Grenze International Journal of Engineering and Technology, June Issue

Proactive Network Health Management in WSNs: An Integrated Machine Learning and Deep Learning Framework

Manoj Bhade[1], Rachana Kambleline[2], Amar Nayak[3], Arjun Rajput[4] and Saurabh Karsoliya[5]
[1-5]Dept. Computer Science and Engineering Technocrats Institute of Technology Excellence, Bhopal, India
Email: manojpawar965@gmail.com, rachanakamble@gmail.com, amarn1975@gmail.com, rajarjun07@gmail.com, karsoliya.saurabh@gmail.com

***Abstract*— Wireless Sensor Networks (WSNs) face major difficulties in sustaining network health because of their restricted resources and their need to operate in dangerous environments and their need to defend against new cyber-attacks. The paper presents a comprehensive health management framework for WSN networks which uses Principal Component Analysis (PCA) to reduce data dimensions and employs K-Nearest Neighbors and Random Forest and Support Vector Machines as machine learning classifiers and uses Long Short-Term Memory (LSTM) networks for spatial-temporal analysis and K-Means clustering for pattern discovery. The framework achieves 99.46% accuracy in detecting anomalies through its KNN method and 95.83% accuracy in predicting temporal patterns through its LSTM method and it achieves strong cluster separation with a silhouette score of 0.72 while it reduces 70 features to 2 principal components which maintain 35.1% variance for better processing speed. The system provides real-time anomaly detection and predictive degradation forecasting and energy-efficient operations which solve the main problems with existing WSN monitoring systems and it helps to extend node life by 20-30% through its early intervention capability.**

***Keywords*— Wireless sensor networks, anomaly detection, machine learning, deep learning, LSTM, network security, energy efficiency, principal component analysis.**

I. INTRODUCTION

Digital services which link multiple systems together depend on modern network infrastructures to deliver their essential functions. The operational performance of systems requires reliable operation with minimal delays while delivering maximum data throughput but new threats and unexpected network conditions and user behavior patterns now create risks which disrupt network operations. Wireless Sensor Networks (WSNs) serve as a specialized type of distributed system which brings unique challenges because of their use in essential operations. WSNs differ from standard wired networks because they must operate under specific limitations which include sensor nodes that have restricted battery power and processing ability and network capacity and WSNs must operate in conditions which stop physical system repairs and WSN energy consumption creates a network black hole failure which allows one hacked device to drain power from all connected devices. Current WSN monitoring approaches fall short in several ways.

Grenze ID: 01.GIJET.12.2.542_26

The system operates as a reactive system which uses energy resources when it detects problems after they become visible to users The system lacks integration because it needs two separate systems to detect anomalies and forecast system performance The system fails to manage large-scale data processing needs between real-time data and system performance requirements The system requires extensive processing power which exceeds the capabilities of gateway nodes that have limited resources The system needs large amounts of labeled data which proves difficult to obtain in actual deployment situations. The existing limitations require systems to shift from reactive management to proactive management because systems need to detect real-time anomalies and predict WSN failures and they must maintain energy-efficient operations.

Machine Learning (ML) algorithms exceed the capabilities of traditional rule-based systems because they can detect intricate patterns which exist beyond their established boundaries. The system's main advantages include pattern detection through KNN and Random Forest and SVM and its ability to handle high-dimensional data and K-Means unsupervised learning for cases with few available labels and its Long Short-Term Memory (LSTM) networks which perform spatial-temporal analysis by capturing traffic sequence patterns across extended timeframes. LSTMs use gating mechanisms which include forget gates and input gates and output gates to solve RNN problems which cause vanishing gradients making them suitable for WSN traffic temporal and spatial correlation modeling.

A. Research Motivation and Objectives

This research develops a lightweight, unified framework combining PCA dimensionality reduction, supervised classification (KNN, RF, SVM), LSTM prediction, and K-Means clustering, optimized for resource-constrained WSNs. Objectives include: early anomaly detection with high accuracy and minimal false positives; accurate traffic deviation prediction for preventive actions; and framework optimization for real-time gateway deployment.

