International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 12 No. 1, 2026
https://theaspd.com/index.php

A Hybrid Framework Using CNN, DNN and RF for Intelligent Intrusion Detection in Wireless Sensor Networks

Ajay Kumar Mehta[1], Cheena Kaushal[2], Priyanka khatana[3], Shipra Khandelwal[4], Neha Solanki[5], Megha Garg[6], Bhupendra Meena[7]

[1,2,,3,4,5,6,7]*Department of Computer Science and Engineering, JECRC University, Jaipur, Rajasthan , India*

Email: ajaymehta7684@gmail.com[1], cheena.kaushal@jecrcu.edu.in[2], priyanka.khatana@jecrcu.edu.in[3], shiprakhandelwal.khandelwal@gmail.com4, neha.solanki@jecrcu.edu.in[5], megha.garg1@jecrcu.edu.in[6], bhupendra.meena@jecrcu.edu.in[7]

Abstract. *Wireless Sensor Networks (WSNs) are essential in a variety of applications, ranging from environmental monitoring to smart and connected cities to industrial automation and control. Given their resource-constrained nature and that WSNs can be deployed in a non-physical secure manner, they are particularly vulnerable to a host of cyber-attacks. Consequently, this study proposes A Hybrid CNN+DNN+RF Framework for Intelligent Intrusion Detection in Wireless Sensor Networks (WSN-DS). Our hybrid approach utilized the feature extraction capabilities of Convolutional Neural Networks (CNNs) and Deep Neural Networks (DNNs) to automatically extract the spatial and non-linear features from the WSN traffic data and subsequently classify these features using a Random Forest (RF) ensemble model to enhance accuracy, robustness, and interpretability. The system presented in this study was trained and assessed on WSN-DS training and test dataset which is the benchmark dataset for intrusion detection in WSNs. The experimental findings of this study show that the hybrid approach surpassed CNN, DNN, and conventional machine learning classifiers with regard to detection quality, along with statistically significant improvements in accuracy, precision, recall, and F1-score. In addition, the framework also achieves acceptable false positive rates, provides greater reliability, and is therefore well suited for implementation where resources are limited, especially for real-time intrusion detection systems in a WSN environment. This study demonstrates the promise of hybrid deep learning–ensemble methods to improve the reliable and secure operation of intelligent WSNs.*

Keywords: *Blockchain, Picture Passwords, Graphical Authentication, Visual-Chain, Cybersecurity, User Authentication.*

INTRODUCTION

Wireless Sensor Networks (WSNs) [1] have become an integral component of modern technological infrastructure, serving purposes from environmental monitoring, health care, and military surveillance, to smart cities. WSNs are widely employed yet can be extremely susceptible to an expanding range of cyberattacks - cyberattacks are possible due to some internal limitations of WSNs (open communication protocols, limited computing power and energy constraints). Thus, securing data transmission and maintaining reliable operation of networks to deliver services across WSNs remains challenging, while Intrusion Detection Systems (IDSs) represent a viable alternative to detect malicious activity and provide defense against intrusion [1]. While past IDS strategies have indicated malicious activity to a certain extent, they are challenged with obstacles associated with growing complexity of traffic within networks and the dynamic and evolvable nature of cyberattack strategies [2]. Dynamic WSN environments may benefit from deep learning strategies such as Convolutional Neural Networks (CNN) and Deep Neural Networks (DNN), as they are well advanced in extracting utility from numerous and high-dimensional variables. Further combining deep learning processes with ensemble learning may provide strong, generalizable performance for WSNs intrusion detection, as ensemble learning approaches greater resilience than on of its constituent parts [2].

The research presented and discussed in this study proposes a hybrid CNN+DNN+RF framework modeling that combines CNN and DNN to achieve automatic feature extraction for machine learning, and RF for final classification. The contributions of this research are summarized in three key points [3]. First, the proposed hybrid model resolves the challenges of employing either deep learning or traditional machine learning standalone, as the weaknesses of each method offset the strengths of the other. Second, the model provides high accuracy and low false positives, and improved robustness on WSN-DS benchmark dataset. Third, the hybrid framework offers a scalable and intelligent IDS framework (in the form of CNN+DNN+RF) that can be deployed in real-time WSN applications, thereby contributing to the development of secure and resilient wireless sensor networks [4].

