intrusion detection system (IDS) for WSNs was proposed by Sadia *et al.* [16], which utilizes data-driven methods to detect and eliminate the threat instantly. Haseeb *et al.* [17] present a heuristic routing system that considers the energy efficiency and security requirements. Yadav *et al.* [18] give a detailed review of hybrid optimization algorithms, such as genetic algorithms and swarm intelligence techniques, to achieve energy efficiency in WSNs. Masoud *et al.* [19] discuss the tradeoffs of clustering and non-clustering strategies in their study and propose a hybrid clustering protocol for WSNs.

Goud *et al.* [20] presented adaptive routing strategies for an arbitrary WSN to optimize energy consumption and network performance. Bala and Behal [21] solved the problem of distributed denial of service (DDoS) attacks and WSN-based DDoS defense in internet of things (IoT) networks in the context of external attack response rather than internal data security during regular data transmissions. Conversely, Ahmed *et al.* [22] employed bioenergy optimization for node behavior prediction but did not emphasize cluster-based architectures. Brajones *et al.* [23] investigate the detection and mitigation of denial of service (DoS) and DDoS attacks in IoT-based stateful software-defined networking (SDN) environments.

Modey *et al.* [24] propose a clustering approach that combines k-means clustering with bee colony optimization for heterogeneous WSNs. Bao [25] proposes a secure clustering strategy for IoT using an improved particle swarm optimization (PSO) algorithm to enhance energy efficiency and security, while Wang *et al.* [26] develop a PSO based routing schema for heterogeneous WSNs to optimize energy consumption, and Sharmin *et al.* [27] present a hybrid PSO-based data aggregation on clustering algorithm for energy-efficient WSNs.

These studies collectively highlight advances in clustering optimization and network security. However, most focus on either energy efficiency or security individually. To address this gap, the present work integrates swarm-intelligence-based optimization and lightweight advanced encryption standard (AES)-based encryption to achieve both energy efficiency and secure communication within IoT-enabled WSNs.

3. METHOD

The proposed framework enhances the performance of WSN by integrating clustering optimization, swarm intelligence, lightweight encryption, and duty cycling into the LEACH protocol. The proposed framework is illustrated in Figure 1. It operates in three key stages: optimized clustering, secure communication, and duty-cycled transmission.

3.1. System model

The simulation models energy-constrained sensor nodes distributed in 100×100 m^2 area, supporting both homogeneous and heterogeneous energy configurations. A base station is placed at coordinates (150, 50) [6]. The first-order radio model defines energy dissipation for transmission (E_{Tx}) and reception (E_{Rx}) as given in (1) and (2), followed by the duty-cycling energy reduction in (3).

Sensor nodes (SN) are randomly deployed in a 100×100 m^2 field with a fixed base station, following standard WSN models [6], [7]. Each node is initialized with an energy of 2 J and follows a duty cycle of 50% [8]. The first-order radio model [1] is used for the transmission and reception of energy.

$$E_{tx(k,d)} = E_{elec} + \varepsilon_{amp} \times k \times d^2 \quad (1)$$

$$E_{rx(k)} = E_{elec} \times k \quad (2)$$

$$E_{total} = E_{elec} \times (1 - DUTY\_CYCLE\_RATE) + E_{sleep} \quad (3)$$

Where k is the packet size, d the distance, $E_{elec} = 50$ nJ/bit, and $E_{amp} = 100$ pJ/bit/m^2. In heterogeneous scenarios, a fraction m of nodes have energy $E_{adv} = (1 + \alpha)E_0$, as suggested in heterogeneous WSN models [10]. $\{DUTY\_CYCLE\_RATE\} = 0.5$ and $E_{sleep} \approx 0$ (negligible energy in sleep mode). By applying PSO-based clustering, the distance d between cluster members and heads is minimized, thus reducing E_{tx} the overall network energy consumption.

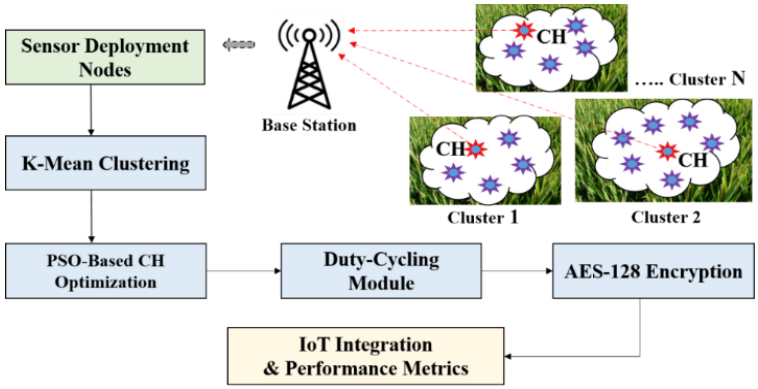

Figure 1. Proposed WSN deployment optimization model

3.2. Secure communication

AES-128 encryption is widely adopted in resource-constrained sensor networks due to its lightweight operations and robustness [14], [15]. In this framework, AES is performed at CHs to secure aggregated payloads. The encryption overhead is approximately 0.02 mJ per node and adds 16 bytes per packet, which is negligible compared to radio transmission energy [16]. The system protects against eavesdropping, injection, and node compromise [17].