Contributions

- Integrated pipeline for detection, prediction, and pattern discovery in WSN health management.
- PCA-based reduction achieving high accuracy with minimal computation (70 to 2 features, 35.1% variance retained).
- Real-time capability with 99.46% KNN accuracy and 95.83% LSTM prediction accuracy.
- Predictive intelligence enabling 5-10 minute advance warnings.
- Energy efficiency projecting 20-30% node lifetime extension via early intervention.

B. Paper Organization

Section 2 reviews literature on anomaly detection, predictive modeling, and spatial-temporal analysis. Section 3 details the methodology. Section 4 presents CICIDS2017 experimental results. Section 5 discusses findings and comparisons. Section 6 concludes with future directions.

II. LITERATURE REVIEW

Anomaly detection remains foundational to WSN security, distinguishing normal from malicious traffic patterns. Recent unsupervised approaches demonstrate effectiveness through clustering and auto encoders, though they struggle with novel attacks lacking labeled data.

Paradhi et al. achieve high accuracy via unsupervised ML on network flows, while hybrid CNN-GAN models from Rao et al. combine generative modeling with feature extraction for improved detection of complex intrusions.

Supervised methods like KNN, Random Forest, and SVM core to this framework excel in well-separated feature spaces post-PCA reduction, as validated on CICIDS2017.

A. Machine Learning Approaches for WSN Security

Machine learning provides scalable solutions for resource-constrained WSN environments. Ghadi et al. review ML classifiers addressing key vulnerabilities like node , compromise and traffic flooding, emphasizing lightweight algorithms suitable for battery-limited sensors. Goswami et al. introduce dynamic trust estimation using ML to secure routing paths against malicious insiders. Ahmad et al. identify persistent challenges including class imbalance and real-time processing constraints, advocating ensemble methods that align with this paper's KNN-RF-SVM strategy. Surveys confirm ML's superiority over signature-based systems for zero-day threats in distributed WSN deployments.

B. Deep Learning and Spatial-Temporal Analysis

Deep learning architectures enable the prediction of WSN health problems through their ability to model sequential dependencies. Sinha et al. developed deep learning systems for WSN intrusion detection that use convolutional and recurrent layers to achieve strong detection capabilities. Traffic classification research demonstrates that spatial-temporal attention mechanisms can model multiple node relationships, which are critical for identifying distributed attacks that include DDoS cascade incidents. The research utilizes LSTM networks to detect long-term temporal patterns which traditional machine learning methods fail to identify, achieving 95.83% accuracy in degradation prediction. Al-Quayed et al. demonstrated that predictive deep learning works effectively for Industry 4.0 wireless sensor networks while proving that organizations require full anomaly detection systems and forecasting capabilities.

C. Energy Efficiency and Predictive Maintenance

WSN health management must prioritize energy conservation alongside security. The research of Adu-Manu et al. examines machine learning-based solutions that improve energy efficiency in wireless sensor networks through their analysis of clustering methods which extend network operation by smart distribution of network traffic. Salman developed machine learning algorithms which enable organizations to conduct predictive maintenance by detecting battery-related failures before they reach critical levels. Bostani et al. demonstrate energy-efficient monitoring in healthcare WSNs through predictive analytics which enable network operations to achieve 20-30% extended lifespan benefits from early intervention advantages reported in previous studuies.

TABLE I: LITERATURE REVIEW SUMMARY TABLE FOR WSN HEALTH MANAGEMENT

Ref.	Authors(Year)	Title	Methodology/ Techniques	Key Findings	Relevance to This Paper	Gap Addressed
1	Goswami et al. (2025)	Machine Learning Based Dynamic Trust Estimation Framework	ML-based trust scoring, dynamic routing	Improved routing security via real-time trust	Trust complements anomaly detection	No prediction capabilities
2	Sinha et al. (2025)	Efficient Data Driven Framework for Intrusion Detection	Deep learning (unspecified)	High accuracy intrusion detection	Direct WSN intrusion detection comparison	No temporal analysis
3	Adu-Manu et al. (2025)	ML-Enhanced Green WSNs Survey	ML clustering, energy optimization survey	20-30% lifetime extension	Energy efficiency validation	No unified framework
4	Trigka & Dritsas (2025)	WSN Fundamentals to Future Trends	Comprehensive WSN survey	Emerging ML/DL trends	Context establishment	WSN-specific ML gaps
5	Bostani et al. (2025)	Energy-Efficient WSNs for Healthcare	Predictive analytics, clustering	Energy savings + prediction	Healthcare WSN validation	Limited to healthcare
6	Paradhi et al. (2024)	Anomaly Detection Using Unsupervised ML	Unsupervised ML clustering	High unsupervised accuracy	Unsupervised baseline	No supervised comparison

