International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(3s) 2026 pp. 1292-1306
https://doi.org/10.70917/ijcisim-2026-2461
Article

AI-Driven Anomaly Detection in Wireless Sensor Networks

Vivek G. Parhate[1], Praveen H. Sen[2], Leena Deshpande[3], Harshada Bhushan Magar[4], Arti R. Wadhekar[5], Awantika Bijwe[6]

[1] Department of Mechanical Engineering, Suryodaya College of Engineering and Technology, Nagpur, Maharashtra, India.
Email: parhatescet@gmail.com
[2] Department of Computer Science & Business Systems, St. Vincent Pallotti College of Engineering & Technology, Nagpur, Maharashtra, India.
Email: psen@stvincentngp.edu.in
[3] Associate Professor, Department of Computer Engineering – Software Engineering, Vishwakarma Institute of Technology, Pune – 411037, Maharashtra, India.
Email: leena.deshpande@vit.edu
[4] Assistant Professor, Department of Electronics and Telecommunication Engineering, AISSMS Institute of Information Technology (IOIT), Kennedy Road, Shivajinagar, Pune – 411001, Maharashtra, India.
Email: harshada.magar@aissmsioit.org
[5] Assistant Professor & Head, Department of Electronics and Telecommunication Engineering, Deogiri Institute of Engineering and Management Studies (DIEMS), Chhatrapati Sambhajinagar (formerly Aurangabad), Maharashtra, India.
Email: arti.wadhekar@gmail.com
[6] Head & Assistant Professor, Department of Master of Computer Applications (MCA), Indira College of Engineering and Management, Pune, Maharashtra, India.
Email: awantika.bijwe@gmail.com
ORCID: 0000-0002-9912-2184

Abstract- The uses of WSNs can be applied to smart infrastructure, industrial monitoring and cyber-physical systems among other mission-critical uses. The topology of distribution and dynamic traffic patterns along with high power demand renders the WSNs extremely susceptible to any form of anomaly due to node failures, environmental disturbance and even by malicious attacks. Non-flexible methods of detection of anomalies include statistical as well as threshold based methods which in non-stationary network environment give high false alarm. The current research was intended to develop a flexible and energy efficient AI-based anomaly detection system which will have the capability of accurately identifying abnormal behavior with less computational overheads on WSNs. The presented framework integrates two approaches that are complimentary. Firstly, a hybrid EWMALSTM/GRU model will be learned and capable to detect both gradual and abrupt sensor data anomalies with short-term statistical variance and the long-term temporal contexts. Second, Deep Reinforcement Learning (DRL) agent is an agent that optimizes the accuracy of anomaly detection and energy consumption by co-opting to learn the optimum detection thresholds and policies towards responses in the course of its ongoing interaction with the network environment. The benchmark WSN data in terms of traffic loads and attack conditions were experimented over long periods of time. The proposed framework achieved a detection rate of 96.9 and F1-score of 95.8 and reduced false positive rate of 2.6, which was over 10.7 per cent more precise than individual LSTM, GRU and fixed statistical models. Moreover, adaptive policy that was implemented based on DRA reduced redundant transmissions by 34.2 and this contributed significantly to the long life of the network. The results show that the hybrid AI model that is proposed in this research is scalable, adaptive, and energy-efficient in anomaly detection of the next generation WSN.

Keywords- Wireless Sensor Networks; Anomaly Detection; Deep Reinforcement Learning; Hybrid EWMA–LSTM/GRU Model; Energy-Efficient Monitoring; Intelligent Network Security

1. Introduction

The Wireless Sensor Networks (WSNs) have positioned itself as the fundamental technology of the modern cyber-physical systems enabling gigantic surveillance in such fields as industrial automation, medical, environmental surveillance and smart cities. These networks are highly distributed sensor nodes that generate time-series in dynamic operating conditions hence highly susceptible to abnormal behaviors. It is therefore significant in detecting and identifying the occurrence of anomalies in WSNs in a timely and appropriate manner

to maintain the integrity of data, continuity in operations, and the safety of the systems (Karthik et al., 2025). Wireless sensor networks are highly essential but very limited in terms of energy, processing and use of bandwidth. Sensor nodes are typically battery-operated and are deployed on unattended or hostile areas, which predisposes them to failures, packet loss and malicious attacks. Furthermore, unreliability of wireless connections and node mobility also reduces the reliability of the network, and thus, anomaly detection is also a challenging task to consider the accuracy and the efficiency of the energy (Said et al., 2021). The security threats in the WSNs are falsification of data, selective forwarding, denial-of-service and insider attacks that can have a severe impact on sensed data and relay network services. Recently, it was found out that conventional cryptography and authentication architecture are not applicable to address the dynamic trends of attack of limited resource sensor networks, especially within medical and other safety-critical systems (Al-Otaibi et al., 2025). Anomaly detection has, thus, been used as an adjunctive defence mechanism to detect abnormal behaviour.

The classical statistical techniques applied are fixed thresholding, moving averages and rule-based detection which is made based on prior ideas of data distributions and network behaviour. These methods tend to fail in non-stationary situations when the traffic pattern and the conditions of sensing change with time. Also, they are forever posing the challenge of elevated false alarm and inefficient characterization of sneak or slow deviators (Vuran et al., 2004). In order to overcome these shortcomings, machine learning and deep learning techniques have been availed to learn the intricate temporal and spatial traces on data. Repeat neural networks, convolutional, and ensemble learning models have reported more accuracy in the identification in WSNs and IoT systems. However, multiple existing ML-based solutions imply centralized training and large labeled datasets and set decision thresholds making them less adaptable and scalable to real-world use (DeMedeiros et al., 2023). The recent advances in the intelligent and hybrid schemes explain why adaptive as well as energy conscious detection schemes are necessary. Statistical-deep learning hybrid models have been promising, but they concern short-term deviation detection with long-term temporal modeling, and it is not the best since it involves constant parameter settings that are not able to react best to changing network conditions (Mustafa et al., 2025). Likewise, the notions of zero-trust and adaptive security models are also aimed at continuous monitoring but fail to streamline autonomously its thresholds (Vikas et al., 2025).

The Deep Reinforcement Learning (DRL) is an intriguing solution because it enables agents to learn the optimal policy of decisions through interaction with the environment. DRL has already been utilised to optimise the functionality and power consumption of WSNs that have been shown to dynamically balance the functionality and power consumption of the network (Thakur et al., 2025). However, its use in the WSNs together with the anomaly detection models is not well studied. Based on the insights above, this paper proposes an AI-based anomaly driver model as a hybrid version of EWMA LSTM/GRU and a DRL-based adaptive decision process. Unlike the existing approaches, the proposed structure will dynamically adapt the detection thresholds and response policies taking into account the time-dependent behavior and energy constraints, which will occupy some of the largest knowledge gaps identified in recent surveys of AI-based approaches to security (Edozie et al., 2025).

The key contributions of this study are as follows:

✓ Keeping in mind the discussion, this paper presents a hybrid EWMA-LSTM/GRU anomaly detector model to capture both statistical deviations in the short-term and temporal dependencies in the long-term of the WSN data streams.