The research presented in this thesis is important because it provides a practical and efficient intrusion detection system, which has been built as a result of combining deep learning and ensemble methods, any WSN environment. This work highlights an advancement of intrusion detection that will improve detection performance and improve the practicality of implementation in resource constrained environments. The hybrid framework represents the first step in changing the security landscape of WSN amid a relentless advancing realm of cyber threat.

1.1Objective of Research

Following are the research objectives:

- To develop a hybrid CNN+DNN+RF framework for intelligent intrusion detection in Wireless Sensor Networks.
- To obtain deep features from network traffic data using convolutional neural network and deep neural network models.
- To increase classification accuracy and robustness of the approach by utilizing Random Forest as the last classifier.
- To test the proposed model against the WSN-DS dataset using common classification performance metrics.
- To improve the security and reliability of Wireless Sensor Networks, via implementation of an efficient intrusion detection system.

By committing to these objectives, it will advance the technical basis for intelligent intrusion detection in Wireless Sensor Networks and narrow the divide between research experimental models and implementing these models into real-world environments. The authors hope that the nuances of these findings can ultimately lead to a more secure, efficient and reliable WSN infrastructure, assuming ongoing monitoring, system optimization, and adaption is maintained. Also, this study contributes to the opportunities of creating hybrid deep learning-ensemble methods into IDS design, and offers real-world directions to future researchers and practitioners in order to provide protective measures for WSN from continuously changing cyber threats.

2 LITERATURE REVIEW

S. Sriram et al. (2025) [5] introduced an event management system utilizing Sui blockchain technology that offers a more secure, efficient, and transparent event management system. In the Sui based event management system, the authors employed NFT based ticketing (to reduce fraud), zkLogin (privacy preserving authentication) and Worldcoin and Sui Wallet (low fee transactions). Using the PoS Sui Blockchain in the event management system creates increased decentralization of event services (no single point of failure), lower transaction fees, better transparency into ticket sales and distribution. This system can be utilized for events of any size, large and small. **C. Viji et al. (2025) [6],** illustrated how blockchain might be useful in library systems. Their research examined the potential usefulness of blockchain in complex types of interlibrary loan systems, digital rights management, and authentication of digital records. They also considered the ability of blockchain to provide tamper-proof provenance record for rare materials, and decentralized networks for resource sharing between libraries. They claimed that blockchain would give libraries additional data security, authenticity, and operational efficiency. **A. A. Abdellatif, et. al. (2025) [7]** architecture guarantees data integrity and confidentiality and supports parallel learning paradigms, including "centralized learning (CL), federated learning (FL), and active federated learning (AFL). The system identifies trusted participants, improves data collection, and adjusts blockchain parameters dynamically. Experiments performed on real datasets demonstrated enhanced scalability, security, and efficiency when learning compared to other existing techniques.

A. Mohajan& S. Jahan, (2025) [8] propose a blockchain-based Dynamic Access Control Scheme (DACS) to implement the principles of Zero Trust (ZT) in distributed systems. "The framework dynamically updates access control lists (ACLs) and enforces policies with smart contracts." A trust metric (TM) is assigned to every node and also behave dynamically whenever malicious activity occurs and is penalized. The Ethereum blockchain-based work validated the efficacy of the framework to protect distributed systems continuously monitoring and supporting risk-aware access control.
H. Arif et al. (2024) [9] commemorates how AI has taken over the space of cybersecurity, yet it also assesses the challenges of privacy, bias, and accountability, as well as developing policies dealing with AI and human capabilities. It's a review of practical applications, and it recommends ways to approach further research into the robust, adaptive defence of attacks. **K. D. O. Ofoegbu, et al. (2024) [10]** "Machine learning (ML) and big data analytics for real-time cyber threat detection: A scalable and accurate approach." "This paper provides real-life case studies of successful implementations in industry." Results:

The incorporation of ML and big data analytics within security comparisons a significant value addition, to be able to preemptively block threats.