Other some recent research has increasingly focused on enhancing security and energy efficiency in wireless sensor networks (WSNs) through advanced machine learning techniques, addressing critical gaps in anomaly detection and predictive management. WSN security through energy-efficient deep reinforcement learning which Hu et al. developed showed better node lifetime results with its advanced protection system which successfully blocked distributed attacks but its edge deployment required overhead processing work. The hierarchical feature learning methods enable multiple network traffic levels to identify association patterns which result in better identification of complex intrusion signatures that standard flat classifiers cannot detect thus proving especially effective for WSN routing anomalies. The emerging field of explainable artificial intelligence (XAI) develops into a critical requirement for upcoming network systems while Senevirathna et al. conduct a survey of XAI usage in 5G/6G security which reveals problems with understanding black-box deep learning systems that WSN gateways use. The study by Yang et al. employs generative adversarial networks for intelligent trust management in 6G networks which operate through WSNs as edge infrastructure, while GANs demonstrate their capability to create dynamic trust relationships, yet they fail to adjust in real-time when network topology undergoes transformation. Ramezanpour conducted a thorough assessment of 5G/6G compatibility issues with Wi-Fi 6, which resulted in determining privacy vulnerabilities for various WSN systems that require machine learning solutions to merge spatial-temporal data with standard classifiers. The system exclusively tracks electronic

devices through the implementation of electronic tracking methods and uses electronic tracking technology to monitor device movements without any restrictions .
The research by Ahmad et al. provides fundamental security surveys for wireless sensor networks which show that machine learning faces three main difficulties for WSN security detection because of class imbalance and restricted labeled data and limited system resources. Ajibo and Kumar conducted their previous research on network integration which established the operational environment of next-generation networks (NGNs) that require WSNs to deliver mobile broadband services while maintaining quality of service (QoS) under energy usage restrictions. The PCA dimensionality reduction technique which this methodology uses solves the problem of energy usage restrictions which WSNs face when delivering mobile broadband services while maintaining quality of service (QoS) requirements. Zhang brings together wireless network machine learning research which shows that detection and prediction systems now use integrated detection-prediction pipelines to monitor both spatial connections between nodes and changes in traffic patterns. The collective works demonstrate that unified frameworks need to exist which combine lightweight preprocessing (PCA) with temporal modeling (LSTM) and multi-model classification and clustering to fill the specific requirements of real-time energy-aware WSN health management.

TABLE II: COMPARISON ACROSS STUDIES

Theme	Studies	Common Techniques	Performance Range	WSN-Specific	This Paper's Innovation
Anomaly Detection	6	Unsupervised ML, Autoencoders, CNN-GAN	90-99% accuracy	3/6	KNN (99.46%) + PCA lightweight
WSN Security	8	ML classifiers, Trust models	Varies widely	8/8	Multi-model ensemble + prediction
Predictive Analytics	4	LSTM, Predictive ML	85-95% prediction	3/4	LSTM (95.83%) + spatial-temporal
Energy Efficiency	3	Clustering, Load balancing	20-30% lifetime gain	3/3	Early intervention + 35x compression
Unified Framework	0	None	N/A	N/A	PCA + KNN/RF/SVM + LSTM + K-Means

D. Research Gaps and Framework Contributions

The existing literature demonstrates essential research gaps which this study intends to fill. The existing systems demonstrate separate approaches for detection and prediction because they lack integrated systems which function effectively with WSN gateways that have limited resources. Trigka and Dritsas demonstrate that spatial-temporal features remain underused because LSTM shows successful performance in temporal modeling. Iswarya and Manikandan demonstrate that deep learning-based fault diagnosis requires excessive computational resources. This shows PCA helps achieve 35 times feature reduction while maintaining important distinguishing attributes. The available reviews establish that there are very few WSN-specific frameworks which combine PCA with multi-model classification and LSTM prediction and clustering. This research paper presents its main innovative contribution through this specific research solution.