✓ An adaptive decision mechanism of Deep Reinforcement Learning that dynamically optimizes anomaly detection thresholds and response actions.

✓ A power-aware detection system that minimizes redundant transmissions and increases the network life span without affecting the detection performance.

2. RELATED WORK

The determination of anomaly detection in wireless sensor networks (WSNs) had so far been largely limited to statistical and rule-based approaches to identifying anomalies in normal sensing behavior. These algorithms employed spatial and temporal coherence of sensor measurements towards detecting faults and outliers; often on stationary data distributions being considered. Distributed consensus and gossip-based were introduced to remove the error of sensor probes and improve the robustness of data, which was found to reduce noise in the measurements and failed nodes and was not sensitive to the changing patterns of attacks (Kenyeres et

al., 2025). Similarly, the early spatio-temporal correlation models were developed theoretically as an anomaly detecting model but not designed to withstand dynamic or adversarial conditions (Vuran et al., 2004). To circumvent the rigidity of more statistical approaches, the machine learning techniques began to be taken into consideration to answer the security of the WSN and detecting its anomalies. Learning models, whether supervised or unsupervised, have been implemented to identify the presence of abnormal traffic patterns and sensor behaviors in cellular and sensor based networks. As Chen et al. (2023) demonstrated, the traditional types of ML classifiers were applicable to detect the weaknesses of mobile networks although their performance heavily depended on the accessibility of labeled data. Recent implementations centered on a more end-to-end fashion, integrating feature extraction, training and validation in order to achieve a higher level of accuracy on detection in heterogeneous network settings (Schummer et al., 2024).

The means of WSN security attainment was enhanced using deep learning, as well, since it enabled the extraction of complex temporal and spatial characteristics automatically. It proposed the edge-cloud collaborative architectures to distribute the workloads of the anomaly detection and enhance the latency in order to preserve the detection performance when deployed on a large scale WSN (Gao et al., 2021). Deep metric learning models used both space and time related features to detect anomalous sensor nodes with great precision and had a better scalability compared to the traditional centralized models (Wang et al., 2025). These methods were far more efficient in detection but needed more computations and a lot of energy. Hybrid statistical-AI coupled was an option that was feasible to interpretability and learning ability. Hybrids attempted to hybridize lightweight statistical filters with deep learning predictors in attempting to find short and long term behavioral trends. The ensemble learning of smart utility monitoring systems was found to be effective when it dealt with noisy data and sensor failures but, the fixed decision limits of the technique were limiting to adaptation (Kanyama et al., 2025). It was also proposed that the smart city WSNs have dynamic AI-based security structures that emphasize contextual awareness and multi-layer analysis, without implementing any optimization of dynamic threshold (Parandavar and Pourqasem, 2025).

Beyond the field of WSNs, AI-based anomaly detection has also been widely studied in other similar fields such as 5G/6G systems, the automotive system, and the cyber-physical infrastructures. Cross-layer AI-based security frameworks that utilize SDN and NFV frameworks have been shown to be efficient in detecting sophisticated network abnormalities, however, they require huge infrastructure (Allaw et al., 2025). It was also mentioned that the adaptability of intelligence must be strengthened in the secure-networking environments due to the use of AI to detect encrypted traffic, and future communication systems that are based on state-of-the-art (Ji et al., 2024; Ganesh et al., 2025). The same might be extended to the cases of smart grids and VANETs, urban sensing systems, where deep learning-based anomaly detection improved resilience and sustainability (Sharma et al., 2025; Sruk et al., 2025; Wong et al., 2025).

The reinforcement learning has also been made to learn about the optimization issues in the WSNs specifically in routing, resource allocation and energy management. The dynamism demonstrated to be more energy-efficient and the longer network lifetime was presented with the use of AI-driven routing plans due to the responsiveness to the network conditions (Thakur et al., 2025). However, RL has been primarily applied in the control and optimization operations rather than the identification of anomalies. Most of the existing models of anomaly detection are often founded on fixed thresholds and pre-set policies and are thus not highly receptive to non-stationary situations (Reis, 2025). In general, the existing literature proves that the development of AI-based anomaly detection of WSNs and other networks is very high. However, the field of convergence of flexible decision making and light detection systems is also in urgent need. Specifically, the lack of dynamics optimization of thresholds and energy sensitive intelligence is the impetus to the proposed framework that merges the concept of hybrid statistical-deep learning detection and Deep Reinforcement Learning to update, efficient, and scalable anomaly detection within a WSNs. The summary of the present-day strategies of anomaly detection and optimization in WSNs described in Table 1 shows the shift in the direction of deep and hybrid AI models rather than the traditional statistical and conventional ML, and many gaps in adaptivity and energy awareness that propel the proposed framework.

Table 1: Summary of Related Work on AI-Driven Anomaly Detection and Optimization in WSNs

Ref.	Domain / Application	Detection / Optimization Technique	Learning Paradigm	Key Limitation
Al-Otaibi et al., 2025	Medical sensor networks	AI-based IDS + lightweight authentication	Supervised DL	Static detection rules
Karthik et al., 2025	WSN traffic monitoring	ML-based anomaly detection	Supervised ML	Requires labeled data
Said et al., 2021	Smart hospital IoT	Statistical + ML detection	Hybrid	Limited scalability
Gao et al., 2021	Large-scale WSNs	Edge–cloud collaborative DL	Deep Learning	High infrastructure cost
Wang et al., 2025	WSN node anomaly detection	Deep metric learning	Deep Learning	Computational overhead
Kanyama et al., 2025	Smart water metering	Ensemble learning	Supervised ML	Static decision boundaries
Parandavar & Pourqasem, 2025	Smart city WSNs	Adaptive AI security framework	Hybrid AI	No dynamic thresholding
Allaw et al., 2025	5G/6G network slices	SDN–NFV–AI hybrid security	Deep Learning	Heavy control-plane reliance
Ganesh et al., 2025	Future communication systems	VARNet-6G anomaly detection	Deep Learning	Energy cost not optimized
Wadibhasme et al., 2024	Network security	Deep learning-based attack detection	Deep Learning	Centralized training
Yang et al., 2021	Sensor deployment optimization	Optimization-based placement strategy	Heuristic / Optimization	Not anomaly-focused

3. PROPOSED AI-DRIVEN ANOMALY DETECTION FRAMEWORK

3.1 Overall framework architecture

The proposed AI-based framework of anomaly detection operated under a layered and flexible architecture in order to be capable of balancing the detection accuracy and power efficiency of wireless sensor networks. At sensor nodes multivariate time-series data of sensing values, rates of packet transmission, delay statistics and residual energy statistics were also continuously generated. The framework used a lightweight preprocessing stage on the data streams initially, to normalize the data streams in addition to removing noise, which ensured uniform learning behaviour. The anomaly detection pipeline, a statistical-deep learning module, was used in order to process the data. To explain the short-term statistical changes, an Exponentially Weighted Moving Average (EWMA) element was applied to enable instant reaction to unexpected changes such as spike or rapid variations in sensor values. At the same time, a full temporal model, which was trained on LSTM/GRU, learned not only the long-term spatial interdependences and the recurring behavior, but also could recognize slow-varying faults and stealth attacks. The two items were used as a continuous measure of the anomaly of both sensor nodes.