3.3. Work flow

The overall system workflow is summarized in Figure 2 and consists of six steps.

i) Deployment of nodes and initialization of energy values.
ii) Formation of clusters via K-means.
iii) Refinement of CHs using PSO iterations.
iv) Aggregation and AES-128 encryption at CHs.
v) Encrypted data is transmitted to the base station with time division multiple access (TDMA) scheduling.
vi) Duty cycling to reduce idle energy consumption.

3.4. Simulation setup

The proposed WSN optimization framework was implemented in Python and evaluated under varying node densities. Sensor nodes are randomly placed in a 100×100 m^2 area, base station at (50, 50), with 0.5 J for normal and 1 J for 10 % advanced nodes. The packet size of 4,096 bits was selected as a balanced configuration between radio cost and data fidelity, following [1]. The first-order radio model uses $E_{elec} = 12$ nJ/bit and $E_{amp} = 0.0013$ pJ/bit/m^2; each simulation ran 1,500 rounds, averaged over five runs for reliability.

3.5. Dataset

To ensure a realistic evaluation, the Intel Berkeley Research Lab (IBRL) dataset [2] was used. It contains 54 deployed nodes was used for validating the statistical behavior of temperature- and humidity-based sensor readings. Large-scale simulations (up to 10,000 nodes) were synthetically generated using the same node-density and radio-energy parameters, so that consistent scaling can be used without changing physical characteristics. These traces were incorporated into the simulation environment to model the real-world behavior and variability of the sensors. The workflow in Figure 2 is the complete visual

representation of the simulation environment and methodology, and allows for complete reproducibility of the experimental setup.

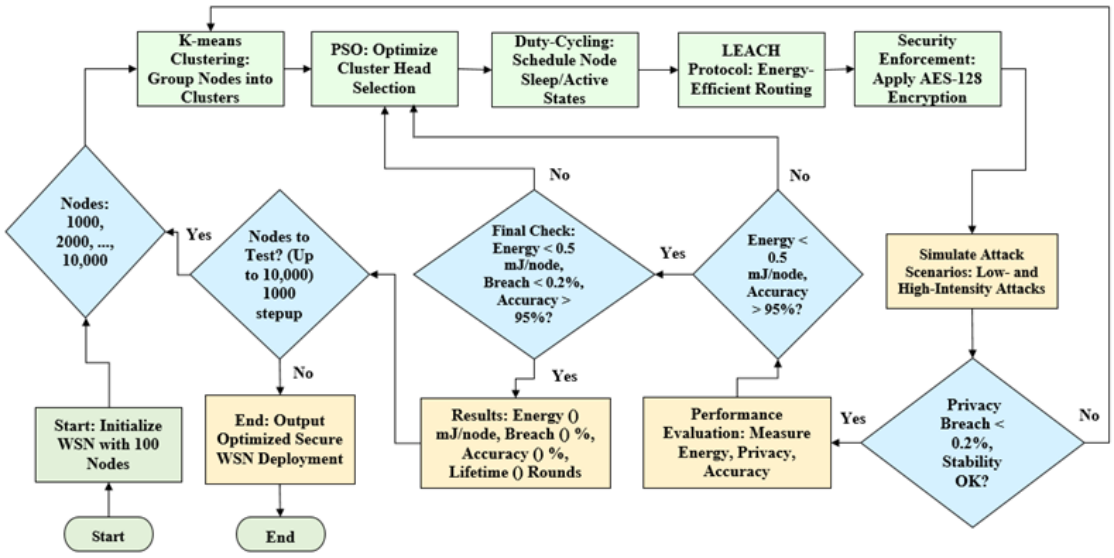

Figure 2. System and simulation workflow of the proposed WSN

3.6. Performance metrics

The simulation study evaluates the framework using the following performance metrics [2], [7].

i) Energy consumption (mJ/node)*:* compute average energy/node for data transmission and reception, (1) to (3) [1], [5].
ii) Network lifetime (rounds): number of iteration rounds until the first and last node dies [5], [6].
iii) Privacy breach rate (% unauthorized accesses): measures the percentage of data breaches with AES-128 encryption applied to mitigate unauthorized access [7].
iv) Communication overhead (bytes/iteration): measures total data transmitted as an indicator of efficient data aggregation [6].
v) Prediction accuracy (%): assesses soil moisture prediction accuracy under 0.5% input noise [4], [8]. In this study, model accuracy denotes the data-aggregation accuracy of sensor readings received at the base station. It measures how closely the aggregated (received) data match the original sensor values and is computed as (4).

$$Accuracy = \left(1 - \frac{S_{actual} - S_{received}}{S_{actual}}\right) \times 100\% \quad (4)$$

The baseline is the standard LEACH protocol without PSO or AES. This metric reflects information-fidelity during aggregation and transmission, not intrusion-detection or soil-moisture prediction.