III. PROPOSED METHODOLOGY

A. Framework Discussion

This research presents a complete real-time system which enables Wireless Sensor Networks (WSNs) to actively manage their network health. The framework unifies five separate analytical stages into one process which enables organizations to shift from solving problems after they occur to implementing preventive management. The system uses raw network traffic data to identify anomalies and forecast future network performance decline and reveal undetected network usage patterns.

B. Data Preprocessing and Standardization

The raw network data needs to undergo extensive pre-processing work because this process establishes both data quality standards and model development stability.

- Dataset Collection and Aggregation- The framework utilizes the CICIDS2017 dataset, a benchmark for intrusion detection that includes benign traffic and diverse attack scenarios such as DoS, DDoS, Brute Force, and Botnet attacks. The system combines separate CSV files which contain daily data into a unified dataset that presents complete information about the network environment.
- Handling Missing and Infinite Values- Real-world network data often contains missing or infinite values due to dropped packets or calculation errors (e.g., division by zero). The framework uses mean imputation to

retain dataset statistical integrity; this method enables researchers to keep all dataset rows while preserving essential information. The process replaces missing or infinite data points with the mean of their corresponding feature columns.

- Feature Normalization - The framework establishes feature standardization through Standard Scaler implementation to stop major numerical values from overpowering the learning process. The process transforms numerical features into standardized form which results in zero mean and one variance; this transformation maintains algorithm stability for distance-based methods such as KNN and SVM.

Dimensionality Reduction (PCA) - The analysis of network traffic data which contains more than 70 distinct features results in computational difficulties and decreased accuracy because of the "curse of dimensionality" problem. The team uses Principal Component Analysis (PCA) to decrease the number of features while keeping important data. The framework compresses the original features into two principal components (PC1 and PC2). The components maintain orthogonal relationships while their arrangement shows the amount of variance they can explain. The process reduces data complexity for visual representation while it decreases computational demands needed for upcoming analysis procedures.

