International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group | Volume 7 Issue 2 PP 246-252, 2026
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.IJERET-V7I2P130

Original Article

Data-Driven Intrusion Detection Techniques for Secure Wireless Sensor Networks Using Machine Learning

Dr. Neetu Sikarwar
Department of Electronice Engineering, Institute of Engineeeirng , Jiwaji University, Gwalior, India.

Received On: 10/04/2026 ***Revised On: 09/05/2026*** ***Accepted On: 17/05/2026*** ***Published On: 23/05/2026***

Abstract *- Denial of Service (DoS) attacks are a major concern for wireless sensor networks (WSNs), which are widely used in IoT-based real-time monitoring applications. In this paper, an intrusion detection framework based on data is proposed to secure communication in WSN using machine learning techniques. The WSN-DS dataset is used with LEACH protocol for Flooding, TDMA Scheduling, Blackhole and Grayhole attack detection. Prior to training the model, the dataset is subjected to data preparation methods such as encoding, normalization, balancing with SMOTE, and train–test splitting. Following their implementation, the Decision Tree and K-Nearest Neighbors (KNN) classifiers are assessed using several metrics such as accuracy (ACC), precision (PRE), recall (REC), F1-score (F1), ROC-AUC, confusion matrix, and SHAP analysis. It is clear from the experimental results that the KNN model (with an ACC rate of 99.39% and an F1-score of 99.38%) and the Decision Tree model (with a ROC-AUC of 99.43%) perform well in the intrusion detection task. The proposed models are compared with other existing methods such as CatBoost, Naïve Bayes, SVC, RF and D-GOPA, which have proved that the proposed models outperform the other methods in terms of detection ACC and classification reliability. The proposed framework considerably increases the efficiency of the security that can be provided for the network, the efficiency with which attacks can be detected and it offers an efficient solution for secure, intelligent applications of wireless sensor networks.*

Keywords *- Wireless Sensor Networks, Intrusion Detection System, Denial of Service (DoS) Attacks, Machine Learning, SHAP Analysis, LEACH Protocol*.

1. Introduction

Wireless sensor networks (WSNs) are a relatively new technology that has piqued scientist's interest for a number of potential uses [1][2][3]. WSN's versatility and ease of use have led to its expansion into other fields, including the military, healthcare, smart cities, environmental monitoring, and even everyday life [4][5]It all boils down to sensor nodes, which are tiny, spatially dispersed, auto-synchronous, and self-organizing components whose purpose is to monitor, collect data, and transmit it to base stations. One defining feature of WSNs is their susceptibility to various forms of attack [6].

There are two main categories of attacks that WSN encounter, though: active and passive [7]. While passive attacks take sensitive information like passwords and bank records, active attacks try to delete or corrupt data [8]. The goal of many active attacks known as DoS attacks is to disable or halt the services offered by WSN [9][10]. A WSN needs an IDS to keep an eye out for any suspicious or unexpected activity and trigger an alarm in the case of an intrusion [11][12]. This is because avoiding or preventing security risks, also known as attacks, is not always feasible. Specifically, wants to improve ability to identify and categorize four distinct forms of DoS attacks.

IDS in WSNs and IoT networks have been touted using a number of ML-based methods throughout the years [13][14]. By taking advantage of ML's pattern-learning capabilities, these methods outperform rule-based systems in automatically detecting anomalies and harmful actions [15]. Because of its capacity to detect irregularities and complicated patterns in network data automatically, ML has become an effective tool in intrusion detection systems [16]. ML models have the ability to learn from previous attack patterns and offer adaptable and dynamic solutions, allowing them to detect both known and unexpected threats [17]. Classifiers such as DT, RF, and Gradient Boosting are well-suited for WSN real-time threat detection due to their high ACC[18].

1.1. Motivation and Contributions of the Study

The growing adoption of WSN in IoT applications increases the need for secure and reliable communication. But WSNs are resource-limited and distributed, thus making them susceptible to DDOS and other cyber-attacks. Current IDS are not effective in detecting dynamic attack patterns. This study aims to improve the ACC of attack detection and network security in a WSN environment by designing a good intrusion detection system architecture. The study primarily focuses on enhancing secure WSN through improved data pretreatment, intrusion detection, performance evaluation, and comparison analysis.

- Develops a ML based intruder detection system for secure WSN.
- Implements the WSN-DS dataset with multiple DoS attack scenarios such as Flooding, TDMA Scheduling, Blackhole and Grayhole attack.
- Uses SMOTE to appropriately preprocess data by encoding and normalizing it, then splits it into train and test sets, and then balances it. This improves unit performance.