3 RESEARCH METHODOLOGY

This project will develop and assess a hybrid CNN+DNN+RF framework for intelligent intrusion detection systems in WSN (Wireless Sensor Networks). The project initiates with the selection of the WSN-DS dataset [11], which consists of a labeled instance representation of normal and malicious traffic. Preprocessing steps included cleaning redundant attributes like timestamps and identifiers, encoding categorical labels into numbers, and normalizing the features to ensure uniform scale across features. The data cleaning procedures guaranteed consistency in data quality and reliable formatting to ensure deep learning models could be applied as intended [12].Data pre-processing was followed by reshaping the data to prepare it for submission to Convolutional Neural Networks, as shown in Fig 1.

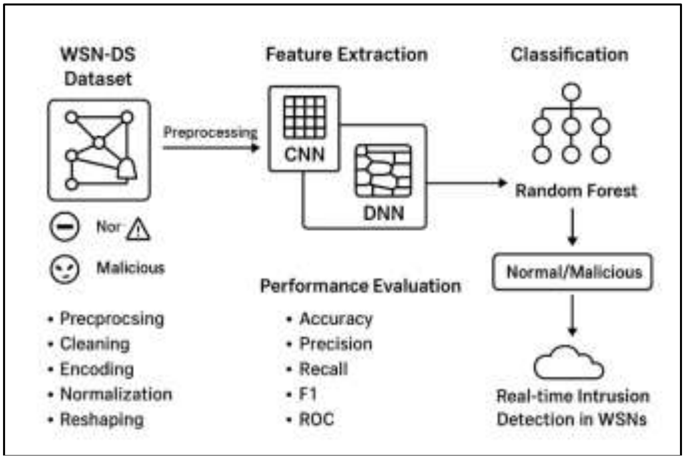

Fig 1. Flow diagram for Research

The CNN was used as part of the first stage of the framework to identify spatial dependencies and layered relationships in the data. The features extracted in the CNN [13] component were submitted to a Deep Neural Network (DNN) for further representation learning, and to account for the non-linearities present in network traffic as a complicated non-linear function. Rather than employing depth as an isolated decision-making mechanism, this research leveraged the advantages of ensemble learning mechanisms and incorporated a Random Forest (RF) classifier in a later stage of the framework. The Random Forest (RF) [14] classifier not only has robust characteristics, what it gains in efficiency and speed translates to interpretability, and the generalization capabilities benefit from combining predictions from many decision trees trained using the CNN and DL deep features.

Training and validation of the model used in this work was completed using a stratified train-test split to ensure all attack types were adequately represented for testing. The model training included tuning of the hyperparameters including batch size, dropout rate, and the number of estimators in the Random Forest, to yield optimal performance. Aspects of the proposed framework were evaluated using the measures of accuracy, precision, recall, F1-score, confusion matrix, ROC curves [15], and precision-recall curves. These measures provided a complete review of model performance, as well as performance per class, as it relates to the firm's ability to detect different types of attacks [16].

The selected approach blends the benefits of deep learning with those of ensemble machine learning (although there are many ways of combining these two approaches) to ensure that the proposed framework provides not only accurate predictions; but also scalable and flexible predictions for actual scenarios in WSN. By carefully blending CNNs, DNNs and RF, this approach ensures that the drawbacks of one method are offset by the complementary nature of another method, guiding us to a robust and intelligent intrusion detection system dedicated to the unique constraints faced in Wireless Sensor Networks[17].

4 PROPOSED WORK

4.1WSN-DS Dataset

The WSN-DS dataset [18] is specifically a benchmark dataset created to evaluate intrusion detection based techniques for Wireless Sensor Networks (WSN). The dataset contains labeled examples of normal and malicious traffic from realistic WSN scenarios, thus the dataset is suitable for training and evaluating detection models. The dataset contains examples of multiple attack types, and examples of normal traffic behavior, thus it is suitable for systematically developing and benchmarking machine learning and deep learning–based intrusion detection mechanisms.

4.2Convolutional Neural Networks (CNNs)

CNNs are deep learning model [19] class which are best known for their ability to extract spatial features and hierarchically layered representations from input data [19]. CNNs are best known for their use and deep learning advancements in the processing of images, but they are also useful for intrusion detection mechanisms because they extract local patterns (and their dependencies) through the pattern exploitation of network traffic data. CNNs automatically acquire features via convolutional layers, thus reliance on manual feature engineering is mitigated.