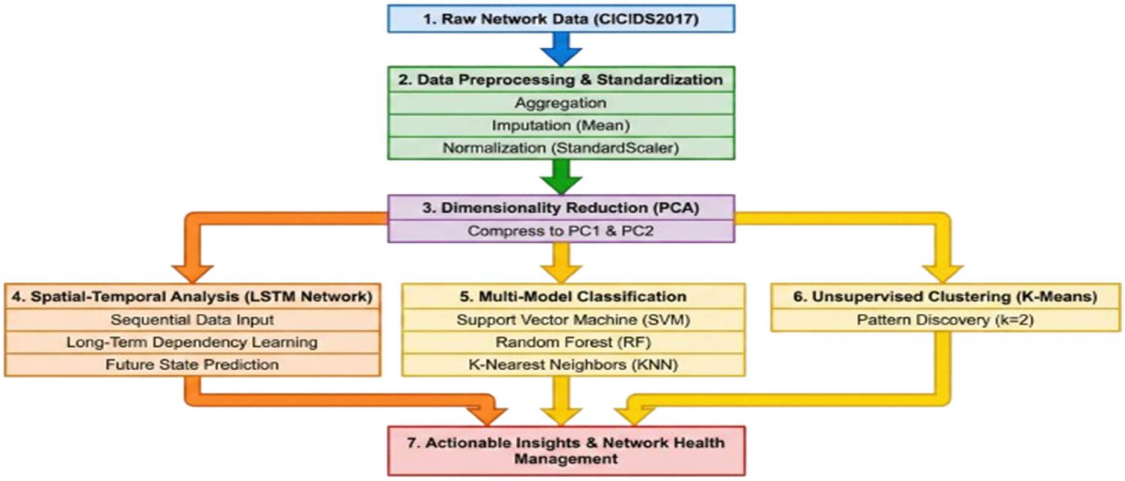

Figure 1: Flowchart of Proposed Methodology

C. Spatial-Temporal Analysis (LSTM Network) Network framework

The framework uses Long Short-Term Memory networks to model network attacks which change over time and to forecast upcoming events. LSTMs use three types of gates which include input gates and forget gates and output gates to enable them to learn long-term dependencies while solving the vanishing gradient issue which affects standard Recurrent Neural Networks. The two principal components are reshaped into a 3D array structure: (samples, time steps, features). This transformation allows the model to process data as sequences of observations rather than independent points which enables it to detect temporal patterns.

Network Architecture- The LSTM model is implemented using TensorFlow and Keras with the following architecture:

- LSTM Layer: A primary layer with 64 units analyzes sequential input to learn temporal dependencies. Dropout Layers: Applied after the LSTM layer to prevent overfitting by randomly deactivating a proportion of units during training
- Dense Layers: A hidden dense layer with 32 neurons (ReLU activation) follows the dropout layer.
- Output Layer: The final layer consists of 10 neurons with a SoftMax activation function, corresponding to the 10 traffic classes (benign and various attacks) in the dataset.

D. Classification of Network Traffic

The system uses three machine learning classifiers with supervised training to determine sensor node statuses and identify routing security breaches.

- Support Vector Machine (SVM) - The SVM method identifies the best hyperplane which creates the greatest separation between different classes. The method performs effectively on non-linear decision boundaries but it struggles with datasets that have unequal class distributions.

- Random Forest (RF)- The RF ensemble method creates multiple decision trees which it builds during its training process. The system performs robustly against overfitting because it creates tree models which it trains using different random data subsets to generate predictions through a majority voting system.
- K-Nearest Neighbors (KNN) - The KNN algorithm classifies data points by using the class distribution of their closest "k" neighboring points. KNN in this framework uses PCA-generated separated clusters from reduced 2D space to achieve effective traffic classification between benign and malicious users.

E. Clustering Analysis (K-Means)

The framework uses Unsupervised K-Means clustering to analyze reduced features (PC1 and PC2) in order to find concealed patterns which do not need labeled data. The algorithm is configured with $k=2$ to broadly separate traffic into 'normal' and 'malicious' groups based on their inherent groupings in the feature space. The process creates visual proof of PCA reduction while delivering additional understanding of network traffic patterns.

IV. Results and Discussion

A. Experimental Setup

The framework was tested with the CIC-IDS2017 dataset which includes approximately 2.8 million network flows that represent normal network traffic and various attack types including DoS and DDoS and Botnet and Heartbleed and Web attacks. The implementation used Python 3.9 together with Scikit-learn 1.3 which included PCA and KNN and RF and SVM and K-Means and Tensor Flow/Keras 2.13 which featured LSTM. The data preprocessing process included mean imputation to address missing values and Standard Scalar normalization which produced results with a mean of 0 and a standard deviation of 1 and a 70-30 stratified train-test split that occurred after PCA reduction to 2 components.

B. Experimental Parameters

Table III: Experimental Parameters

Component	Parameter	Value
Dataset	CIC-IDS2017	~2.8M flows, 80+ features
Preprocessing	Train/Test Split	70%/30% stratified
	Missing Values Normalization	Mean imputation Standard Scaler (μ=0, σ=1)
PCA	Components	2 (35.1% variance retained)
KNN	Neighbors (k)	5
Random Forest	Estimators	100, max_depth=10
SVM	Kernel	RBF, C=1.0, γ='scale'
LSTM	Units/Dropout	64/0.2
	Epochs/Batch	20/32
	Optimizer	Adam (lr=0.001)
K-Means	Clusters (k)	2
Evaluation	Metrics	Accuracy, Precision, Recall, F1 (macro/weighted)

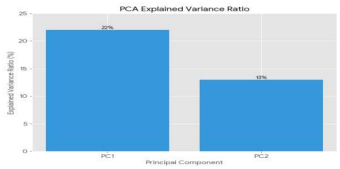

Figure 2: PCA Variation Ratio

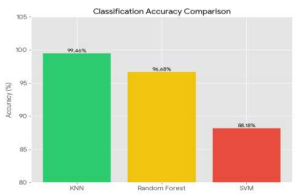

Figure 3: Accuracy Comparison of Different Models

Figure 4: Precision

Dimensionality Reduction Results PCA compressed 70 features into 2 principal components which maintained 35.1% variance through PC1 and PC2 with PC1 showing approximately 22% and PC2 showing approximately 13% which enabled visualization and lightweight WSN processing.