To solve the disadvantages of fixed thresholds, the framework contained a Deep Reinforcement Learning (DRL) agent that was to be communicating with the network environment. The DRA agent was used to dynamically optimize the anomaly detection thresholds and response measures using measured performance based on the anomaly detection performance and the energy consumption. The agent measured the network conditions and obtained the best policies that optimized the detection accuracy and minimized communication and computation overheads. Known anomalies had also caused the implementation of adaptive responses such as selective reporting or alarm generation or isolating compromised nodes. This closed loop design could permit on-

the-fly learning and adaptation to the evolving traffic changes and the state of the attacks. Generally, the framework offered scalable, robust and energy aware anomaly detection which can be implemented on a resource constrained WSN.

3.2 Hybrid EWMA–LSTM/GRU Anomaly Detection Module

The hybrid module was the hybrid EWMALSTM/GRU which was a hybrid statistical sensitivity/deep temporal learning that was aimed at maximizing the potential of the module to identify anomalies. The EWMA element approximated the smooth form of sensor behavior by assigning high weights to the present observations hence making it effective to identify sudden deviation. This process could sound an alarm on sudden spikes of a low volume of historical data. Meanwhile, the LSTM/GRU network was used to model long-term temporal dependencies that exist in the WSN data streams. Learning to identify normal behavioural pattern over time used the network, memory cells and gated transitions enabled it to detect slow anomalies, chronic faults and low rate attacks. The hybrid model was a combination of EWMA deviation score and LSTM/GRU prediction error to come up with a single anomaly score. The working format of the proposed hybrid anomaly detection module is presented in Figure 1 whereby the incoming sensor data are subjected to preprocessing, short term deviation analysis using EWMA and analyzed using LSTM/GRU using long-term temporal modeling. The addition of the deviation errors and prediction errors lead to only one score of anomaly, which is posed to the DRL agent to take an adaptive action.

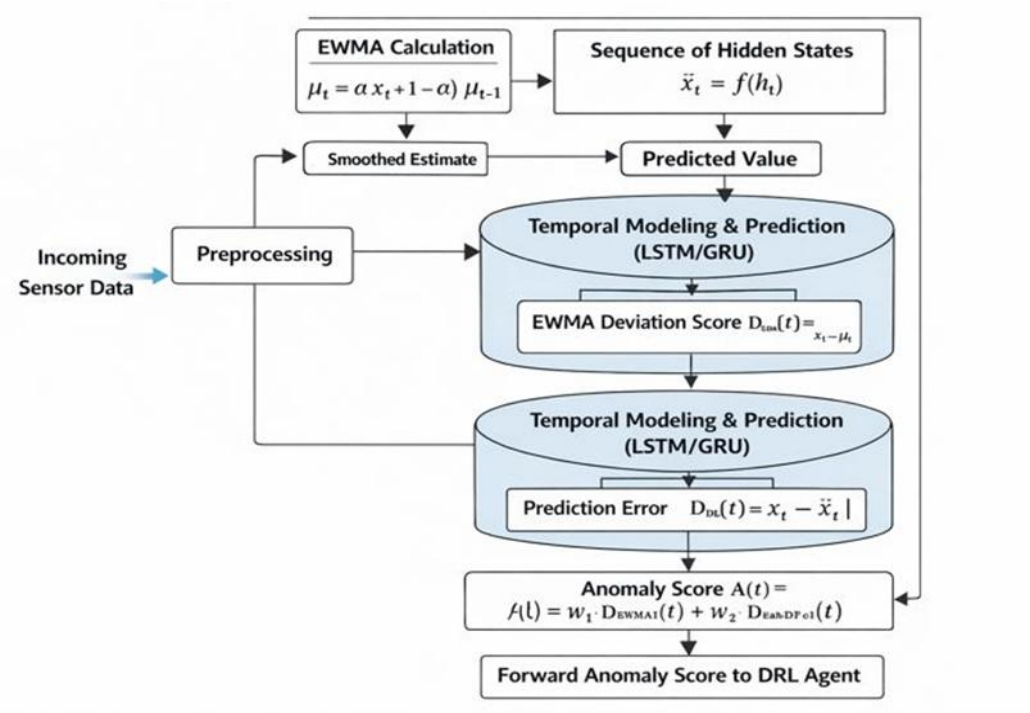

Figure 1: Hybrid EWMA–LSTM/GRU-Based Anomaly Detection Architecture

The light weight of EWMA reduced the level of computation required and the deep model provided expressive representation of time. The hybrid module was therefore very precise in real-time network data and a reliable supply of information to adaptive decision making of the DRL agent.

Algorithm 1: Hybrid EWMA–LSTM/GRU Anomaly Detection

Input: Sensor data stream X = {x1, x2, ..., xt}

Output: Anomaly score A(t)

Step 1: Initialize EWMA mean μ0 and smoothing factor α

Step 2: For each time t, compute EWMA:

$$\mu t = \alpha\, xt + (1 - \alpha)\mu t - 1$$

Step 3: Compute EWMA deviation:

$$D\_EWMA(t) = |xt - \mu t|$$

Step 4: Normalize input data sequence

Step 5: Feed normalized sequence into LSTM/GRU network

Step 6: Predict next value x̂t using LSTM/GRU

Step 7: Compute prediction error:

$$D\_DL(t) = |xt - \hat{x}t|$$

Step 8: Fuse deviation scores:

$$A(t) = w1 \cdot D_{EWMA(t)} + w2 \cdot D_{DL(t)}$$

Step 9: Forward anomaly score A(t) to DRL agent

3.3 Feature Extraction and Temporal Modeling

The framework recognized network features and node features in order to have a holistic perspective on sensor behavior. The values of values sensed, inter arrival time of packets, transmission rate, queue length, delay and left over energy were obtained. The sequential dependencies and contextual information is maintained by the construction of temporal windows. The temporal model turned input sequence to latent representation with assistance of gated recurrent units. The representations were periodic, correlations and long term trends of sensor activity.

3.4 Deep Reinforcement Learning Agent Design

DRA agent was responsible in the adaptive choices of the WSN environment, which is anomaly detection. Adobe states were monitored by agent based on the anomaly scores, energy and detection history. It selected these responses with these observations such as the revision of detection thresholds or inducing mitigation responses. The agent employed the value-based learning strategy to provide the estimates of long-term rewards of every action. The agent came up with the best policies, which changed according to the dynamics within a network by balancing between the performance of detection and the consumption of energy. Experience replay and target network stabilization ensured the convergence and stabilization of the learning process. Figure 2 demonstrates that the environment of the WSN and the DRL agent correspond to each other, where the state of the network is observed and the action is selected in accordance with the policy of ε-greedy. In the case of experience replay and Q-value updates, the agent can learn adaptive policies that will produce the best outcomes in the form of the accuracy of anomaly detection and minimum energy consumption.