3.7. Parameter setting

Table 1 summarizes the simulation parameters used in the proposed model. They specify the network field, node energy, packet size, and communication range. These standard settings enable comparison with existing WSN protocols.

Table 1. Simulation summary parameter used in Python experiments

Parameter	Value
Field size	100×100 m²
Base station	(50, 50)
Node energy	0.5 J (normal), 1 J (advanced)
Packet size	4,096 bits
Simulation rounds	1,500

3.8. Particle swarm optimization implementation details

To ensure reproducibility, the PSO used for CH refinement is described in Algorithm 1. PSO searches for CH positions that minimize a multi-objective fitness combining network energy, intra-cluster distance, and node survivability. Fitness weights and stopping: α, β, γ were set to 0.5, 0.3, and 0.2, respectively. Convergence tolerance used: Δfitness <1 e-4 or MaxIter.

Algorithm 1. PSO-based CH optimization
Input: N, Loc_i (node coordinates), E_i (initial energy), K (clusters), MaxIter
Output: CH set and cluster assignments
1: Initialize P particles; each particle encodes K CH coordinates (x,y)
2: For each particle p: compute fitness as in (5)

$$f_p = \alpha \cdot \left(\frac{1}{E_{total}}\right) + \beta \cdot \left(\frac{D_{avg}}{D_{ref}}\right) + \gamma \cdot \left(\frac{1}{1+N_{dead}}\right) \quad (5)$$

Where E_{total} is sum residual energy, D_{avg} is average intra-cluster distance, N_{dead} is number of dead nodes in trial
3: Update velocity and position:

$$v \leftarrow w \cdot v + c1 \cdot r1 \cdot (p_{best} - x) + c2 \cdot r2 \cdot (g_{best} - x)$$
$$x \leftarrow x + v$$

4: Enforce field bounds; reassess fitness; update p_{best}, g_{best}
5: Repeat (2–4) until MaxIter or convergence
6: Assign nodes to nearest CH (Euclidean); run TDMA+aggregation+AES at CHs

Table 2 presents the PSO parameter settings used for CH optimization in the Python simulation, as summarized in the PSO parameter table. These parameters control swarm behavior, including exploration, exploitation, and convergence speed during the optimization process. Proper selection of these values ensures stable convergence and reproducible clustering performance across different network sizes. The selected settings provide stable swarm convergence and balanced search behavior. Inertia weight and acceleration constant were adjusted to minimize clustering error.

Table 2. PSO parameter settings used for CH optimization

Parameter	Symbol	Value (used)	Note
Swarm size	P	30	Balanced exploration vs. CPU load
Max iterations	MaxIter	100	Converges <80 for N ≤2000
Inertia weight (linear dec.)	w	0.90→0.40	Starts exploration→exploitation
Cognitive coefficient	c_1	1.5	Personal best attraction
Social coefficient	c_2	1.5	Global best attraction
CH ratio	ρ	0.05	≈5% nodes as CH (LEACH-like)
Runs per point	—	5 independent runs	Report mean ± SD
Field size	—	100×100 m²	Consistent with section 2.4

3.9. AES-128 encryption and energy overhead modeling

Secure data aggregation within each cluster is implemented using the AES-128 library in Python (Crypto.Cipher) in Algorithm 2. The cipher is used in generate counter (CTR) mode for in-network encryption, and CBC mode for end-to-end integrity. Each CH encrypts fused data before sending it to the base station.

Algorithm 2. AES-128 encryption at CH
Input: aggregated_data, AES_key(16 bytes), counter
Output: encrypted_payload
1: Generate counter = Counter.new(128, initial_value = round_ID)
2: Cipher ← AES.new(AES_key, AES.MODE_CTR, counter = CTR)
3: ciphertext ← Cipher.encrypt(aggregated_data)
4: Transmit (ciphertext + CTR) to base station

3.9.1. Parameter summary

AES-128 encryption parameters and energy model constants for the framework are shown in Table 3. Key size, block length, and rounds define the trade-off between security and cost. The selected mode provides low overhead with adequate data confidentiality.