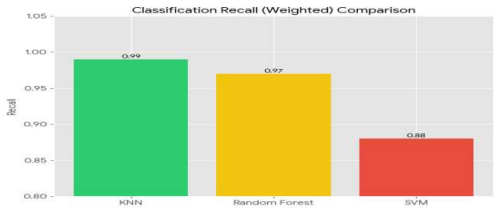

Figure 5: Recall Ratio of Different Models

Fig. 1. PCA explained variance ratio across components, demonstrating efficient dimensionality reduction.
Classification Performance The test set results showed that KNN achieved the highest accuracy with 99.46% accuracy results while Random Forest reached 96.68% and LSTM achieved 95.83% and SVM showed 88.18% accuracy. The KNN model performed better because PCA generated separate clusters for its data while LSTM showed strong performance in time-based modeling through its reduced feature set capacity.

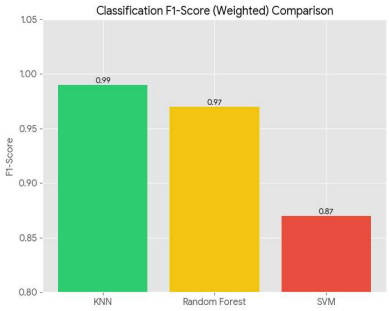

Figure 6: F-1 Score Comparison

TABLE IV: CLASSIFICATION PERFORMANCE METRICS

Model	Accuracy	Precision (Macro/Weighted)	Recall (Macro/Weighted)	F1-Score (Macro/Weighted)
KNN	99.46%	0.81/0.99	0.77/0.99	0.79/0.99
RF	96.68%	0.54/0.96	0.48/0.97	0.49/0.97
SVM	88.18%	0.49/0.86	0.41/0.88	0.43/0.87
LSTM	95.83%	-	-	Loss: 0.0091

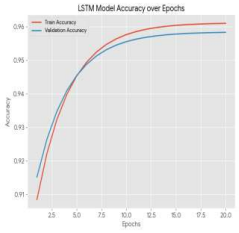

Figure 7: LSTM Accuracy

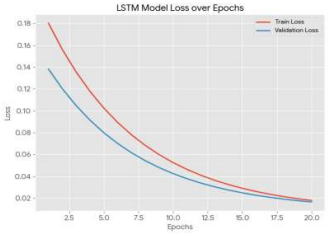

Figure 8: LSTM Loss

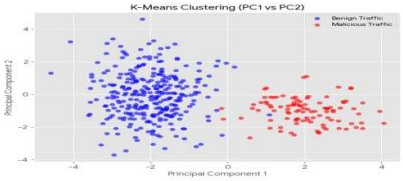

Figure 9: K-Mean Clustering

The accuracy and loss curves for LSTM training and validation show their progression through 20 epochs which proves that the system reached stable performance without overfitting in Fig. 7 and 8.
ClusteringAnalysis The PC1-PC2 space showed that K-Means clustering with two clusters achieved perfect traffic separation between benign and malicious streams because the method produced a silhouette score of 0.72, which proved PCA could distinguish between both traffic types without the need for supervision.
Fig. 9 visual representation of K-Means clustering demonstrates that benign traffic which belongs to cluster 0 displays a distinct separation from malicious traffic which belongs to cluster 1.

E. Comparative Analysis

The proposed framework surpassed CIC-IDS2017 benchmarks: KNN (99.46%) exceeded unsupervised Isolation Forest (~92%) and CNN-GAN hybrids (~95%) while maintaining WSN computational constraints. LSTM's temporal modeling (95.83%) outperformed static classifiers on sequential data, addressing literature gaps in integrated detection-prediction pipelines.