- Uses ACC, PRE, REC, F1, ROC-AUC, confusion matrix, and SHAP analysis as performance metrics to evaluate the suggested framework.
- Improves the security, attack detection and reliable communication of IoT-based wireless sensor network.

1.2. Justification and Novelty

WSN are expected to play a crucial role in the IoT applications, but the limited computational resources and susceptibility to DoS attacks have created substantial security challenges. Current intrusion detection techniques are prone to several limitations in dealing with imbalance attack data, in identifying a wide range of attack patterns and with interpretation of the features. This paper suggests a data-driven ID framework to overcome these drawbacks for WSN-DS data set to detect Flooding, TDMA Scheduling, Blackhole and Grayhole attacks. The suggested method is a hybrid strategy that improves IDS capabilities by combining data encoding, data normalization, data balancing with SMOTE, and systematic data pre-processing. Securing wireless sensor networks has never been easier than with this work's innovative architecture that combines balanced attack detection, explainable feature contribution analysis, and comparative intrusion categorization.

1.3. Structure of the Paper

The following is the outline of the paper: Section II covers the literature review and prior work on wireless sensor network intrusion detection; Section III lays out the methodology that used, including the framework for intrusion detection and dataset preprocessing; Section IV discusses the experimental results and performance comparisons; and Section V summarizes the study by pointing out the main findings, limitations, and areas for future research.

2. Literature Review

Cyberattack detection and wireless sensor network (WSN) security enhancement are addressed in this section through a discussion of ML-based intrusion detection methods and security measures. A. G and P. P. S (2026) proposed method to be competitive in detection ACC and FP with very low cost of computation. The suggested framework has a REC of 95.7, an ACC of 96.1 and a PRE of 95.6, a FP rate of 0.08 with a detection time of 0.02 s and a memory use of 12 MB, according to the experimental analysis of the NSL-KDD dataset [19].

M. V. Aasha Verghese (2025) approached is evaluated using MATLAB simulations across dense and sparse topologies under multiple node failure scenarios. Results showed a DR of 95.4%, a FPR of 3.2%, and an overall ACC of 96.8%, consistently outperforming statistical and learning-based baselines in dynamic WSN conditions [20]. K. V et al. (2025) presented a strategy to enhance detection PRE by utilizing a cross-correlation approach to glean the most pertinent attributes from the WSN-Shacking dataset. In order to reliably identify and categorize different forms of network intrusions, a customized DNN architecture is then trained with these enhanced features. With experimental findings showing a REC of 94.27%, a PRE of 96.41%, and an ACC of 95.84%, the suggested model is clearly effective [21].

N. A. Manzoor et al. (2025) implemented by Python software tool and performed efficiently obtain the results. The proposed system's findings are compared to those of the state-of-the-art. This study analyzes relevance of results and their future prognosis. This study introduces a proposed DCNN classifier that demonstrates an impressive ACC of 97.3% and a sensitivity of 92.4%, as determined through comparative analysis of the datasets [22]. S. Shukla et al. (2024) distributed learning approach is employed to update the intrusion detection system in real-time. A federated learning-based CNN-LSTM is trained on several local client nodes for real-time updates of the system. The NSL-KDD dataset is used for both centralized and distributed training. The suggested method achieved a remarkable 97.68% ACC with a negligible loss of 0.1568 [23].

R. Kalaivani et al. (2024) presented the POA for optimizing mobile secure routing in an IDS for WSN. POA, leveraging swarm intelligence, enhances network resilience through dynamic path optimization, effectively countering security risks. Numerical validation attests to POA 's, achieving an energy consumption of 0.08J and 12% of average energy Consumption 0.05J, alive node of 92% and Dead Node of 10% [24].

There is a lack of attention to class imbalance, interpretability, and computational complexity in resource-constrained contexts in the existing intrusion detection algorithms for WSNs, which primarily focus on enhancing detection effectiveness. On top of that, the majority of algorithms lack efficient pre-processing steps or analysis that compares various types of attacks. The capacity to properly identify and safeguard communications in WSN necessitates the presentation of an effective and understandable intrusion detection architecture. So, an efficient and interpretive intrusion detection system is essential for improving attack detection and safety of communications in WSNs, as summarized in Table 1.