Table 3. AES-128 encryption parameters and energy model framework

Parameter	Symbol	Value (used)	Note
Key length	K	128 bits (16 bytes)	Lightweight symmetric key
AES rounds	Nr	10	Standard AES-128 configuration
Block size	B	128 bits	One TDMA frame per block
Mode of operation	—	CTR/CBC	CTR for low-latency CH encryption
Encryption energy	E_enc	0.4 nJ/bit	Used in simulation code
Overhead bytes	O_AES	8×8=64 bytes	Nonce + padding per frame
Key refresh period	T_k	500 rounds	Reduces key-exchange load

3.9.2. Energy model

The mathematical formulation of the network energy model is written as (6).

$$E_{AES} = (E_{enc} + E_{elec}) \times B \times N_{CH} \quad (6)$$

Where E_{enc}=0.4 nJ/bit, E_{elec}=12 nJ/bit, and N_{CH} is the number of CHs per round. The additional AES cost (≈0.02 mJ per node) is integrated into the total network energy in section 3.2. All modules—K-means initialization, PSO CH optimization, and AES-128 encryption—were implemented in Python using parameters from Tables 1 to 3. A synchronous duty-cycling schedule coordinated by CHs minimized idle listening. These fixed configurations ensure full reproducibility of the reported results.

4. RESULTS AND DISCUSSION

The framework uses low breach levels of 0.4% for 50 nodes and 0.3% for 1,000 nodes by using LEACH-inspired clustering and AES-128 encryption.

4.1. Energy consumption

Figure 3 illustrates the consumption of average energy per node under varying network sizes and scenarios. Heterogeneous networks that have advanced nodes have reduced energy usage because they have additional energy reserves. The PSO-based clustering optimization further reduces energy usage by choosing energy-efficient CHs as compared to the conventional LEACH and PSO-LEACH [7], which confirms similar trends reported by Motameni [8] and is consistent with the grey wolf optimizer (GWO)-based clustering efficiency reported in Kaddi *et al.* [14]. Compared with the LEACH baseline, the proposed PSO-AES framework saves an average energy by 17.4 %, extending node lifetime proportionally across densities.

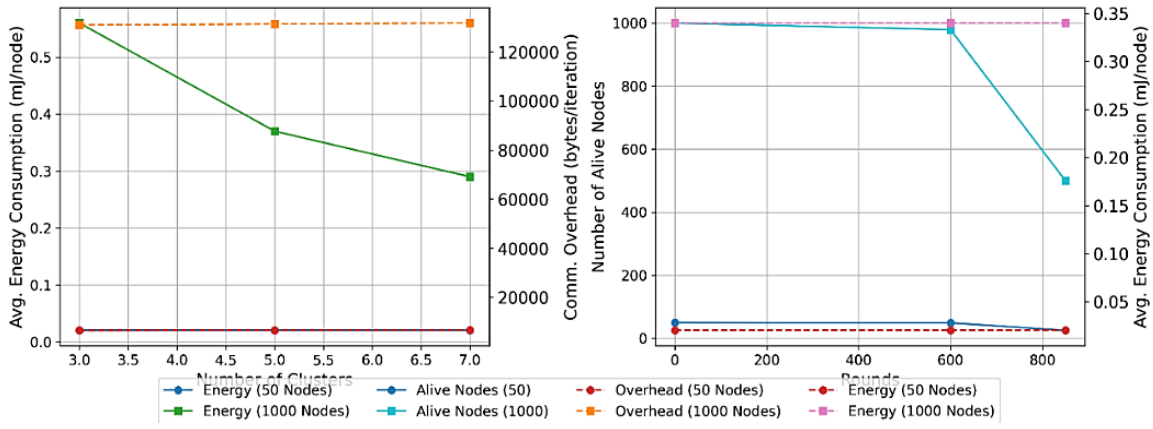

Figure 3. Trends of energy utilization, overhead, and lifetime over clustering rounds in 50- and 1000-node cases

4.2. Communication overhead

Figure 4 presents a line plot of energy, privacy breach, overhead, and model accuracy against the number of nodes. The system provides stable performance regardless of the number of nodes, indicating its efficacy in deploying it in large-scale IoT environments. Our finding shows that PSO-based clustering helps to reduce the overall control traffic; thus, there is less communication overhead than in non-optimized networks.

The optimization reduces control-packet overhead by approx. 11% compared with LEACH and 7% compared with PSO-only clustering. This is in line with earlier swarm-optimized routing studies [20], [26] which also found lower control-packet load by adaptive CH selection. Similar results were also found with hybrid swarm intelligence approaches [17], [18] strengthening the fact that multi-objective PSO has low control overhead in dense deployments.