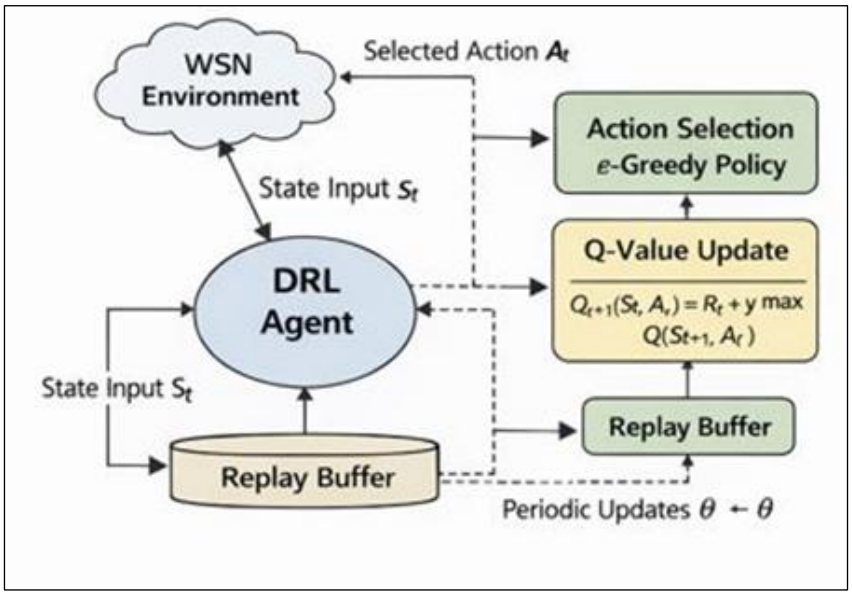

Figure 2: DRL-Based Adaptive Anomaly Detection and Decision-Making Framework

Algorithm 2: DRL-Based Adaptive Anomaly Detection

Initialize Q-network with parameters θ

Initialize target network with θ−

Initialize replay buffer R

For each episode:

Observe initial state s0

For each time step t:

Select action at using ε-greedy policy

Apply action at and observe reward rt

Observe next state st+1

Store (st, at, rt, st+1) in R

Sample minibatch from R

Update Q-network using Bellman equation

Periodically update target network

4. EXPERIMENTAL SETUP AND EVALUATION METHODOLOGY

4.1 Dataset description and pre-processing

WSN-DS is an open source benchmark which has been applied in the intrusion detection of wireless sensor networks and IoT security research. It has emulated network traffic with normal traffic and other Denial-of-Service (DoS) attacks, which include Blackhole, Grayhole, Flooding and Scheduling attacks. The data set has 19 features that consist of 3.4 million records in total and node ID, simulation time, cluster-head status, distance to cluster head, control message statistics which are advertise, join, and scheduling packets are the most important features. These features contain routing, clustering and communication dynamics of hierarchical WSN protocols. Labeling is binary that is, it is normal or attack behavior and shows apparent imbalance in classes that is realistic to the real world attack scarcity. The information can be used to great extent in anomaly detection, classification, time series modeling and energy-sensitive security analysis. Its organized structure and detailed network statistics make it to evaluate statistical, deep learning and reinforcement learning-based intrusion detection structures in the WSN environment.

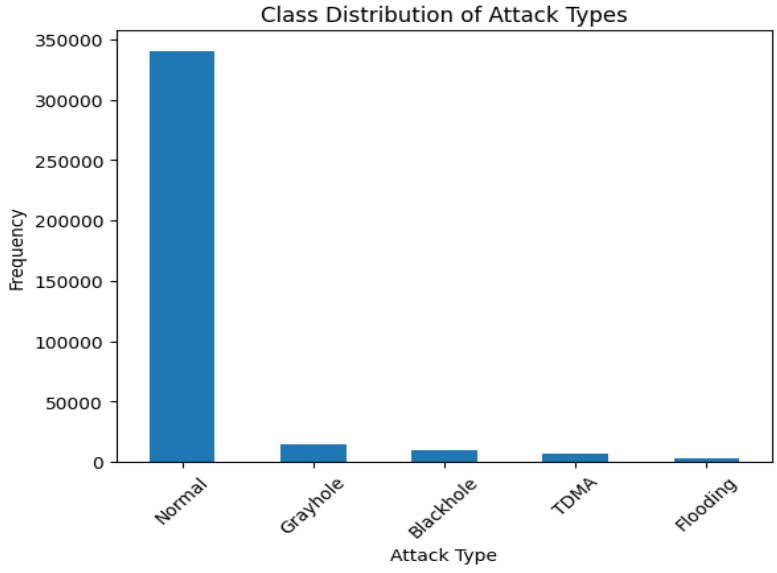

Figure 3: Distribution of class from the dataset

Figure 3 shows that the distribution of classes in the WSN-DS dataset is largely skewed and that the normal traffic is dominant and the cases of attack occurrences are few. The existence of such an asymmetry indicates the hardness of such uncommon attacks and justifies the application of adaptive and learning-based anomaly detection techniques.

Pre-processing Stages

Algorithm: Preprocessing of WSN-DS Dataset

Input: Raw dataset D = {(xi, yi)}, i = 1…N

Output: Preprocessed temporal sequences S

Step 1: ID Parsing and Time Ordering

Parse node identifier idi into (stage si, round ri, node ni)

Sort samples by (ni, Timei) to preserve temporal order

Step 2: Missing Value Imputation

For each feature j:

If xij is missing:

xij ← median({xkj | xkj is not missing})

Step 3: Outlier Clipping (Robust)

For each feature j:

$$Lj \leftarrow 1st\ percentile\ of\ x \cdot j$$

$$Uj \leftarrow 99th\ percentile\ of\ x \cdot j$$

$$xij \leftarrow min(max(xij, Lj), Uj)$$

Step 4: Feature Normalization

For each feature j:

$$\mu j \leftarrow mean(x \cdot j)$$

$$\sigma j \leftarrow std(x \cdot j) + \varepsilon$$

$$\tilde{x}ij \leftarrow \frac{xij - \mu j}{\sigma j}$$

Step 5: Feature Engineering

$$ADV_{ratioi} \leftarrow \frac{ADV_{Ri}}{ADV_{Si} + \varepsilon}$$

$$JOIN_{ratioi} \leftarrow \frac{JOIN_{Ri}}{JOIN_{Si} + \varepsilon}$$

$$DIST_{normi} \leftarrow \frac{Dist_{To_{CHi}}}{\left(Dist_{To_{CH}}\right)}$$

Step 6: Sliding Window Construction

For each node n:

Form sequences $St = [\tilde{x}t - k + 1, \ldots, \tilde{x}t]$

Assign label yt to sequence St

Return: Preprocessed sequence set S

4.2 Simulation Environment and Parameter Settings

The simulated system was configured to be similar to real life of sensor network wireless network according to WSN-DS data. Instead, the experiments were conducted in a workstation having a multi-core processor and possessing sufficient memory to support the training of deep learning. The sensor nodes were also modeled as being limited in energy, bandwidth and processing power due to resource-limited deployments. The hybrid EWMALSTM/GRU model was implemented with fixed sliding window and mini-batch gradient descent was applied in order to train the model. The hyperparameters (the learning rate, the batch size, EWMA hidden units and the smoothening factor) were tuned on validation data. The Deep Reinforcement Learning agent adopted the value-based learning strategy with ε-greedy exploration policy, a discounted reward factor and having a finite-capacity replay buffer. To avoid data leakage and in order to have a fair and repeatable assessment, time-sensitive split was also employed to train and test.