4.3Deep Neural Networks (DNNs)

DNNs [20] are multilayer feed-forward neural networks that can learn high dimensionality, multi-class, non-linear relationships in data. Explicitly, DNNs [20] consist of a number of hidden layers which contain neurons that generate transformations to inputs while representing progressively higher-level representations of inputs. In contrast to CNNs, DNNs can find and refine features and even identify deeper non-linear dependencies in network traffic, thus improving the accuracy and robustness of classifiers.

4.4Random Forest (RF)

A Random Forest [21] is an ensemble machine learning algorithm that creates many decision trees while training and combines the predictions from these trees for a final classification. In the Random Forest, every tree is trained on random subsets of data and features to promote generalization and reduce overfitting. RF is ideal for intrusion detection because of its high accuracy, interpretability, computational efficiency, and overall flexibility, making it an ideal candidate for classification of features extracted from more complex deep learning models within constraints commonly found in resource-limited environments such as WSNs.

Input: WSN-DS dataset $D = \{(x_i, y_i)\}_{i=1}^{N}$ where x_i are traffic features and $y_i \in$ {Normal,Attack}

Output: Predicted class $\hat{y}$ for new traffic instance

Step 1: Data Preprocessing

1. Remove redundant attributes (timestamps, IDs)
2. Encode categorical features into numeric values
3. Normalize features:

$$x_i{}' = \frac{x_i - \mu}{\sigma}$$

4. Reshape data for CNN input

Step 2: CNN Feature Extraction

1. Apply convolution operation:

$$h_{ij}^{(l)} = f\left(\sum_{m,n} x_{i+m,j+n}^{(l-1)} \cdot w_{mn}^{(l)} + b^{(l)}\right)$$

where f is ReLU activation.

2. Apply pooling to reduce dimensionality:

$$p_{ij}^{(l)} = \max_{m,n} h_{i+m,j+n}^{(l)}$$

Step 3: DNN Representation Learning

1. Flatten CNN output and pass through fully connected layers:

$$z^{(k)} = f\big(W^{(k)} h^{(k-1)} + b^{(k)}\big)$$

2. Use dropout to prevent overfitting:

$$z^{(k)} \sim \text{Bernoulli}(p) \odot f\big(W^{(k)} h^{(k-1)} + b^{(k)}\big)$$

Step 4: Random Forest Classification

1. Train multiple decision trees $T_1, T_2, \dots, T_M$ on feature subsets.
2. Each tree predicts class $\hat{y}_j = T_j(z)$.
3. Final classification by majority voting:

$$\hat{y} = \operatorname*{argmax}_{c \in C} \sum_{j=1}^{M} \mathbf{1}\left(T_j(z) = c\right)$$