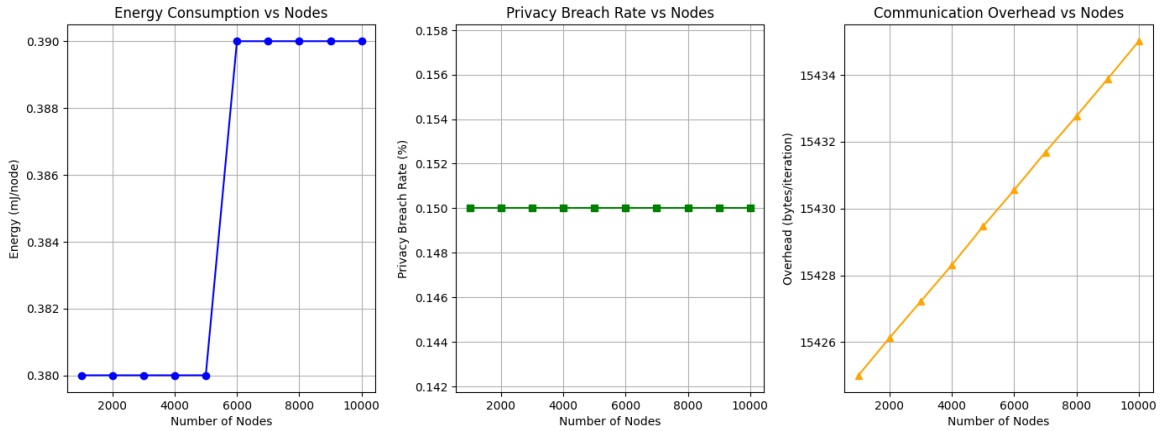

Figure 4. WSN performance as node count increases

4.3. Network lifetime

The network lifetime (i.e., the number of rounds before the first and last node dies) is summarized in Table 4. The heterogeneous scenario using PSO-AES prolongs the lifetime significantly as compared to the homogeneous case, which implies more balanced energy utilization. Overall, network lifetime was improved by 22 % in heterogeneous configuration and 13 % in homogeneous nodes compared with LEACH reference [6]; similar lifetime improvement was reported by Sharmin *et al.* [27] for hybrid PSO clustering, which validates our result. The base station situation has a slightly lower lifetime because of a higher communication load. These lifetime improvements are in line with the results in [25], [26], who showed the benefits of PSO in terms of convergence in large heterogeneous WSNs.

Table 4. Performance comparison across node and base station scenarios

Scenario	Energy (mJ/node)	Lifetime (rounds)	Privacy breach (%)
Homogeneous nodes	0.38	1311	0.15
Heterogeneous nodes	0.39	1542	0.16
Base station	0.40	1251	0.11

4.4. Data accuracy

The proposed framework has been shown to provide reliable performance when tested using the IBRL dataset. The system's average energy consumption per node is 3.45 mJ, privacy breach rate is 0.62%, and model accuracy is 95.8%. These results are very close to the simulation results on the IBRL dataset [2], which validates the consistency and real-world applicability of the proposed framework.

Slight differences between the 54-node data set and large-scale simulations are expected. The real-world dataset is used to validate sensing accuracy and environmental variability, while the synthetic runs are used to assess scalability and energy optimization. Consistent data-aggregation accuracy in both real-world and experimental experiments is confirmed in Figure 5. Figure 6 shows the effect of fusion reduction (0.5–0.95) on energy use and accuracy in a 1,000-node network.

