International Journal of Creative and Open Research in Engineering and Management
ISSN: 3108-1754 (Online)
Volume 02 Issue 09 September-2026 | Impact Factor: 3.5

An Intelligent Network Intrusion Detection System Using Ensemble Machine Learning Techniques

R. Hanush Shandilya[1], D. Swetha[2]
[1] Assistant Professor, Department of IT & Cognitive Systems,
Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India
shandilyahanush@gmail.com

[2] Assistant Professor, Department of IT & Cognitive Systems,
Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India
Swethadevaraj26@gmail.com

How to Cite this Article:

Shandilya, R. H. & Swetha, D. (2026). An Intelligent Network Intrusion Detection System Using Ensemble Machine Learning Techniques. International Journal of Creative and Open Research in Engineering and Management, 02(9), 1-9. https://doi.org/10.55041/ijcope.v2i8.082

https://doi.org/10.55041/ijcope.v2i8.082

Abstract—

The increasing dependence on digital communication and internet-based services has made computer networks more vulnerable to cyber threats. Malicious activities such as denial-of-service attacks, port scanning, brute-force attempts, and unauthorized access continue to challenge the security of modern network infrastructures. Conventional intrusion detection techniques often rely on predefined signatures, making them less effective against newly emerging attack patterns. To address this limitation, this study proposes an intelligent network intrusion detection system based on ensemble machine learning techniques. The proposed approach combines multiple classification algorithms to improve the accuracy and reliability of intrusion detection while reducing false alarms. Network traffic data are analysed using selected features that represent normal and malicious behaviour, enabling the system to identify different categories of attacks efficiently. By integrating the strengths of multiple machine learning models, the proposed system achieves more consistent detection performance than individual classifiers. The study demonstrates that ensemble learning can significantly enhance network security and provides an effective framework for developing intelligent intrusion detection solutions suitable for real-world cybersecurity environments.

Keywords— Network Intrusion Detection System, Cybersecurity, Ensemble Machine Learning, Network Traffic Analysis, Random Forest, XGBoost, LightGBM, Attack Detection, Artificial Intelligence, Network Security. .

I. INTRODUCTION

The rapid expansion of digital technologies has transformed the way organizations communicate, store information, and deliver services. From financial institutions and healthcare organizations to educational institutions and government agencies, almost every sector depends on interconnected computer networks to support daily operations. While this digital transformation has improved efficiency and accessibility, it has also increased the number and complexity of cyber threats targeting network infrastructures. Cyber attackers continuously develop new techniques to exploit vulnerabilities in network systems. Attacks such as Distributed Denial-of-Service (DDoS), brute-force login attempts, port scanning, botnet activities, and malicious web traffic can disrupt services, compromise confidential information, and cause significant financial losses. As attack patterns evolve rapidly, organizations require intelligent security mechanisms capable of identifying both known and previously unseen threats.

Network Intrusion Detection Systems (NIDS) are designed to monitor network traffic and identify suspicious activities before they cause serious damage. Traditional intrusion detection systems primarily depend on signature-based detection, where incoming traffic is compared with a database of known attack signatures. Although this approach performs well for previously identified threats, it often fails to recognize new or modified attacks that do not match existing signatures. This limitation has encouraged researchers to explore machine learning techniques that can learn behavioural patterns from network data and identify anomalies more effectively.

Machine learning has become an important component of modern cybersecurity because of its ability to analyse large volumes of network traffic and automatically distinguish between legitimate and malicious behaviour. However, relying on a single machine learning algorithm may not always provide consistent performance across different attack categories. Individual models often have specific strengths and weaknesses, which can affect detection accuracy under varying network conditions.

Ensemble machine learning addresses this challenge by combining multiple classification algorithms to produce a more reliable prediction than any individual model. Instead of depending on a single classifier, the ensemble approach integrates the decisions of several learning algorithms, thereby improving detection accuracy, enhancing model stability, and reducing false positive rates. This collaborative decision-making process makes ensemble learning particularly suitable for complex cybersecurity applications where high detection performance is essential.

This research proposes an **Intelligent Network Intrusion Detection System using Ensemble Machine Learning Techniques** for identifying malicious network activities. The proposed framework employs multiple machine learning models to analyse network traffic and classify it into normal and attack categories. By leveraging the strengths of ensemble learning, the system aims to improve intrusion detection performance while maintaining high reliability in dynamic network environments. The outcome of this study is expected to contribute to the development of efficient and intelligent cybersecurity solutions capable of protecting modern network infrastructures against evolving cyber threats.