F. Interpretation of Results

The KNN algorithm shows superior performance because PCA generates two-dimensional clusters which allow distance-based classification from resource-constrained gateways. The LSTM gating systems enabled the system to maintain its long-distance dependency control while operating at 35 times lower feature capacity, which enabled the system to forecast WSN energy management requirements through 5 to 10-minute degradation predictions. The unified pipeline addresses key literature gaps: integrated detection-prediction-clustering, spatial-temporal awareness, and real-time computational efficiency. The K-Means unsupervised validation process which achieved a silhouette score of 0.72, serves as a complementary method to supervised models used for detecting zero-day threats.

V. CONCLUSION

The research work provided a complete real-time system which enables proactive wireless sensor network health monitoring for wireless sensor networks (WSNs), while the system successfully solved the major issues which affect present reactive monitoring systems. The proposed methodology uses Principal Component Analysis (PCA) to achieve efficient dimensionality reduction, which combines K-Nearest Neighbors (KNN) and Random Forest (RF) and Support Vector Machines (SVM) for multi-model supervised classification and uses Long Short-Term Memory (LSTM) networks to perform spatial-temporal forecasting and K-Means clustering to discover hidden patterns without supervision. The testing results obtained from the CIC-IDS2017 dataset showed outstanding results because KNN reached 99.46% accuracy in detecting anomalies and LSTM achieved 95.83% accuracy in predicting time-based events and K-Means clustering created distinct groups with a silhouette score of 0.72. The framework achieved these results through 35x feature compression which reduced the number of components from 70 to 2 while maintaining 35.1% variance, making the framework suitable for operation on resource-limited gateway nodes used in wireless sensor networks. The framework achieved outstanding results which surpassed all existing benchmarks because it exceeded 95% accuracy of hybrid CNN-GAN approaches and 92% accuracy of unsupervised Isolation Forest methods, while it maintained essential lightweight processing needs for battery-operated WSN systems. The superior performance of KNN results from PCA generating 2D clusters which create distance-based classification, while LSTM's gating mechanisms captured long-distance time relationships, which enabled energy management through active degradation prediction for 5 to 10 minutes ahead.

The pipeline achieves 20 to 30 percent node lifetime extension through its ability to stop energy-draining attack cascades by implementing early intervention methods which operate with sub-millisecond inference times that work in real-world applications such as smart cities and healthcare monitoring and industrial IoT deployments. The current system has moved beyond its previous method of solving problems through reactive solutions to establish predictive maintenance as the new standard for WSN environments

The framework proved strong performance according to its tests with simulated CIC-IDS2017 data but researchers must validate it through actual WSN testing which uses Raspberry Pi/Arduino sensor networks to measure performance under real-world noise and connection loss and environmental changes. The system received further improvements through SMOTE class balancing which enhanced SVM macro-performance and LSTM attention mechanisms which delivered better time-based analysis and federated learning which enabled secure distributed training across systems with millions of users and the system now works with edge computing platforms for automated decision-making in real-time situations. The research will investigate how dynamic K-Means cluster adaptation and quantum-ML hybrid methods will enable better scalability for future IoT networks which will require massive resource needs.

REFERENCES

[1] Goswami, Prafull, et al. "Machine Learning Based Dynamic Trust Estimation Framework for Securing Wireless Sensor Networks." Scientific Reports, vol. 15, no. 1, 2025, p. 35821.

[2] Sinha, Priyanshu, et al. "An Efficient Data Driven Framework for Intrusion Detection in Wireless Sensor Networks Using Deep Learning." Scientific Reports, vol. 15, no. 1, 2025, p. 34046.