Step 5: Performance Evaluation

1. Accuracy:

$$\text{Acc} = \frac{TP + TN}{TP + TN + FP + FN}$$

2. Precision:

$$\text{Prec} = \frac{TP}{TP + FP}$$

3. Recall:

$$\text{Rec} = \frac{TP}{TP + FN}$$

4. F1-score:

$$F1 = 2 \cdot \frac{\text{Prec} \cdot \text{Rec}}{\text{Prec} + \text{Rec}}$$

End of Algorithm

5 RESULT ANALYSIS

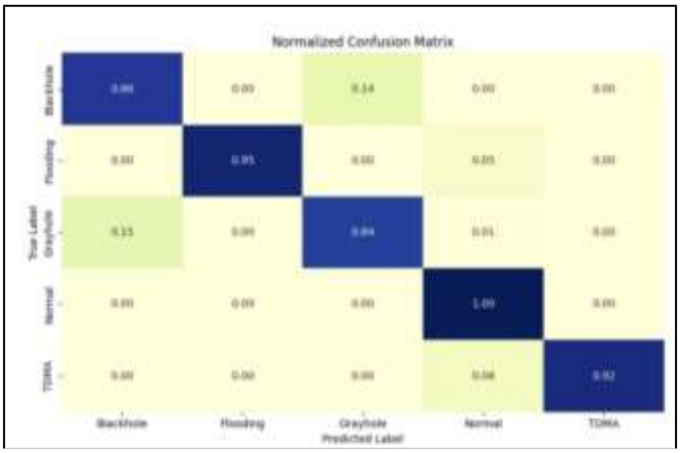

Fig 2. Normalized Confusion Matrix

The normalized confusion matrix in Fig 2. of the proposed CNN+DNN+RF hybrid framework, where it is focused on classification performance with respect to five attack classes: Blackhole, Flooding, Grayhole, Normal, and TDMA [22]. Diagonal values indicate correctly classified samples in a confusion matrix, while off-diagonal values indicate misclassifications. The model above exhibited significant detection rates of all classes respectively, with Normal (100%) and Flooding (95%) showing the highest, while Grayhole (84%) and Blackhole (86%) resulted in minor confusion with other attacks. The visual representation of the model data further demonstrated the minimization of misclassification errors across the samples identified in a wide range of WSN attack classes. For a correctly classified sample in a Non-Malicious attack, the model was able to minimize misclassification with Non-Ideal and TDMA attack models, resulting in significant performance accuracy for those classes.

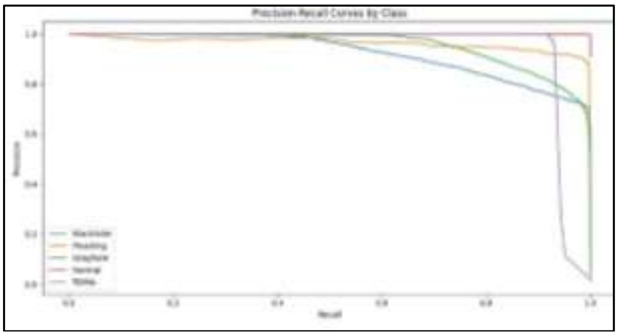

Fig 3. Classwise Precision-Recall Curves

This Fig 3.outlines the Precision-Recall (PR) curves of each attack class and normal traffic, demonstrating the dichotomy between precision and recall. The curves show very high precision across all classes with Normal and TDMA models almost having perfect performance. The Blackhole and Grayhole models had lower recall in some areas rather than precision, but still had good precision. These results provided confirmation of the strong capabilities of the model, showing remarkable strength on the false positives and very high levels of proficiency detecting the different classes of attacks in the WSN traffic.

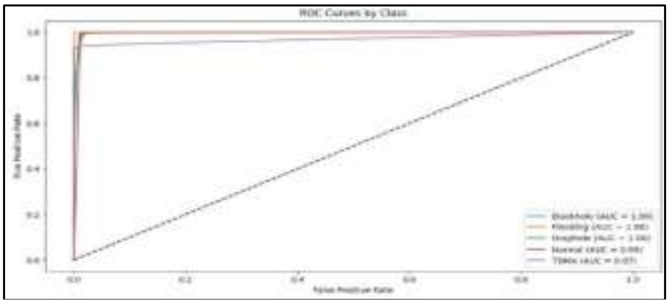

Fig4. Receiver Operating Characteristic Curves (ROC) by Class

This Fig 4. presents the Receiver Operating Characteristic (ROC) curves for each class, together with their respective Area Under the Curve (AUC) values. The curves show a great deal of separation ability, with Blackhole, Flooding, and Grayhole scoring perfect AUC = 1.0, Normal scored 0.99, and TDMA scored 0.97. Therefore, these results indicated the hybrid model has great discriminatory ability, where the near-one AUC values suggest the framework achieves greater detection capability across all types of traffic in WSNs.