Table 1: Literature Review of Intrusion Detection Techniques for Wireless Sensor Networks

Ref.	Author & Year	Method / Technique	Dataset	Key Findings	Limitations
[19]	A. G and P. P. S (2026)	Lightweight intrusion detection framework	NSL-KDD dataset	Achieved competitive intrusion detection with low computational cost and reduced false positives.	Limited evaluation on real-time WSN environments and diverse attack scenarios.
[20]	M. V. Aasha Verghese (2025)	MATLAB-based intrusion detection approach	Dense and sparse WSN topologies	Improved intrusion detection performance under multiple node failure scenarios.	Relies mainly on simulation-based evaluation with limited real-world deployment analysis.
[21]	K. V et al. (2025)	Cross-correlation feature extraction with DNN	WSN-Shacking dataset	Enhanced intrusion detection and attack classification using optimized feature selection.	Deep learning architecture increases computational complexity and resource consumption.
[22]	N. A. Manzoor et al. (2025)	DCNN-based intrusion detection model	Comparative dataset analysis using Python	Demonstrated effective intrusion detection capability and classification performance.	Limited explainability and interpretability of intrusion detection decisions.
[23]	S. Shukla et al. (2024)	Federated learning-based CNN-LSTM	NSL-KDD dataset	Enabled real-time distributed intrusion detection with improved learning performance.	High training complexity and communication overhead in distributed environments.
[24]	R. Kalaivani et al. (2024)	Pelican Optimization Algorithm (POA) for secure routing	Wireless Sensor Networks	Improved secure routing, network resilience, and energy efficiency.	Focuses mainly on routing optimization rather than comprehensive intrusion detection analysis.

3. Methodology

The methodology of the proposed intrusion detection system is presented in Fig. 1. The WSN-DS dataset, generated using the LEACH protocol, is collected and analyzed to identify multiple DoS attacks. The dataset undergoes preprocessing steps including encoding with OneHotEncoder, normalization with StandardScaler, balancing with SMOTE, and train–test splitting. Training and evaluation of DT and KNN classifiers for IDS follows. If wants to make sure that intrusion detection in WSNs is accurate and efficient, use metrics like REC, ACC, PRE, ROC-AUC, confusion matrix, and SHAP analysis to measure system performance.

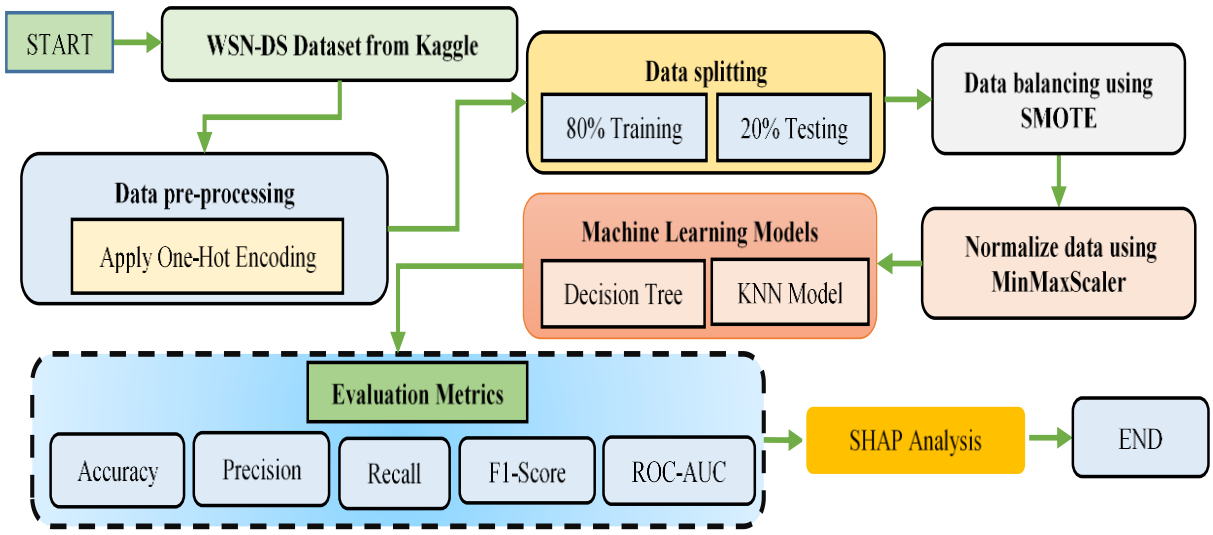

Fig 1: Flowchart of the Proposed Machine Learning-Based Intrusion Detection Framework for Wireless Sensor Networks

3.1. Data Collection and Analysis

The WSN-DS dataset using the LEACH method [25]. Flooding, Scheduling (TDMA), Blackhole, and Grayhole are the four kinds of denial-of-service attacks that may be more accurately detected and categorized using the dataset's abundance of attack scenarios and WSN characteristics. Among its 19 characteristics, there are 374,4661 records.