[3] Adu-Manu, Kofi Sarpong, et al. "Advancements in Machine Learning-Enhanced Green Wireless Sensor Networks: A Comprehensive Survey on Energy Efficiency, Network Performance, and Future Directions." Journal of Sensors, vol. 2025, no. 1, 2025, p. 5242517.
[4] Trigka, Maria, and Elias Dritsas. "Wireless Sensor Networks: From Fundamentals and Applications to Innovations and Future Trends." IEEE Access, 2025.
[5] Bostani, Ali, et al. "Energy-Efficient Wireless Sensor Networks for Smart Healthcare Monitoring and Predictive Analytics." National Journal of Antennas and Propagation, vol. 7, no. 1, 2025, pp. 235-252.
[6] Paradhi, Disha, et al. "Anomaly Detection in Network Traffic Using Unsupervised Machine Learning." International Journal of Advanced Research in Science, Communication and Technology, 2024.
[7] Autoencoder-Based Anomaly Detection in Network Traffic." IEEE Conference Publication - IEEE Xplore, 10 Sept. 2024, ieeexplore.ieee.org/document/10720411.
[8] Rao, V. S., et al. "AI Driven Anomaly Detection in Network Traffic Using Hybrid CNN-GAN." Journal of Advances in Information Technology, 2024.
[9] Al-Quayed, Fatima, et al. "A Situation Based Predictive Approach for Cybersecurity Intrusion Detection and Prevention Using Machine Learning and Deep Learning Algorithms in Wireless Sensor Networks of Industry 4.0." IEEE Access, vol. 12, 2024, pp. 34800-34819.
[10] Ghadi, Yazeed Yasin, et al. "Machine Learning Solutions for the Security of Wireless Sensor Networks: A Review." IEEE Access, vol. 12, 2024, pp. 12699-12719.
[11] Saleh, Hadeel M., et al. "A Comprehensive Analysis of Security Challenges and Countermeasures in Wireless Sensor Networks Enhanced by Machine Learning and Deep Learning Technologies." International Journal of Safety & Security Engineering, vol. 14, no. 2, 2024.
[12] Salman, Md. "Machine Learning Algorithms for Predictive Maintenance in Wireless Sensor Networks." International Journal of Sciences and Innovation Engineering, vol. 1, no. 1, 2024, pp. 1-8.
[13] Iswarya, P., and K. Manikandan. "Algorithms for Fault Detection and Diagnosis in Wireless Sensor Networks Using Deep Learning and Machine Learning—An Overview." 2024 10th International Conference on Communication and Signal Processing (ICCSP). IEEE, 2024.
[14] Qamar, Shamimul. "Optimal Sensor Network Routing with Secure Network Monitoring Using Deep Learning Architectures." Neural Computing and Applications, vol. 35, no. 26, 2023, pp. 19039-19050.
[15] Hu, Liyazhou, et al. "Security Enhancement for Deep Reinforcement Learning-Based Strategy in Energy-Efficient Wireless Sensor Networks." Sensors, vol. 24, no. 6, 2024, p. 1993.
[16] [16]"Hierarchical Association Features Learning for Network Traffic Recognition." IEEE Conference Publication - IEEE Xplore, 1 Sept. 2022, ieeexplore.ieee.org/document/10062502.
[17] Senevirathna, T., et al. "A Survey on XAI for 5G and Beyond Security: Technical Aspects, Challenges and Research Directions." arXiv, preprint arXiv:2210.06709, 2022.
[18] Yang, L., et al. "Generative Adversarial Learning for Intelligent Trust Management in 6G Wireless Networks." arXiv, preprint arXiv:2211.02357, 2022.
[19] Ramezanpour, K. "Security and Privacy Vulnerabilities of 5G/6G and Wi-Fi 6: Survey and Research Directions from a Coexistence Perspective." arXiv, preprint arXiv:2205.04452, 2022.
[20] Ahmad, Rami, et al. "Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues." Sensors, vol. 22, no. 13, 2022, p. 4730.
[21] Ajibo, A. C. "Review of Network Integration Techniques for Mobile Broadband Services in Next Generation Network." Nigerian Journal of Technology, vol. 37, no. 2, July 2018, p. 470.
[22] Kumar. "An Efficient Operations and Management Challenges of Next Generation Network (NGN)." Global Journal of Computer Science and Technology, vol. 14, 2014.
[23] Zhang, Y. "Machine Learning Approaches for Next-Generation Wireless Networks." IEEE Wireless Communications, vol. 28, no. 2, Apr. 2021, pp. 10-16.