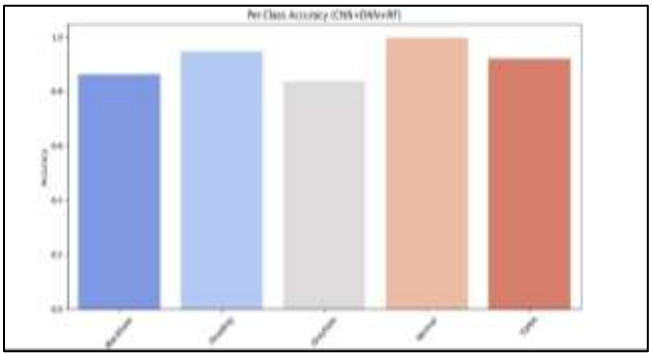

Fig 5. Per-Class Accuracy (CNN+DNN+RF)

Fig 5. shows the per-class accuracy rate of the hybrid CNN+DNN+RF framework across the five classes of traffic. Normal traffic achieved the highest accuracy (close to 1.0), Flooding traffic and TDMA traffic were the next best performing, while Grayhole traffic and Blackhole traffic were strong but comparatively lower in the accuracy statistic. This shows that while the system does very well detecting most of the attacks, attacks like Grayhole, which are more complex and subtle, likely need further and more advanced enhancements, as these attacks deserve more attention to increase detection success.

Table 1. Classification Report of CNN+DNN+RF Model on WSN-DS Dataset

Class	Precision	Recall	F1-Score	Support
Blackhole	0.71	0.81	0.76	2043
Flooding	0.90	1.00	0.95	631
Grayhole	0.84	0.76	0.80	2985
Normal	1.00	1.00	1.00	67,965
TDMA	0.99	0.93	0.96	1309
Accuracy			**0.98**	74,933
Macro Avg	0.89	0.90	0.89	74,933
Weighted Avg	0.98	0.98	0.98	74,933

The Classifier report shown in Table 1, clearly demonstrates that the Hybrid CNN+DNN+RF Framework excels for the WSN-DS dataset with an overall accuracy of 98% and a weighted average F1-score of 0.98. Since normal traffic accounts for >67,965 instances of data traffic and is the majority class of the WSN-DS dataset, it was classified perfectly with precision/ recall/ F1-score = 1.0, which confirms the model's ability to distinguish and classify legitimate data traffic vs. attacks. The attack classes of Flooding (F1 = 0.95) and TDMA (F1 = 0.96) may not exhibit perfect equivalent classification of the normal traffic, but they did exhibit significant precision and recall. The other two attacks (Blackhole - F1 = 0.76, Grayhole - F1 = 0.80) exhibited lower performance than the other two attacks reflecting some confusion as the attack traffic was non-existent (grayhole flooding) and was very close to the pattern of normal traffic, however, they certainly were classified between this spectrum as an attack. Overall, the macro-average scores of Precision = 0.89, Recall = 0.90, F1 = 0.89 firm decision that the framework presented solid balanced performance across the board and against the minority attacks as well. These results further reinforce that the hybrid approach deep learning - ensemble approach will prove successful within fielded WSN to protect against these attacks. It must be realized that if these attacks did evolve into real and evolving information frontier threats, that accuracy and robust performance must be a capability; neither can be compromised against both efficacy and accuracy of responses to threats in the field.

Table 2. Comparative Analysis of IDS Approaches on WSN-DS

Study	Methodology	Dataset	Overall Accuracy	Per-Class Performance	Key Strength	Limitation Compared to Proposed
Kasasbeh et al. (2023)	Sampling technique + ML classifiers	WSN-DS	95%	Not specified	Tackles class imbalance via sampling	Shallow ML → lacks deep/nonlinear feature learning
Talukder et al. (2024/2025)	MLSTL-WSN & hybrid ML approaches	WSN-DS	96%	Blackhole (46%), Flooding (63%), Grayhole (68%), Scheduling (86%), Normal (99%)	Introduces hybrid ML with task learning	Poor per-class detection, especially for severe attacks
Proposed Work (Hybrid CNN+DNN+RF)	CNN (spatial features) + DNN (nonlinear mapping) + RF (ensemble classification)	WSN-DS	98%	Balanced, improved recognition across all attack types	Combines deep learning + ensemble ML for robust detection	

The ideal Hybrid CNN+DNN+RF as shown in Table 2 ,evidently outscores Kasasbeh'ssampling+ML pipeline (95%) and Talukder's hybrid ML (96%) by achieving 98% accuracy whilst yielding improvements in minority-class attack detection. Kasasbeh's sampling approach helps with data balancing but cannot provide a deep representation of the data, while Talukder's system improves classifications soil, but resulted in worse rates for attack specific detection. The proposed hybrid framework draws upon the feature extraction from CNN+DNN algorithms and the ensemble robustness from the RF method to address these gaps, therefore making it the best candidate for implementation as a real-time IDS in WSNs.