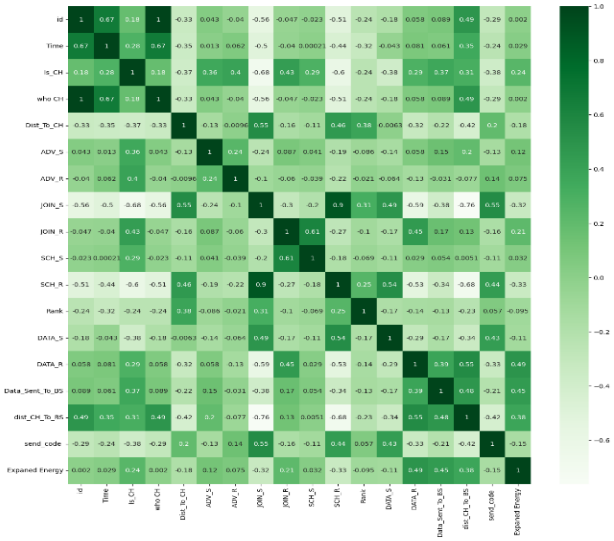

Fig 2: Correlation Matrix of Features for Intrusion Detection

Fig. 2 displays the network attribute correlation matrix used for intrusion detection in WSN. High correlations, such as those between j0/kG_s and dist_CH_to_BS (0.76), are clear indicators of relationships between attributes.

3.2. Data Preprocessing

In WSN, data preprocessing is essential for any IDS to be effective. Making sure the data is ready for ML models is a multi-step process. Here, dataset is subjected to the essential data preprocessing procedures.

3.3. Data Encoding using OneHotEncoder

In this step, label encoding is performed to convert non-numerical class labels into numerical values suitable for ML models. The One-Hot Encoder technique is applied to transform labels into numerical representations, enabling efficient processing and unbiased analysis during model training and evaluation.

3.4. Data Splitting

There is a training set that makes up 80% of the dataset and a testing set that makes up 20%. Each client receives an identically distributed 80% of the training data, and the global model is tested using the remaining 20% of the test set. This separation made it easier for the model to learn from the training set, and also allowed for a more objective assessment of its performance on the testing set.

3.5. Data Balancing using SMOTE

The SMOTE is a kind of oversampling that increases the amount of samples from the minority class by creating synthetic data from current samples and their neighbors. Class imbalance is effectively addressed by this approach, which also helps reduce the risk of overfitting caused by random oversampling methods.

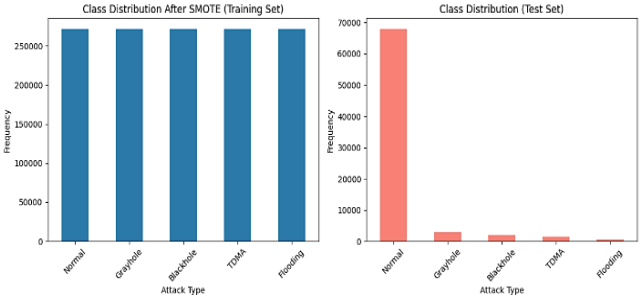

Fig 3: Class Distribution Before and After Applying SMOTE Technique

Fig 3 shows the distribution of classes after applying the technique SMOTE, where the training set is made balanced with around 27,000 examples for each class, whereas the testing data maintained its imbalance with around 68,000 instances of normal class.

3.6. Data Normalization using MinMaxScaler

Data normalization is a preprocessing method for improving within-range features. Data read from the CSV file, including its variance, mean, and standard deviation, impact learning efficiency. This model gets its 0 mean and 1 standard deviation from the input data by using StandardScaler from rooted in'sklearn. Using the Standard Scalar function from the 'Preprocessing' module, all datasets are normalized.

3.7. Machine Learning for Intrusion Detection Systems

ML models are trained for effective prediction and classification using labeled datasets in supervised learning. This research looks at the usage of DT and KNN algorithms to identify legitimate and malicious actions in WSNs.

