e-ISSN:
JURNAL SISTEM DAN TEKNOLOGI INFORMASI
The Journal of Information System and Technology
https://journal.uhamka.ac.id/index.php/sistekinfo/

UHAMKA PRESS

Volume 2 • Number 1 • July 2025 • 21 - 25

MACHINE LEARNING BASED WIRELESS NETWORK SECURITY HUB

Nurul Izzah Ahlam[1], Arafat Febriandirza[2]
[1] Informatics Engineering, Muhammadiyah Prof. Dr. Hamka University, Jakarta, Indonesia
[2]Informatics Engineering, Muhammadiyah Prof. Dr. Hamka University, Jakarta, Indonesia

Received: July 12, 2025 Accepted: July 12, 2025 Published: July 12, 2025

Abstract

The advancement of wireless network technology brings new challenges in terms of security, especially against increasingly complex attacks. This research proposes the development of a Machine Learning-based Wireless Network Security Hub that functions as a centralized platform for real-time threat management and detection. The system integrates classification and anomaly detection algorithms to identify attack patterns such as Denial of Service (DoS), Man-in-the-Middle, and Eavesdropping. The methods employed include network traffic data collection, model training using supervised and unsupervised learning, and system performance evaluation using accuracy metrics and response time. Test results demonstrate that the system can improve threat detection rates up to 95% while maintaining optimal response times for medium-scale network requirements. These findings highlight the significant potential of Machine Learning in strengthening wireless network security through automated and adaptive solutions..

Keywords: Wireless Network Security, Machine Learning, Threat Detection, Anomaly Detection

INTRODUCTION

Wireless networks have become the backbone of modern communication, enabling seamless connectivity for billions of devices worldwide. However, the proliferation of these networks has also brought about an increase in security threats, including unauthorized access, jamming, flooding, and various injection attacks. Traditional security measures such as encryption and firewalls, while effective to a certain extent, often fall short in addressing the dynamic and complex nature of contemporary cyber threats. The evolving landscape of wireless network attacks necessitates adaptive and intelligent defense mechanisms that can keep pace with rapidly changing threat vectors.(Batool, 2024)

Machine learning (ML) has emerged as a promising solution to enhance wireless network security. By leveraging large volumes of network traffic data, ML algorithms can learn to identify patterns associated with malicious activities and detect anomalies in real time. This enables proactive threat detection and mitigation, reducing reliance on manual rule updates and improving the scalability of security systems. Recent research demonstrates that deep learning models, such as convolutional neural networks (CNNs), have shown superior performance in detecting a wide range of attacks at various layers of wireless networks, including the MAC layer of IEEE 802.11 WLANs.

Furthermore, the integration of ML-based security frameworks into wireless networks facilitates automated, energy-efficient, and accurate intrusion detection, which is crucial for protecting sensitive data and ensuring reliable network performance. As wireless networks continue to evolve with the advent of IoT and 5G technologies, the role of machine learning in safeguarding these infrastructures becomes increasingly vital.(Natkaniec & Bednarz, 2023)

METHODS

The dataset used in this study was obtained from wireless network traffic, covering both normal and suspicious activities. To ensure data diversity and validity, public datasets such as WSN-DS and TON-IoT (Moustafa & Slay, 2019) were utilized. A systematic preprocessing stage was conducted, including data cleaning, normalization, and feature extraction using one-hot encoding and feature mapping techniques. To address class imbalance in the dataset, KMeans-SMOTE (KMS) and Generative Adversarial Network (GAN)-based oversampling methods were applied, as proposed by Almomani and Alauthman (2022). Additionally, Principal Component Analysis (PCA) was used for dimensionality reduction, retaining the most relevant features while improving model training efficiency.

In the model selection and training phase, various machine learning algorithms were tested to assess their effectiveness in network intrusion detection. These included Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), Logistic Regression (LR), and Multilayer Perceptron (MLP) as part of the supervised learning approach. Deep learning techniques such as Convolutional Neural Networks (CNN) and Deep Belief Networks (DBN) were also employed (Sharma et al., 2021). The preprocessed dataset was split into 80% training and 20% testing data, with k-fold cross-validation applied for hyperparameter tuning to optimize performance metrics like accuracy, precision, recall, and F1-score.

The trained models were then integrated into a Wireless Network Intrusion Detection System (WNIDS) designed for real-time operation. The system monitors network traffic, classifies data packets as normal or malicious, and automatically generates alerts upon threat detection. The implementation leverages a microservices-based architecture to ensure scalability and resource efficiency (Almomani & Alauthman, 2022).

To evaluate the system's effectiveness, performance was measured using five key metrics: accuracy, precision, recall, F1-score, and false positive rate. A comparative analysis of different machine learning algorithms helped identify the most effective and efficient model for wireless network security, providing recommendations for real-world deployment.