6 CONCLUSION

This paper has proposed an advanced intrusion detection framework that integrates Convolutional Neural Networks (CNN), Deep Neural Networks (DNN), and Random Forest (RF). The integration finds anomalous activities in Wireless Sensor Networks (WSNs) using the WSN-DS dataset. The results from the experiments show that the applied proposed hybrid model captures excellent performance overall; resulting in an accuracy of 98% overall and a weighted F1-score of 0.98. The hybrid framework had outstanding reproduction when classifying Normal, Flooding, and TDMA classes to better identify unwanted attacks, while the precision and recall for the Blackhole and Greyhole attacks being lower has its challenges from their similar behavior to using normal network traffic. Consequently, Figures \ref{roc1} and \ref{pr1} confirmed that the system demonstrates reliability across all classes of attacks. In summary, this study shows how hybrid deep learning and ensemble methods can improve the accuracy of intrusion detection attacks, while still being friendly to adopt in resource-limited environments of WSNs.

Future Work

Although the proposed model provided good results, there are some areas for future research. First, the model must be further optimized because the performance on Blackhole and Grayhole attacks was relatively low. We could explore more feature engineering approaches, attention mechanisms, or transfer learning techniques to improve this.Second, although we used a benchmark dataset, further work must evaluate the framework with real-world WSN traffic. This aspect is critical to ensure the model can generalize well to outside deployments and is robust to work on diverse deployment scenarios. We could design lightweight versions of the model, for less computational or processing complexity. This is especially important when deploying such models on resource constrained WSN nodes. Another promising research area to explore is using explainable AI (XAI) approaches, where explanation methods would enhance the explainability or transparency of detection results to support trust properties in security-sensitive applications.Finally, we could explore extending the framework to detect zero-day attacks, or attack the framework with formulations or training for use in other IoT and edge-computing environments. These efforts will help substantiate the applicability of the framework for secure next-generation wireless networks.

Declaration:

Conflict of Interest

It is hereby declared that there is no conflict of interest

Funding Statement

It is hereby declared that there is no source of funding

Author Contribution

1st author drafted this manuscript, 2nd and 3rd author guided to draft the paper and reviewed the drafted paper.

And 4th ,5h, and 6th author also guided the 1st author in over all process of writing the manuscript , and helped in resource management. 7th author helped in grammatical editing of manuscript.

Data availability statement: Yes the dataset is taken from Kaggle

Research Involving human/animal: Not Applicable (It is dataset based paper so not such requirments)

Informed Consent: Not applicable(No consent required as free to use from kaggle)