3.7.1. Decision Tree

The DT is a very general tool that has many applications, such as pattern recognition, image processing and ML [26]. Root, branch, and leaf nodes are the fundamental building blocks of a DT. Partitioning the whole dataset into identical subsets forms the root node. Attribute combinations are represented by the branches, while the decision-making process is symbolized by the leaf nodes.

3.7.2. K-Nearest Neighbors

KNNs is a regression and nonparametric classification algorithm [27]. The technique finds the data point's k-nearest neighbors and utilizes their majority class as a criterion for classification. Incorporating it into a pattern recognition training dataset allows the classifier to be trained using its nearest neighbors. Consequently, only the top k nearest neighbors are considered in the classification.

3.8. Evaluation Metrics

ROC curves, PRE, REC, F1, inference time, and ACC are all widely used metrics to assess the performance of intrusion detection models. These metrics are computed using the

parameters of the confusion matrix: TP, TN, FP, and FN. TP and TN represent correctly detected attack and normal samples, respectively. FP and FN reflect cases that were misclassified. ACC is defined in Equation (1) as the proportion of correctly identified samples as a percentage of the total samples. Equation (2) defines PRE as the percentage of projected attacks that are accurate, while Equation (3) measures REC as the percentage of actual attacks that are accurate in identifying which samples were attacked. Equation (4) gives the F1, which is a balanced measure of model performance, as the harmonic mean of REC and PRE.

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \quad (1)$$

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

$$F1-Score = \frac{2*Precision+Recal}{Precision+Recall} (4)$$

4. Result Analysis and Discussion

The Intel Core i5-4210U CPU, 8.00 GB of RAM, 64-bit Windows OS, and 1.70 GHz processor are the specifications used to evaluate the proposed intrusion detection models. The DT and KNNs models' performance measures are displayed in Table II. These metrics include ACC, PRE, REC, F1, and ROC-AUC. While the DT model demonstrated superior ROC-AUC results (99.43%), the KNN model had the highest results in terms of ACC metrics (99.39%). Both models are shown to be effective and dependable for IDS.

Table 2: Performance Evaluation of Decision Tree and KNN Models for Intrusion Detection

Matrix	Decision Tree	KNN
Accuracy	0.9822	0.9939
Precision	0.9851	0.9938
Recall	0.9822	0.9939
F1-Score	0.9822	0.9938
ROC-AUC	0.9943	0.9926

WSN intrusion detection techniques KNN and DT both include confusion matrices, as shown in Fig. 4. In the case of the DT algorithm, 67,877 records of Class 3 and 1,941 records of Class 2 have been classified correctly, proving its capability to detect intrusions with zero misclassifications. Likewise, the KNN algorithm recorded 67,903 records and 2,786 records for classes 3 and 2, respectively.

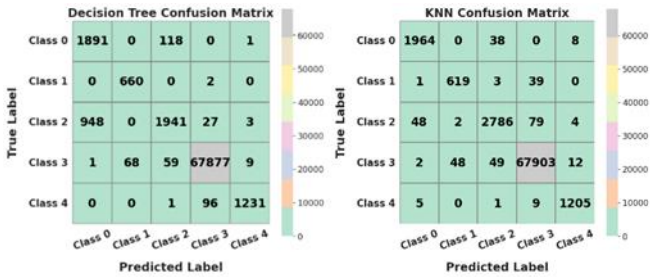

Fig 3: Confusion Matrices for Decision Tree and KNN-Based Intrusion Detection

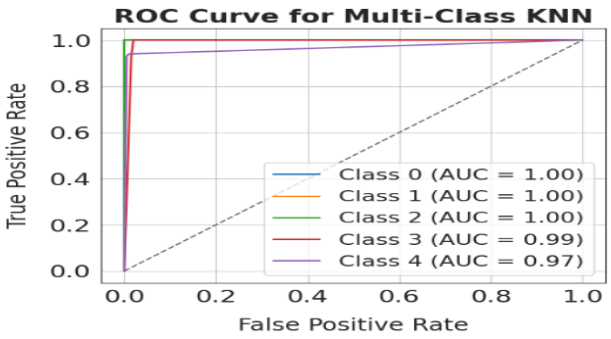

Fig 4: ROC Curve of Multi-Class KNN Classifier for Intrusion Detection

A multi-class KNN classifier was utilized to categorize intrusions in WSNs, and its ROC curves are displayed in Fig. 5. In terms of ACC, the multi-class KNN classifier gave excellent results since AUCs were 1.00 for Class 0, 1, and 2, 0.99 for Class 3, and 0.97 for Class 4.