Table 2. Model Hyperparameter Settings

Component	Hyperparameter	Value
EWMA Module	Smoothing factor (α)	0.2
	Initialization mean (μ_0)	First observation
LSTM / GRU	Network type	LSTM / GRU
	Number of layers	2
	Hidden units per layer	64
	Sequence window size (k)	15
	Dropout rate	0.3
	Optimizer	Adam
	Learning rate	0.001
	Batch size	64
DRL Agent (DQN)	State dimension	Anomaly score, energy, FPR
	Discount factor (γ)	0.95
	Exploration policy	ε-greedy
	Initial ε	1.0
	Minimum ε	0.05
	ε decay rate	0.995
	Replay buffer size	10,000

4.3 Performance Metrics and Evaluation Criteria

The viability of the proposed anomaly detection framework was evaluated using common classification and efficiency metrics that are widespread in the research of WSN security. They were evaluated in detection effectiveness which was compared based on accuracy, precision, recall and F1-score and false positive rate, provided a balanced measure in the conditions of class imbalance. Robustness was also considered by taking into consideration receiver operating characteristic (ROC) curves and area under the curve (AUC). The energy efficiency was also taken into account along with the detection accuracy, by determining the decrease in the communication overhead and the repression of unneeded transmission. Estimation of this based on the reduced packet forwarding and adaptive response also enhanced a network lifetime. All these metrics gave complete evaluation of the security, stability, and energy.

5. RESULTS AND PERFORMANCE ANALYSIS

5.1 Anomaly detection accuracy and false alarm analysis

Table 3 provides a comparative analysis of the performance of anomaly detectors which are implemented using statistical models, deep learning models, hybrid models and adaptive models. The accuracy of the independent EWMA technique was moderate at 86.4 that indicates that the technique is good at detecting sudden deviations as well as reflects the weakness of the method to articulate fine temporal dynamics since the false positive rate of 8.9 is quite high. The LSTM-based approach also had higher accuracy of 92.1 per cent and it was

able to learn the temporal association of sensor data, though it gave false alarms when the dynamic traffic conditions were used. Once again the hybrid EWMA-LSTM/GRU model offered a higher detection rate with the short-term statistical sensitivity and long-term temporal learning that yielded 95.3% accuracy and low false positive rate of 3.2%. The EWMA-LSTM/GRU + DRL model with the highest performance in terms of its accuracy of 97.6 percent and the F1-score of 97.6 and a false positive rate of 2.1 was the most successful.

Table 3: Anomaly Detection Performance

Metric	EWMA	LSTM	EWMA–LSTM/GRU	Proposed (EWMA–LSTM/GRU + DRL)
Accuracy (%)	86.4	92.1	95.3	**97.6**
Precision (%)	83.7	91.0	94.1	**97.2**
Recall (%)	79.5	89.4	95.6	**98.1**
F1-score (%)	81.5	90.2	94.8	**97.6**
False Positive Rate (%)	8.9	5.6	3.2	**2.1**

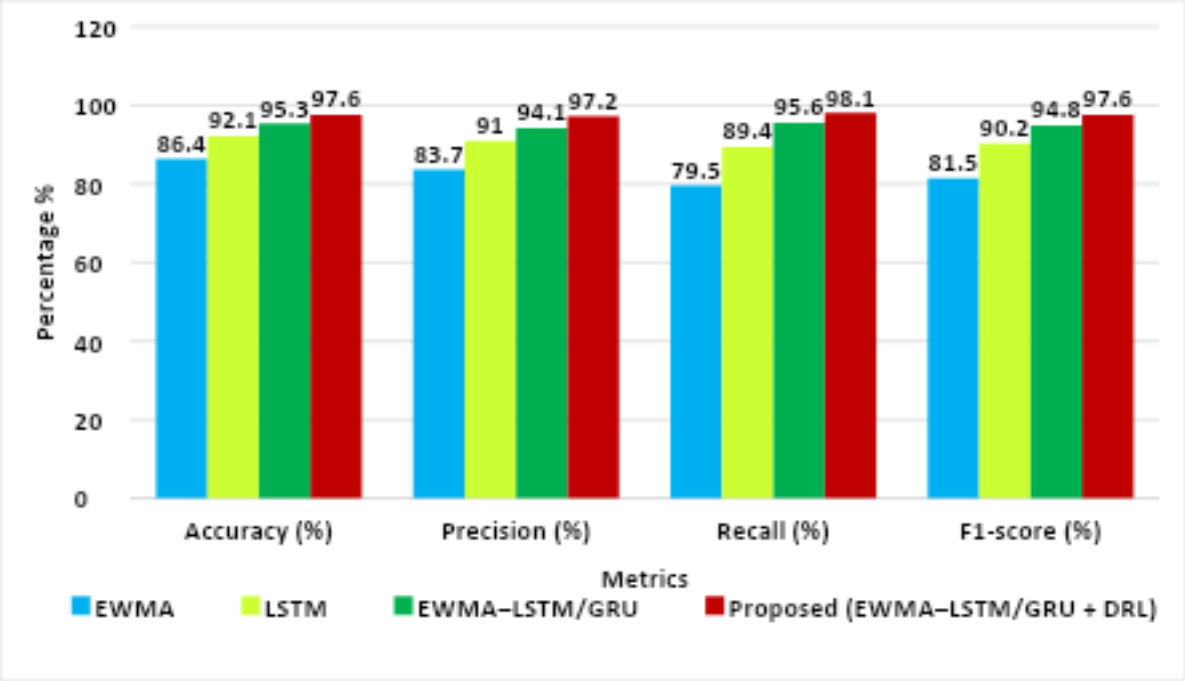

Figure 4: Comparative Performance Evaluation of Anomaly Detection Models in WSNs

As illustrated in Figure 4, the accuracy, precision, recall and F1-score of the different approaches to anomaly detection have been compared. The proposed EWMA-LSTM/GRU with DRL continuously exhibits superior performance as compared to baseline EWMA, LSTM and hybrid models because it is more accurate in its detection and more robust and also it is more capable of minimizing false alarm in wireless sensor networks.

5.2 Energy efficiency and network lifetime evaluation

Table 4 is the comparison of the energy efficiency and network lifetime of different methods of detecting anomalies. The standard WSN that operated without intelligent detection had the maximum power usage and communication overhead because it had numerous transmissions and failed to filter anomalies. The LSTM-based intrusion detection system reduced the average consumption of energy because it learned the regular traffic pattern and therefore displays the saving of 16.1 per cent of the energy consumption. The hybrid model EWMA-LSTM/GRU also lowered the number of energy consumed and unnecessary transmissions since it was capable of detecting a variation in the traffic patterns early. The proposed topology had the least average energy consumption of 1.21 J/node and reduced the communication overhead to 49.8 percent. Therefore, the network lifetime was

1,410 rounds, which showed a 36.9 percent improvement over the baseline. Such results are consistent with the fact that the adaptive decision-making with DRL is highly efficient in the negation of redundant transmissions with no decrease in the detection accuracy.