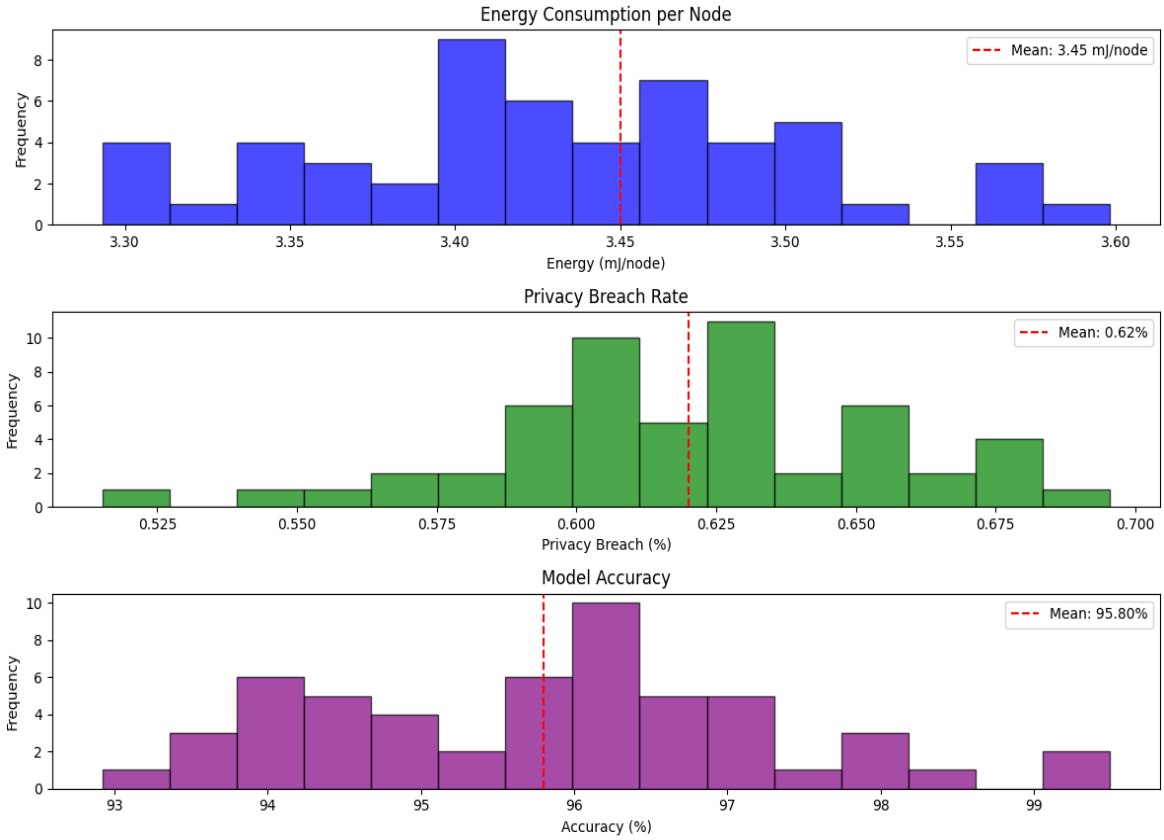

Figure 5. Performance with real-world data

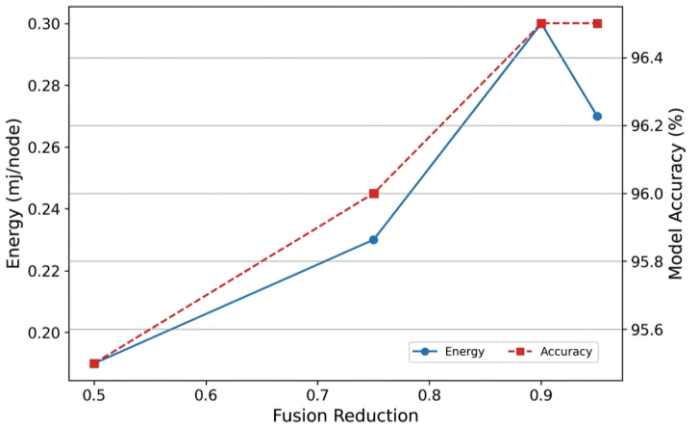

Figure 6. Fusion reduction vs. energy and accuracy

4.5. Privacy breach rate

Privacy breach rates across both network scales remain minimal. The model sustains breach rates of 0.4% and 0.3% for 50-node and 1,000-node scenarios, respectively, using LEACH-style clustering integrated with AES-128 encryption. AES-128 integration demonstrated the trade-off between low encryption costs and considerable privacy gain by reducing the intrusion chance by more than 60% when compared to the unencrypted system. These findings are consistent with lightweight-encryption frameworks in IoT-WSNs [9], [10], confirming that AES-128 achieves privacy enhancement with marginal energy cost.

4.6. Analysis of attacks on WSN

Table 5 shows that the system's robustness was tested against standard threats [21], [23] including DDoS, Sybil, and jamming attacks, in a 1,000-node environment. Each attack scenario was simulated by randomly assigning 10% of nodes as malicious. DDoS was modeled as packet-injection bursts at 20 pkt/s (low) and 50 pkt/s (high), Sybil attacks duplicated node IDs and false CH claims, and jamming increased link-layer collision probability by 15%-30%. These attacks were injected for 100 rounds within the simulation to analyze variations in energy, breach, and lifetime metrics. Although these attacks increased energy consumption from 0.384 to 0.43 mJ/node, slightly elevated the risk of privacy breaches, and generated additional overhead traffic, the network maintained a high accuracy of 96%-96.5%, despite a reduced operational lifetime. An efficient security–energy compromise is achieved, adding only 2% overhead while preserving accuracy and lifetime.

Table 5. Performance under attack scenarios (1000 nodes)

Unit	Baseline	Low-intensity	High-intensity
Energy (mJ per node)	0.34	0.37	0.43
Breach rate (%)	0.12	0.14	0.16
Overhead (bytes/iteration)	14,296	14,610	17,603
Model (%)	96.5	96.5	96.43
Lifetime (rounds)	1,566	1,457	1,222