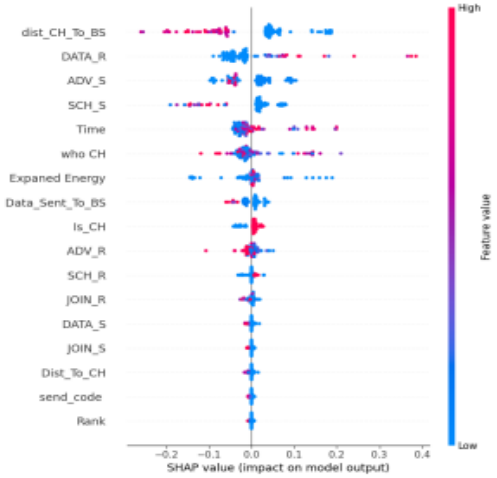

Fig 5: SHAP summary plot Analysis for Intrusion Detection

The influence of various network attributes on the intrusion detection system model is shown in Fig. 6, the SHAP summary figure. Dist CH TO BS, DATA R, and ADV S are three of the most crucial features for the model's prediction; their combined effect has a maximum SHAP value of 0.4.

4.1. Comparison and Discussion

The effectiveness of several ML techniques for detecting intrusions in WSNs is compared in Table III. The DT algorithm outperformed the competition with a 98.22% ACC rate, and KNN came in first with a 99.39% ACC rate and 99.38% F1. In contrast to the other algorithms, which include CatBoost, NBs, SVC, RF, and D-GOPA, the proposed models had better intrusion detection and classification capabilities.

Table 3: Comparative Performance Analysis of Machine Learning Models for Intrusion Detection in Wireless Sensor Networks

Model	Accuracy	Precision	Recall	F1-Score
Decision Tree	0.9822	0.9851	0.9822	0.9822
KNN	0.9939	0.9938	0.9939	0.9938
CatBoost [28]	0.9798	0.9803	0.9798	0.9798
Naïve Bayes [29]	0.9537	0.967	0.954	0.958
SVC[30]	0.902	-	-	-
RF[31]	0.94	0.94	0.85	0.88
D-GOPA[31]	0.96	0.96	0.96	0.96

Attacks on WSN were successfully detected using the DT and KNN algorithm models, which improved classification ACC. While the KNN model enhanced IDS through similarity learning, the DT offered clear and concise conclusions.

5. Conclusion and Future Scope

A growing number of applications rely on WSNs. The difficult problem of protecting WSNs using ML approaches, and more especially of reducing the impact of DoS attacks, is the focus of this research. For WSNs, the suggested intrusion detection system can spot Flooding, TDMA Scheduling, Blackhole, and Grayhole attacks. The framework integrates preprocessing methods such as encoding, normalization, and SMOTE-based balancing to enhance the ability of intrusion detection and classification. Based on the experimental analysis, the proposed approach achieves 99.39% ACC, 99.38% PRE, 99.39% REC and 99.38% F1, and obtains 99.43% ROC-AUC value, indicating the effectiveness of attack detection performance and secure network communication performance. The results of the comparative evaluation shows the effectiveness of the proposed approach on some alternative approaches in terms of the efficiency of intrusion detection and reliability. The study, however, only applies to the WSN-DS dataset and certain attack categories, which may limit its applicability in real-time large-scale WSNs and changing patterns of cyberattacks. There is scope to implement DL and hybrid intrusion detection methods in large scale real-time WSN environments in the future work. Advanced models such as LSTM, CNN, BiLSTM, Transformer, and federated learning and optimization algorithms can be combined to enhance the effectiveness of attack detection, scalability, energy efficiency, and adaptability to changing cyber threats.

References

[1] P. R. Chandre, P. Mahalle, and G. Shinde, "Intrusion prevention system using convolutional neural network for wireless sensor network," *IAES Int. J. Artif. Intell.*, vol. 11, no. 2, p. 504, Jun. 2022, doi: 10.11591/ijai.v11.i2.pp504-515.

[2] V. K. Sharma, "STRATEGIC FRAMEWORK FOR AI-ENHANCED PORTFOLIOS IN WIRELESS ENGINEERING: A LITERATURE REVIEW," *Int. J. Core Eng. Manag.*, vol. 8, no. 03, pp. 77–83, 2025.