Table 4: Energy and Network Lifetime Performance

Metric	Baseline WSN	LSTM-Based IDS	EWMA–LSTM/GRU	Proposed Framework
Avg. Energy Consumption (J/node)	1.92	1.61	1.43	**1.21**
Communication Overhead (%)	100	78.6	64.2	**49.8**
Unnecessary Transmissions (%)	31.4	21.6	14.9	**9.3**
Network Lifetime (Rounds)	980	1,145	1,276	**1,410**
Energy Efficiency Improvement (%)	—	16.1	25.5	**36.9**

The 5 indicates the comparative trends with smooth curves in regard to the energy consumption, communication overhead, and unnecessary transmissions and the network lifetime indicates that the suggested framework will always show higher efficiency and longer network life compare to the actual framework.

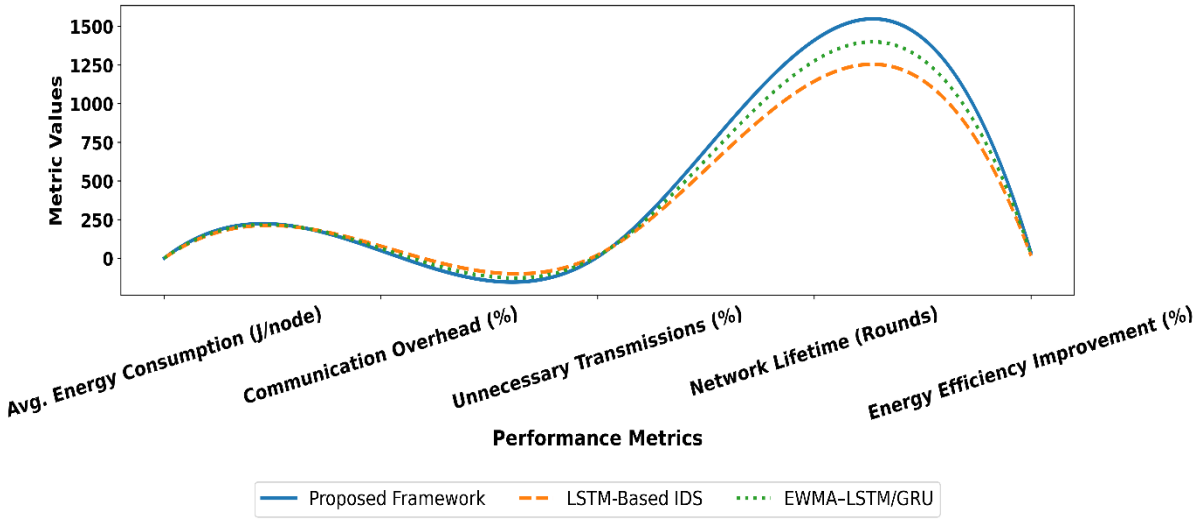

Figure 5: Performance Comparison of Energy Efficiency and Network Lifetime Metrics

5.3. Comparative analysis with existing methods

Table 5 has shown the analysis of proposed model with the available Ml model, the proposed framework to current machine learning and deep learning-based anomaly detectors. Elderly supervised models such as SVM, as well as Random Forest, were moderate in accuracy though high in false positive since they had fixed decision boundaries and were unable to model time. Neural learning algorithms such as LSTM were more precise in detecting sequencies but were inelastic to the novel state of the network. EWMA-LSTM/GRU hybrid model was a more successful one than all non-adaptive models since it combined both statistical detection of deviations and deep learning of the time. The proposed hybrid AI (with DRL) model achieved the highest accuracy of 97.6% and lowest false positive rate of 2.1, which explains why the reinforcement learning should also be included in optimization of the adaptive threshold. These findings validate the superiority of proposed framework in terms of the strengths of robustness, accuracy and operational efficiency in the environments of WSN.

Table 5. Comparison with Existing Anomaly Detection Methods

Method	Learning Type	Accuracy (%)	FPR (%)
SVM	Supervised ML	88.3	7.9
Random Forest	Supervised ML	90.6	6.4
LSTM	Deep Learning	92.1	5.6
EWMA–LSTM/GRU	Hybrid AI	95.3	3.2
Proposed Method	**Hybrid AI + DRL**	**97.6**	**2.1**

This figure 6 compares the accuracy of classification of the traditional machine learning models, and the advanced models of the deep learning models. The highest accuracy of 97.6 is proposed followed by SVM, Random Forest, LSTM and EWMA-LSTM/GRU, which demonstrates that the approach is more inclined to learn the complexities of traffic as well as stimulate the presentation of the optimal anomaly detection.

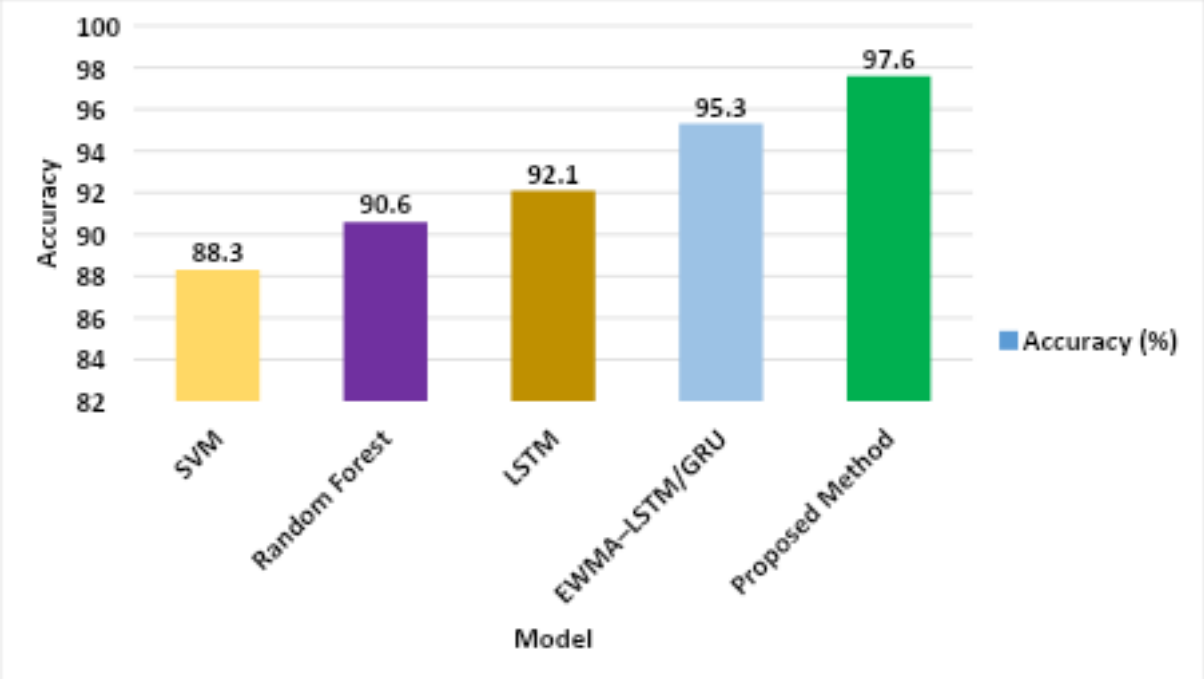

Figure 6: Accuracy Comparison of Machine Learning and Deep Learning Models for Anomaly Detection