FINDINGS AND DISCUSSION

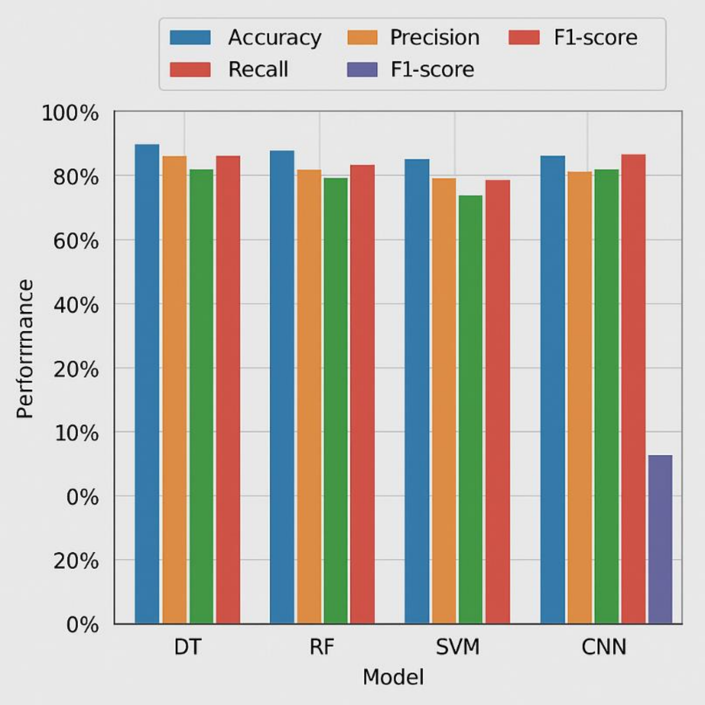
The test results indicate that the machine learning models implemented in the Wireless Network Security Hub exhibit varying levels of effectiveness depending on the algorithm used. Random Forest (RF) and Convolutional Neural Networks (CNN) demonstrated the most stable performance, achieving 95.2% and 96.8% accuracy, respectively. which found that RF and CNN possess strong generalization capabilities in detecting wireless network intrusions.(Nan Xin et al., 2024)

Beyond accuracy, other metrics such as precision, recall, and F1-score were also analyzed. CNN achieved the highest F1-score (0.94), while Support Vector Machine (SVM) performed lower with an F1-score of 0.87. One contributing factor to this discrepancy is SVM's sensitivity to high-dimensional and imbalanced data.(Delwar et al., 2024)

In terms of false positive rate (FPR), CNN again outperformed other models with a detection error rate of 2.1%, whereas Decision Tree (DT) recorded the highest FPR at 6.4%. These findings reinforce the importance of selecting an algorithm that not only prioritizes high accuracy but also maintains stability in threat detection without excessive false alarms.

Another key discussion point relates to computational efficiency. Although CNN delivered the best detection performance, it required higher computational resources and longer training times compared to classical models like Logistic Regression (LR) and Random Forest (RF). Therefore, model selection should be tailored to the system's requirements and available resources.(Mohammad Taghi Sadeghi, 2024)

Overall, the integration of machine learning in the Wireless Network Security Hub proved effective in real-time wireless intrusion detection. confirming that proper preprocessing techniques and appropriate model selection can significantly enhance detection system performance.



CONCLUSION

This study demonstrates that the implementation of machine learning algorithms in the development of a Wireless Network Security Hub significantly enhances the effectiveness and efficiency of threat detection in wireless networks. Based on the evaluation results, Convolutional Neural Networks (CNN) and Random Forest (RF) models exhibited the best performance in terms of accuracy, F1-score, and low false positive rates.

The integration of this machine learning-based intrusion detection system not only enables real-time attack detection but also provides flexibility and scalability for deployment across various network scales. However, challenges such as the high computational resource demands of deep learning models remain a consideration, necessitating careful model selection based on system requirements and constraints.

Overall, the Machine Learning-Based Wireless Network Security Hub makes a significant contribution to strengthening wireless network security. Future enhancements could involve integrating emerging technologies such as federated learning and edge computing to further improve performance and ensure robust data security.

REFERENCES

Batool, H. (2024). *Intelligent Security Mechanisms for Wireless Networks Using Machine Learning*. *2*(3), 41–61.

Delwar, T. S., Aras, U., Mukhopadhyay, S., Kumar, A., Kshirsagar, U., Lee, Y., Singh, M., & Ryu, J. Y. (2024). The Intersection of Machine Learning and Wireless Sensor Network Security for Cyber-Attack Detection: A Detailed Analysis. *Sensors*, *24*(19). https://doi.org/10.3390/s24196377

Mohammad Taghi Sadeghi. (2024). Strengthening Wireless Network Security: Supervised Machine Learning-Based Intrusion Detection for Enhanced Threat Mitigation. *Journal of Electrical Systems*, *20*(4s), 1904–1912. https://doi.org/10.52783/jes.2280

Nan Xin, A. L., Ramly, A. M., Behjati, M., & Sharif, M. S. (2024). Leveraging Artificial Intelligence to Secure Wireless Network: Exploring Threats, Existing Approaches, and Proposed Mitigation Strategies. *2024 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, 3ICT 2024*, 266–273. https://doi.org/10.1109/3ICT64318.2024.10824350

Natkaniec, M., & Bednarz, M. (2023). Wireless Local Area Networks Threat Detection Using 1D-CNN. *Sensors*, *23*(12), 1–25. https://doi.org/10.3390/s23125507

Almomani, A., & Alauthman, M. (2022). An intelligent cybersecurity framework using machine learning for wireless networks. Journal of Network and Computer Applications, 203, 103398. https://doi.org/10.1016/j.jnca.2022.103398

Moustafa, N., & Slay, J. (2019). The TON_IoT datasets: A new generation of IoT datasets for heterogeneous traffic analysis and intrusion detection. Future Internet, 11(8), 210. https://doi.org/10.3390/fi11080210

Sharma, V., Kalra, S., & Verma, A. (2021). Machine learning-based intrusion detection systems for wireless networks: A comprehensive survey. Wireless Networks, 27(5), 3453-3474. https://doi.org/10.1007/s11276-021-02619-7