[3] M. R. Anand and K. Abhilash, "Transforming Energy-Intensive Smart Factories with AI: TCN-based Forecasting and DQN-Driven Operational Optimization for Healthcare Manufacturing," in *International Conference on Intelligent Computing, Information and Control Systems (ICOIICS-2025)*, Nepal: IEEE, 2025, pp. 508–515, November. [Online]. Available: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=Wm2jcU0AAAAJ&citation_for_view=Wm2jcU0AAAAJ:zYLM7Y9cAGgC

[4] H. Fares, A. D. Vibhute, Y. Mouniane, and H. Bouijij, "Intrusion Detection in Wireless Sensor Networks using Machine Learning," *Procedia Comput. Sci.*, vol. 252, pp. 912–921, 2025, doi: 10.1016/j.procs.2025.01.052.

[5] B. F. More and S. Pawar, "Smart Home System using IoT and AI," *Int. J. Manag. Technol. Eng.*, vol. 8, no. 11, pp. 2241–2246, NOVEMBER, 2018, [Online]. Available: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=NlfrhQ4AAAAJ&citation_for_view=NlfrhQ4AAAAJ:u-x6o8ySG0sC

[6] M. Kari, "Intelligent Deep Learning-Based System for Improved Phishing Identification Accuracy in Web Platforms," in *2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON)*, IEEE, Mar. 2026, pp. 1–6. doi: 10.1109/I3CTCON68242.2026.11508030.

[7] S. Singh, "Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation," in *2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud)*, New York City, NY, USA: IEEE, 2025, pp. 1–6, November, December. doi: 10.1109/CSCloud66326.2025.00055.

[8] A. M. Arabiat and Y. G. Eljaafreh, "Intrusion Detection in Wireless Sensor Networks Using ML Based Classification of Denial of Service (DoS) Attacks," *J. Commun.*, pp. 501–514, Aug. 2025, doi: 10.12720/jcm.20.4.501-514.

[9] T. A. Khan *et al.*, "Multi-Source Cyber Intrusion Detection Using Ensemble Machine Learning," *J. Comput. Sci.*, vol. 21, no. 1, pp. 111–123, Jan. 2025, doi: 10.3844/jcssp.2025.111.123.

[10] M. Kumar and M. K. Shah, "AI-Driven DDoS Detection for Network Security: A Performance Analysis of Machine-Deep Learning Methods on Network Traffic Data," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, Houston, TX, USA: IEEE, 2026, pp. 1–6, February. doi: 10.1109/ICAIC67076.2026.11395710.

[11] V. K. Bollu, "Threat Landscape in Artificial Intelligence Systems: Taxonomy, Attack Vectors and Security Implications," *World J. Adv. Res. Rev.*, vol. 29, no. 1, pp. 285–294, January, 2026, doi:

https://doi.org/10.30574/wjarr.2026.29.1.0007.
[12] V. Sharma, "Zero Trust Architecture for 5G Networks," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 12, no. 6, Nov. 2024, doi: 10.37082/IJIRMPS.v12.i6.232707.
[13] M. Patel and U. Korat, "Swarm Optimization Algorithm-Enhanced Clustering Techniques for Reliable Wireless Sensor Networks Communication," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, Houston, TX, USA: IEEE, 2026, pp. 1–6, February. doi: 10.1109/ICAIC67076.2026.11395724.
[14] V. K. Sharma, "AI-Based Anomaly Detection for 5G Core and RAN Components," *Int. J. Sci. Res. Eng. Manag.*, vol. 6, no. 1, pp. 1–6, june, 2022, doi: 10.55041/IJSREM11453.
[15] D. P. Guda and C. Appani, "Graph Neural Networks for Dynamic Malware Behaviour Analysis and Classification in Advanced Persistent Threats (APT)," *Int. J. Commun. Networks Inf. Secur.*, vol. 14, no. 3, 2022.
[16] S. Singh, "Advancing Wireless Communications with Open Radio Access Network," in *2025 6th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, Tirunelveli, India: IEEE, Jul. 2025, pp. 682-687,. doi: 10.1109/ICDICI66477.2025.11135206.
[17] S. K. Sarangi, R. Lenka, J. Mishra, R. Sahu, and A. Nanda, *Malicious detection and trust calculation using residual recurrent neural network for trust with quality of service-aware multicast routing in mobile ad-hoc network system*, vol. 161. 2025. doi: https://doi.org/10.1016/j.engappai.2025.112130.
[18] D. Bhattacharjee, "Design and Evaluation of Deep Generative AI Model for Intrusion Detection in Cyber Threat Monitoring," in *2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, Mohali, Punjab, India: IEEE, 2025, pp. 1–6, December. doi: https://doi.org/10.1109/ISAECT68904.2025.11318752.
[19] A. G and P. P. S, "A Lightweight Entropy-Based CUSUM Framework for Intrusion Detection in WSN Environments," in *2026 World Conference on Computational Science and Technology (WcCST)*, IEEE, Mar. 2026, pp. 610–614. doi: 10.1109/WcCST67302.2026.11496167.
[20] M. V. Aasha Verghese, "Betti Number-Based Anomaly Detection for Intrusion Detection in Wireless Sensor Networks," *IEEE Sens. J.*, vol. 26, no. 3, pp. 5125–5132, Feb. 2026, doi: 10.1109/JSEN.2025.3640421.
[21] K. V, P. B, B. B. F, A. Govindaram, S. M, and N. Appavu, "AI-Driven Security Architecture for Wireless Sensor Networks Using Deep Learning," in *2025 IEEE 2nd International Conference for Women in Computing (InCoWoCo)*, IEEE, Nov. 2025, pp. 1–5. doi: 10.1109/InCoWoCo68239.2025.11407131.
[22] N. A. Manzoor, M. F. Akbar, and M. A. Prasanna, "Enhancing Intrusion Detection in Wireless Sensor Networks Using Deep Convolutional Neural Networks," in *International Conference on Smart Systems for Applications in Electrical Sciences, ICSSES 2025*, 2025. doi: 10.1109/ICSSES64899.2025.11009697.
[23] S. Shukla, A. S. Raghuvanshi, S. Majumder, and S. Singh, "FedHNN: A Federated Learning Based Hybrid Neural Network for Real-Time Intrusion Detection Systems," in *Proceedings - 2nd IEEE International Conference on Device Intelligence, Computing and Communication Technologies, DICCT 2024*, 2024. doi: 10.1109/DICCT61038.2024.10533096.
[24] R. Kalaivani, K. Aruna, S. Tamilarasan, and J. Jayapriya, "Pelican Optimization Algorithm for Mobile Secure Routing in Intrusion Detection Systesm in Wireless Sensor Networks," in *2nd IEEE International Conference on Data Science and Network Security, ICDSNS 2024*, 2024. doi: 10.1109/ICDSNS62112.2024.10690985.
[25] B. Kasasbeh, "WSN-DS," Kaggle.
[26] M. A. Talukder, S. Sharmin, M. A. Uddin, M. M. Islam, and S. Aryal, "MLSTL-WSN: machine learning-based intrusion detection using SMOTETomek in WSNs," *Int. J. Inf. Secur.*, 2024, doi: 10.1007/s10207-024-00833-z.
[27] A. John, I. F. Bin Isnin, S. Hamid Hussain Madni, and M. Faheem, "Intrusion detection in cluster-based wireless sensor networks: Current issues, opportunities and future research directions," *IET Wirel. Sens. Syst.*, vol. 14, no. 6, pp. 293–332, Dec. 2024, doi: 10.1049/wss2.12100.
[28] M. A. Talukder, M. Khalid, and N. Sultana, "A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction," *Sci. Rep.*, vol. 15, no. 1, p. 4617, Feb. 2025, doi: 10.1038/s41598-025-87028-1.
[29] D. Jeevaraj, B. Karthik, T. Vijayan, and M. Sriram, "Feature Selection Model using Naive Bayes ML Algorithm for WSN Intrusion Detection System," *Int. J. Electr. Comput. Eng. Syst.*, vol. 14, no. 2, pp. 179–185, Feb. 2023, doi: 10.32985/ijeces.14.2.7.
[30] G. Al Sukkar and S. Al-Sharaeh, "Enhancing Security in Wireless Sensor Networks: A Machine Learning-based DoS Attack Detection," *Eng. Technol. Appl. Sci. Res.*, vol. 15, no. 1, pp. 19712–19719, Feb. 2025, doi: 10.48084/etasr.7191.
[31] S. Ifzarne, H. Tabbaa, I. Hafidi, and N. Lamghari, "Anomaly Detection using Machine Learning Techniques in Wireless Sensor Networks," *J. Phys. Conf. Ser.*, vol. 1743, no. 1, Jan. 2021, doi: 10.1088/1742-6596/1743/1/012021.