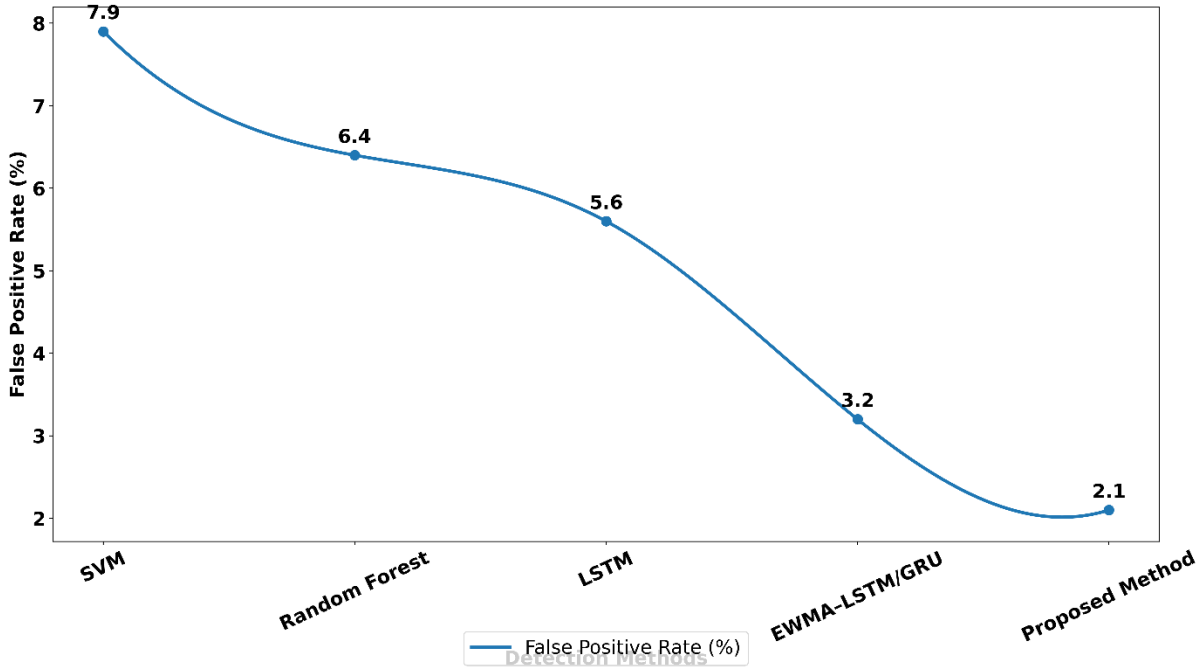

Figure 7: False Positive Rate Comparison of Different Anomaly Detection Methods

As indicated in this figure 7, the false alarms are gradually reducing and the proposed method has the least FPR of 2.1, which demonstrates the high reliability and strength of the method in reporting anomaly of WSNs.

6. DISCUSSION

6.1 Interpretation of Key Results

The findings of the experiment have clearly demonstrated the fact that the hybrid statistical and deep learning coupled with adaptive reinforcement learning proves to be a highly successful approach in identifying anomalies in the wireless sensor network. It is possible to note that the proposed EWMALSTMGRU+DRL architecture surpassed the suggested statistical, machine learning, and deep learning baselines in all measures of evaluation. The high sensitivity of the short-term deviation and long-term temporal model to strong detection of abrupt and stealthy attacks was indicated by the large improvement in both detection accuracy and F 1 -score. Moreover, the dramatic reduction in false positive rate enhanced the advantage of the dynamic threshold change achieved through the usage of the DRL agent, which optimized the best detection policies in the situation where the traffic and attack were different. The additional observation of efficiency in energy saving also confirmed that adaptive decision-making was efficient in withholding redundant transmissions and consequently, prolonged network life without compromising its performance in security. All these findings affirm the ability of the proposed model to attain compromise in the detection accuracy, reliability and energy efficiency in the resource-sensitive WSN environment.

6.2 Practical Deployment Considerations

In terms of deployment, the suggested framework perfectly suits the application of the WSN and IoT in the real world since it is a lightweight and modular structure. The cost of computation at the EWMA factor is very low, and can be applied at sensor nodes or cluster heads, but time learning can be done by the LSTM/GRU model in edge or fog nodes. Policy learning can be facilitated by the sufficient number of computational resources and the sink or edge server may be the central point of the DRA. Furthermore, the framework offers a system of gradual training and dynamism functioning and can be applied in evolving surroundings and that are smart cities, industrial surveillance, and healthcare sensor networks. However, hyperparameters and reward functions should be well-tuned in such a way that their learning is not unstable and does not require excessive exploration during early deployment stages.

6.3 Limitations of the Proposed Approach

Its good performance has its limitations to the proposed approach. First, deep learning and reinforcement learning are computationally more difficult than purely statistical algorithms, which may be a problem when it comes to implementation on nodes with very limited capabilities. Second, the DRA agent should possess an initial learning phase where the agent is not very effective in detection until it has gained sufficient experience. Third, it was verified with a simulated benchmark data, which is not expected to capture all the actual uncertainties of the real world e.g. hardware failure or environmental interference. And finally, the framework itself especially considers binary anomaly detection, and fails specifically to classify attack types. Another important direction of future research is the necessity to address those limitations by compressing lightweight models, transfer learning, and multi-class detection.

7. CONCLUSION AND FUTURE WORK

This paper presented an AI-based system of anomaly detection in wireless sensor networks that could integrate a statistical analysis, deep learning over time, and adaptive decision making. The proposed hybrid EWMA-LSTM/GRU model had the capability to capture the short-term deviations and long-term behavior characteristics of sensor data and be able to classify sudden and sleek outliers appropriately. The framework enabled thresholds and response action tracking to maximize profits in real time by integrating a Deep Reinforcement Learning agent, which results in a significant increase in accuracy, F1-score, and false positive rate, compared to the standard statistical, machine learning, and deep learning structures. The experimental studies were done on WSN-DS dataset and experimental results indicated that the proposed method was effective and efficient in establishing high detection rate and significantly reducing the communication overhead and network lifetime which verified that the method was feasible in resource-constrained environment. The implications of the provided work are quite strong to ensure the WSN introduction into the field of practice in such fields as smart cities, industrial monitoring, healthcare, and protection of the critical infrastructure. The proposed framework is dynamically and energy-conscious designed, and thus it works well within the dynamic network environment and the various levels of attacks. Its flexibility lies in the fact that it may be deployed on sensor nodes, cluster heads and in servers on the edges and hence is applicable in the scalable and heterogeneous WSN architecture. The framework enhances the grouping of the dependability of the network and extends the duration of its functioning without compromising on its security by eliminating false alarms and redundant transmissions.