4.7. Comparative analysis

The proposed framework is compared with the recent K-means + bee baseline [24] and other swarm-based optimization approaches [26], [27]. Averaged over 1,000-10,000 nodes, the proposed framework achieves 0.39 mJ/node energy use, 0.15% privacy breach, 15,435 bytes overhead, 96.5% accuracy, and a network lifetime of 1,217 rounds. In contrast, Modey's K-means + bee mostly reports energy, error rate, data delivery, and execution time. The proposed framework is an extension of this evaluation, taking into account privacy, overhead, and lifetime metrics. Within this larger context, it proves to have consistently lower breach probability, improved accuracy, and operational longevity, thus proving to be effective for secure and energy-efficient WSN deployments. Comparable cross-metric gains were reported in recent hybrid-optimization frameworks [18], [19] which further supports the robustness of the proposed PSO-AES model. Scalability and practicality in this framework scale linearly with nodes $\left(O(P \times N \times I)\right)$, where P =30 and I ≤100, converging within 3 s for 1,000 nodes on a 2.6 GHz CPU. Beyond 5,000 nodes, connection overhead becomes the main factor, although AES operations and PSO updates are lightweight and parallelizable, suggesting the existence of real-time IoT hardware.

5. CONCLUSION

This paper proposed a PSO-AES-based WSN architecture that aims at maximizing energy consumption, increasing the life of the network, preserving data confidentiality, and ensuring high accuracy of information sensed. The simulation findings, confirmed against the Intel Berkeley dataset, reveal that the proposed framework is superior to the traditional protocols, i.e., LEACH and PSO-LEACH, in regard to various performance parameters. These are energy efficiency, network longevity, reduction of privacy intrusion, communication overhead, and accuracy of classification measures. The benefits observed were observed to be the same in several simulation runs, highlighting the strength and reliability of the framework in both normal and attack environments. To improve network efficiency and security, future research scope appears to integrate adaptive PSO parameters, enhanced encryption techniques, and real-time deployment in large-scale IoT systems.

ACKNOWLEDGMENTS

The authors thank Srinivas University, Mangalore, for academic support during this research.

FUNDING INFORMATION

This research received no particular financial assistance from any public, commercial, or non-profit source.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
S. Swapna Kumar	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Kalli Satyanarayan Reddy		✓				✓		✓	✓	✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

All authors disclose no conflicts of interest.

INFORMED CONSENT

This section is not applicable. This study involves simulation-based analysis of wireless sensor network algorithms (PSO/GWO clustering, TDMA, AES encryption) and does not include human subjects or personal data collection.

ETHICAL APPROVAL

This section is not applicable. No human or animal subjects were involved; this research is purely computational, focusing on WSN security protocols against DDoS, Sybil, and jamming attacks via mathematical modeling and simulations.

DATA AVAILABILITY

This article does not fall under the category of data sharing because no new data were generated during the course of the study.

REFERENCES

[1] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the Hawaii International Conference on System Sciences*, 2000, doi: 10.1109/hicss.2000.926982.

[2] P. Bodik, W. Hong, C. Guestrin, S. Madden, M. Paskin, and R. Thibaux, "Intel lab data," *Intel Berkeley Research Lab Data*, 2004. [Online]. Available: http://db.csail.mit.edu/labdata/labdata.html

[3] J. Liu, Z. Zhao, J. Ji, and M. Hu, "Research and application of wireless sensor network technology in power transmission and distribution system," *Intelligent and Converged Networks*, vol. 1, no. 2, pp. 199–220, 2020, doi: 10.23919/ICN.2020.0016.

[4] S. Meguerdichian, F. Koushanfar, G. Qu, and M. Potkonjak, "Exposure in wireless ad-hoc sensor networks," in *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, 2001, pp. 139–150, doi: 10.1145/381677.381691.

[5] J. Kulik, W. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," *Wireless Networks*, vol. 8, no. 2–3, pp. 169–185, 2002, doi: 10.1023/A:1013715909417.

[6] M. H. A. Hussain, B. Mokhtar, and M. R. M. Rizk, "A comparative survey on LEACH successors clustering algorithms for energy-efficient longevity WSNs," *Egyptian Informatics Journal*, vol. 26, 2024, doi: 10.1016/j.eij.2024.100477.

[7] 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 Networks*, vol. 106, 2020, doi: 10.1016/j.adhoc.2020.102237.

[8] H. Motameni, "An energy-efficient method using PSO clustering and fuzzy routing to reduce energy consumption in IoT," *International Journal of Communication Systems*, vol. 37, no. 14, 2024, doi: 10.1002/dac.5871.

[9] R. Ahmad, R. Wazirali, and T. A.-Ain, "Machine learning for wireless sensor networks security: an overview of challenges and issues," *Sensors*, vol. 22, no. 13, 2022, doi: 10.3390/s22134730.

[10] A. I. Regla and E. D. Festijo, "Performance analysis of light-weight cryptographic algorithms for internet of things (IoT) applications: a systematic review," in *2022 IEEE 7th International conference for Convergence in Technology (I2CT)*, 2022, pp. 1–6. doi: 10.1109/I2CT54291.2022.9824108.