References

1. N. Kumar, A. Sharma, and R. Kumari, “An efficient deep learning based solution for intrusion detection in wireless sensor networks,” *Evolutionary Intelligence*, 2023. [Online]. Available: https://doi.org/10.1007/s12065-023-00780-1
2. M. Alazab, M. Al-Qurishi, and A. Hossain, “EIDM: Enhanced Intrusion Detection Model for IoT using deep learning,” *The Journal of Supercomputing*, vol. 79, pp. 18337–18358, 2023. [Online]. Available: https://doi.org/10.1007/s11227-023-05197-0
3. R. Kale, R. S. Jadon, and S. Sharma, “Hybrid deep learning anomaly detection framework for network intrusion detection system,” *arXiv preprint arXiv:2212.00966*, 2022. [Online]. Available: https://arxiv.org/abs/2212.00966
4. M. Ghosh and R. K. Pal, “An intelligent and efficient network intrusion detection system using a novel stacked non-symmetric deep autoencoder,” *Computers & Electrical Engineering*, vol. 99, p. 107812, 2022. [Online]. Available: https://doi.org/10.1016/j.compeleceng.2022.107812
5. S. Sriram, P. R. Tharaniesh, P. Saraf, N. Vijayaraj, and T. Murugan, "Enhancing Digital Identity and Access Control in Event Management Systems Using Sui Blockchain," *IEEE Access*, 2025.
6. C. Viji, J. Jagannathan, N. Rajkumar, A. Mohanraj, B. Nachiappan, and J. A. J. Kovilpillai, "Leveraging Blockchain Technology to Enhance Library Security," in *Enhancing Security and Regulations in Libraries With Blockchain Technology*, IGI Global, pp. 181–200, 2025.
7. A. A. Abdellatif, K. Shaban, and A. Massoud, "Blockchain-enabled distributed learning for enhanced smart grid security and efficiency," *Computers and Electrical Engineering*, vol. 123, p. 110012, 2025.
8. A. Mohajan and S. Jahan, "Embedding Security Awareness into a Blockchain-Based Dynamic Access Control Framework for the Zero Trust Model in Distributed Systems," 2025.
9. H. Arif, A. Kumar, M. Fahad, and H. K. Hussain, "Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research," *International Journal of Multidisciplinary Sciences and Arts*, vol. 3, no. 1, pp. 242–251, 2024.
10. K. D. O. Ofoegbu, O. S. Osundare, C. S. Ike, O. G. Fakeyede, and A. B. Ige, "Real-Time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach," 2024.
11. S. O. Olabanji et al., "AI-driven cloud security: Examining the impact of user behavior analysis on threat detection," *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, 2024.
12. M. R. Labu and M. F. Ahammed, "Next-Generation cyber threat detection and mitigation strategies: a focus on artificial intelligence and machine learning," *Journal of Computer Science and Technology Studies*, vol. 6, no. 1, pp. 179–188, 2024.
13. S. Ismail, M. Nouman, D. W. Dawoud, and H. Reza, "Towards a lightweight security framework using blockchain and machine learning," *Blockchain: Research and Applications*, vol. 5, no. 1, p. 100174, 2024.
14. I. Shivhare and A. Majumdar, “A hybrid deep learning model for network intrusion detection,” *arXiv preprint arXiv:2306.07601*, 2023. [Online]. Available: https://arxiv.org/abs/2306.07601

15. H. Alavizadeh and M. Alazab, “A reinforcement learning approach for network intrusion detection using deep Q-learning,” *arXiv preprint arXiv:2111.13978*, 2021. [Online]. Available: https://arxiv.org/abs/2111.13978

16. I. Debicha, A. Ouali, and R. Ben Ayed, “Adversarial training for robust deep learning-based intrusion detection systems,” *arXiv preprint arXiv:2104.09852*, 2021. [Online]. Available: https://arxiv.org/abs/2104.09852

17. P. Wu, X. Zhang, and H. Wang, “LuNet: A CNN-RNN hierarchical model for intrusion detection,” *arXiv preprint arXiv:1909.10031*, 2019. [Online]. Available: https://arxiv.org/abs/1909.10031

18. H. Zhang, Y. Liu, and M. Li, “A deep adversarial learning framework for intrusion detection,” *arXiv preprint arXiv:1901.07949*, 2019. [Online]. Available: https://arxiv.org/abs/1901.07949

19. G. Fernandez and O. Baali, “A study on deep learning approaches for supervised and unsupervised network intrusion detection,” *arXiv preprint arXiv:1910.02203*, 2019. [Online]. Available: https://arxiv.org/abs/1910.02203

20. A. Alazab, M. Abawajy, and T. Islam, “Big data-driven intrusion detection using distributed deep learning,” *Journal of Big Data*, vol. 6, no. 1, p. 33, 2019. [Online]. Available: https://doi.org/10.1186/s40537-019-0248-6

21. Kasasbeh, B., Saifan, R., &Zaqout, I. (2023). *A novel sampling technique for detecting cyber denial-of-service attacks in wireless sensor networks*. In Proceedings of the 10th International Conference on Sensor Networks (SENSORNETS 2023) (pp. 69–76). SCITEPRESS.

22. Talukder, M. A., Kabir, M. N., Rahman, A., Haque, M. A., & Al Mamun, A. (2024). *MLSTL-WSN: A machine learning approach with self-training for intrusion detection in wireless sensor networks*. *International Journal of Information Security*, 23, 421–439. Springer.