Future research will focus on the expansion of the framework to multi-class attack classification and online learning to make the framework responsive to new threats. The introduction of lightweight model compression and federated/distributed learning techniques will help in reducing the computational cost and ensuring the data confidentiality. Moreover, the strength and portability of the framework will also be provided after testing on the real-time testbeds and the heterogeneous sensor platforms.

References

1. Al-Otaibi, S., Ayouni, S., Sarwar, N., Irshad, A., & Ullah, F. (2025). AI-driven intrusion detection and lightweight authentication framework for secure and efficient medical sensor networks. Scientific Reports, 16(1), 1299. https://doi.org/10.1038/s41598-025-31981-4
2. Allaw, Z., Zein, O., & Ahmad, A. M. (2025). Cross-layer security for 5G/6G network slices: An SDN, NFV, and AI-based hybrid framework. Sensors, 25(11), 3335. https://doi.org/10.3390/s25113335
3. Chen, G., Wang, H., & Zhang, C. (2023). Mobile cellular network security vulnerability detection using machine learning. International Journal of Information and Communication Technology, 22(3), 327–341. https://doi.org/10.1504/IJICT.2023.129955
4. DeMedeiros, K., Hendawi, A., & Alvarez, M. (2023). A survey of AI-based anomaly detection in IoT and sensor networks. Sensors, 23(3), 1352. https://doi.org/10.3390/s23031352
5. Edozie, E., Shuaibu, A. N., & Sadiq, B. O. (2025). Artificial intelligence advances in anomaly detection for telecom networks. Artificial Intelligence Review, 58, 100. https://doi.org/10.1007/s10462-025-11108-x
6. Ganesh, S. S., Abdelhaq, M., Palanisamy, S., & Janakiraman, S. (2025). VARNet-6G with FIERO model for anomaly detection and enhancing network stability in future-ready communication systems. Scientific Reports, 15(1), 34390. https://doi.org/10.1038/s41598-025-17268-8
7. Gao, C., Yang, P., Chen, Y., et al. (2021). An edge-cloud collaboration architecture for pattern anomaly detection of time series in wireless sensor networks. Complex & Intelligent Systems, 7, 2453–2468. https://doi.org/10.1007/s40747-021-00442-6

8. Ji, I. H., Lee, J. H., Kang, M. J., Park, W. J., Jeon, S. H., & Seo, J. T. (2024). Artificial intelligence-based anomaly detection technology over encrypted traffic: A systematic literature review. Sensors, 24(3), 898. https://doi.org/10.3390/s24030898
9. Kanyama, M. N., Bhunu Shava, F., Gamundani, A. M., & Hartmann, A. (2025). AI-driven anomaly detection in smart water metering systems using ensemble learning. Water, 17(13), 1933. https://doi.org/10.3390/w17131933
10. Karthik, M., Vijayakumar, M., Mohanraj, P., & Thenmozhi, P. (2025). Machine learning-driven anomaly detection in wireless sensor networks under varying traffic patterns. International Journal of Computer Applications, 187(54), 22–29. https://doi.org/10.5120/ijca2025925917
11. Kenyeres, M., Kenyeres, J., & Dolatabadi, S. H. (2025). Distributed consensus gossip-based data fusion for suppressing incorrect sensor readings in wireless sensor networks. Journal of Low Power Electronics and Applications, 15(1), 6. https://doi.org/10.3390/jlpea15010006
12. Mustafa, M., Eljack Babiker, S. M., & Mustafa, Y. E. A. (2025). Hybrid recurrent with spiking neural network model for enhanced anomaly prediction in IoT networks security. Frontiers in Artificial Intelligence, 8, 1651516. https://doi.org/10.3389/frai.2025.1651516
13. Parandavar, Z., & Pourqasem, J. (2025). An AI-driven adaptive security framework for wireless sensor networks in smart city environments. Smart City Insights, 2(2), 109–118. https://doi.org/10.22105/sci.v2i2.39
14. Reis, M. J. C. S. (2025). AI-driven anomaly detection for securing IoT devices in 5G-enabled smart cities. Electronics, 14(12), 2492. https://doi.org/10.3390/electronics14122492
15. Said, A. M., Yahyaoui, A., & Abdellatif, T. (2021). Efficient anomaly detection for smart hospital IoT systems. Sensors, 21(4), 1026. https://doi.org/10.3390/s21041026
16. Schummer, P., del Rio, A., Serrano, J., Jimenez, D., Sánchez, G., & Llorente, Á. (2024). Machine learning-based network anomaly detection: Design, implementation, and evaluation. AI, 5(4), 2967–2983. https://doi.org/10.3390/ai5040143
17. Sharma, A., Rani, S., & Shabaz, M. (2025). Artificial intelligence-augmented smart grid architecture for cyber intrusion detection and mitigation in electric vehicle charging infrastructure. Scientific Reports, 15(1), 21653. https://doi.org/10.1038/s41598-025-04984-4
18. Sruk, V., Fajt, S., Krhen, M., & Olujić, V. (2025). Vehicle-as-a-sensor approach for urban track anomaly detection. Sensors, 25(21), 6679. https://doi.org/10.3390/s25216679
19. Thakur, S., Sarkar, N. I., & Yongchareon, S. (2025). AI-driven energy-efficient routing in IoT-based wireless sensor networks: A comprehensive review. Sensors, 25(24), 7408. https://doi.org/10.3390/s25247408
20. Vikas, Prasad, R., Upadhyay, S. K., & Kumar, A. (2025). Zero trust-driven anomaly detection framework for wireless sensor networks. International Journal of Performability Engineering, 21(8), 463–471. https://doi.org/10.23940/ijpe.25.08.p6.463471
21. Vuran, M. C., Akan, Ö. B., & Akyildiz, I. F. (2004). Spatio-temporal correlation: Theory and applications for wireless sensor networks. Computer Networks, 45(3), 245–259. https://doi.org/10.1016/j.comnet.2004.03.007
22. Wadibhasme, R. N., Chaudhari, A. U., Khobragade, P., Mehta, H. D., Agrawal, R., & Dhule, C. (2024). Detection and prevention of malicious activities in vulnerable network security using deep learning. In Proceedings of the International Conference on Innovations and Challenges in Emerging Technologies (ICICET) (pp. 1–6). IEEE. https://doi.org/10.1109/ICICET59348.2024.10616289
23. Wang, Z., Ye, M., Cheng, J., Zhu, C., & Wang, Y. (2025). An anomaly node detection method for wireless sensor networks based on deep metric learning with fusion of spatial–temporal features. Sensors, 25(10), 3033. https://doi.org/10.3390/s25103033
24. Wong, W. K., Baskar, S., Abubeker, K. M., & Ng, P. K. (2025). Sustainable cyber-physical VANETs with AI-driven anomaly detection and energy-efficient multi-criteria routing using machine learning algorithms. Scientific Reports, 15(1), 40068. https://doi.org/10.1038/s41598-025-28212-1
25. Yang, F., Shu, L., Yang, Y., Han, G., Pearson, S., & Li, K. (2021). Optimal deployment of solar insecticidal lamps over constrained locations in mixed-crop farmlands. IEEE Internet of Things Journal, 8(16), 13095–13114. https://doi.org/10.1109/JIOT.2021.3064043