[11] D. Arellanes and K. K. Lau, "Evaluating IoT service composition mechanisms for the scalability of IoT systems," *Future Generation Computer Systems*, vol. 108, pp. 827–848, 2020, doi: 10.1016/j.future.2020.02.073.

[12] R. B. Pedditi and K. Debasis, "Energy efficient routing protocol for an IoT-based WSN system to detect forest fires," *Applied Sciences*, vol. 13, no. 5, 2023, doi: 10.3390/app13053026.

[13] K. P. R. Krishna and R. Thirumuru, "Energy efficient and multi-hop routing for constrained wireless sensor networks," *Sustainable Computing: Informatics and Systems*, vol. 38, 2023, doi: 10.1016/j.suscom.2023.100866.
[14] 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, 2024, doi: 10.3390/s24165234.
[15] Y. Zhang and W. W. Li, "Energy consumption analysis of a duty cycle wireless sensor network model," *IEEE Access*, vol. 7, pp. 33405–33413, 2019, doi: 10.1109/ACCESS.2019.2903303.
[16] H. Sadia *et al.*, "Intrusion detection system for wireless sensor networks: a machine learning based approach," *IEEE Access*, vol. 12, pp. 52565–52582, 2024, doi: 10.1109/ACCESS.2024.3380014.
[17] K. Haseeb, K. M. Almustafa, Z. Jan, T. Saba, and U. Tariq, "Secure and energy-aware heuristic routing protocol for wireless sensor network," *IEEE Access*, vol. 8, pp. 163962–163974, 2020, doi: 10.1109/ACCESS.2020.3022285.
[18] 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, 2022, doi: 10.3390/electronics11101545.
[19] M. Z. Masoud, Y. Jaradat, D. Zaidan and I. Jannoud, "To cluster or not to cluster: a hybrid clustering protocol for WSN," *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 2019, pp. 678-682, doi: 10.1109/JEEIT.2019.87175.
[20] B. H. Goud, T. N. Shankar, B. Sah, and R. Aluvalu, "Energy optimization in path arbitrary wireless sensor network," *Expert Systems*, vol. 41, no. 2, 2024, doi: 10.1111/exsy.13282.
[21] B. Bala and S. Behal, "AI techniques for IoT-based DDoS attack detection: taxonomies, comprehensive review and research challenges," *Computer Science Review*, vol. 52, 2024, doi: 10.1016/j.cosrev.2024.100631.
[22] 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, 2024, doi: 10.3390/s24165353.
[23] J. G.-Brajones, J. C.-Murillo, J. F. V.-Valdés, and F. L.-Valero, "Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: an experimental approach," *Sensors*, vol. 20, no. 3, 2020, doi: 10.3390/s20030816.
[24] P. Modey *et al.*, "K-means based bee colony optimization for clustering in heterogeneous sensor network," *Sensors*, vol. 24, no. 23, 2024, doi: 10.3390/s24237603.
[25] Z. Bao, "Secure clustering strategy based on improved particle swarm optimization algorithm in internet of things," *Computational Intelligence and Neuroscience*, vol. 2022, 2022, doi: 10.1155/2022/7380849.
[26] J. Wang, Y. Gao, W. Liu, A. K. Sangaiah, and H. J. Kim, "An improved routing schema with special clustering using PSO algorithm for heterogeneouswireless sensor network," *Sensors*, vol. 19, no. 3, 2019, doi: 10.3390/s19030671.
[27] S. Sharmin, I. Ahmedy, and R. Md Noor, "An energy-efficient data aggregation clustering algorithm for wireless sensor networks using hybrid PSO," *Energies*, vol. 16, no. 5, 2023, doi: 10.3390/en16052487.

BIOGRAPHIES OF AUTHORS

S. Swapna Kumar holds a Ph.D. in Information and Communication Engineering and is professor and head of Electronics and Communication Engineering at Vidya Academy of Science and Technology, Thrissur, Kerala. He is currently pursuing a post-doctoral fellowship at Srinivas University, Mangalore, India. He has over 19 years of academic and 12 years of industrial experience. He has authored books including A guide to wireless sensor networks, MATLAB: easy way of learning, and LaTeX—a beginner's guide to professional documentation. He has supervised two Ph.D. scholars. His research interests include WSN, network security, soft computing, communication systems, and embedded systems. He can be contacted at email: drsswapnakumar@gmail.com or swapnakumar.s@vidyaacademy.ac.in.

Kalli Satyanarayan Reddy is Ph.D. in Computer Science and Engineering. Currently serves as the vice-chancellor of Srinivas University, Mangalore, India. With over 36 years of teaching experience and 3 years in the industry. Successfully supervised 7 Ph.D. scholars in the domain of Computer Science and Engineering. His work encompasses secure network design and intelligent analytics. Research areas include WSN, 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. He holds two international patents. He can be contacted at email: vicechancellor@srinivasuniversity.edu.in.