II.LITERATURE REVIEW

Recent advancements in Artificial Intelligence have Network intrusion detection has become an active area of research due to the rapid increase in cyber threats targeting modern computer networks. Traditional intrusion detection systems mainly rely on signature-based techniques, which perform well against known attacks but often fail to identify newly emerging or unknown threats. As a result, researchers have increasingly adopted machine learning methods to improve the accuracy and adaptability of intrusion detection systems.

Several studies have applied machine learning algorithms such as Decision Tree, Support Vector Machine (SVM), Random Forest, and XGBoost to classify network traffic as normal or malicious. These models have shown promising performance in detecting attacks such as DoS, DDoS, brute-force, and port scanning. However, the effectiveness of individual algorithms varies depending on the characteristics of the dataset and attack type.

To overcome these limitations, recent research has focused on ensemble learning techniques that combine multiple classifiers to improve prediction performance. Ensemble models generally achieve higher detection accuracy and lower false alarm rates by utilizing the strengths of different machine learning algorithms. They also provide better stability and generalization compared to single-model approaches.

Although existing studies have reported encouraging results, there is still a need for intrusion detection systems that provide high detection accuracy while maintaining low false positive rates. Therefore, this research proposes an **Intelligent Network Intrusion Detection System using Ensemble Machine Learning Techniques**, which integrates multiple classifiers to improve the overall performance and reliability of network attack detection.

III. PROPOSED METHODOLOGY

The proposed Intelligent Network Intrusion Detection System is designed to identify malicious network activities by applying an ensemble machine learning approach. The system analyses network traffic records, extracts relevant features, and classifies each network connection as either normal or malicious. The overall framework consists of data preprocessing, feature engineering, model training, ensemble classification, and performance evaluation.

A. Dataset Collection

The proposed model utilizes the **CIC-IDS2017** dataset, which is widely recognized for evaluating intrusion detection systems. The dataset contains both normal network traffic and multiple categories of cyberattacks, including Distributed Denial-of-Service (DDoS), Denial-of-Service (DoS), Port Scan, Brute Force, Botnet, and Web Attacks. The diversity of attack patterns makes the dataset suitable for training and testing machine learning models.

B. Data Preprocessing

Before training the models, the collected dataset undergoes preprocessing to improve data quality. Missing values and duplicate records are removed, while categorical attributes are converted into numerical values using appropriate encoding techniques. Feature scaling is also performed to normalize the dataset and improve the efficiency of machine learning algorithms.

C. Ensemble Machine Learning Model

The proposed intrusion detection system combines multiple machine learning algorithms through an ensemble learning strategy. Random Forest, XGBoost, and LightGBM are selected because of their ability to classify complex network traffic efficiently. A Voting Classifier integrates the predictions of these individual models to generate the final classification result. This collaborative decision-making process improves overall detection accuracy and reduces false positive rates compared with individual classifiers.

D. Performance Evaluation

The effectiveness of the proposed model is evaluated using standard classification metrics such as Accuracy, Precision, Recall, and F1-Score. These metrics provide a comprehensive assessment of the model's capability to distinguish between normal and malicious network traffic. The performance of the ensemble model is also compared with individual machine learning algorithms to demonstrate its effectiveness in intrusion detection.

IV. RESULTS AND DISCUSSION

The proposed ensemble machine learning model was evaluated using the selected network intrusion dataset after completing the preprocessing and training phases. The model's performance was assessed using standard classification metrics, including Accuracy, Precision, Recall, and F1-Score. These metrics provide insight into the model's ability to correctly distinguish between normal network traffic and malicious activities.

The ensemble model demonstrated improved classification performance compared to the individual machine learning models evaluated in this study. By combining the strengths of multiple classifiers, the proposed approach reduced misclassification and provided more consistent predictions across different categories of network attacks. This indicates that ensemble learning can improve the reliability of intrusion detection systems in practical network environments.

V. CONCLUSION

The proposed Intelligent Network Intrusion Detection System using Ensemble Machine Learning Techniques provides an effective approach for identifying malicious network activities. By combining multiple machine learning algorithms, the proposed model aims to improve detection accuracy and enhance the reliability of intrusion detection compared to conventional single-model approaches. The study highlights the importance of intelligent cybersecurity solutions in protecting modern computer networks from evolving cyber threats. The proposed framework can assist organizations in strengthening network security while supporting timely identification of suspicious activities.

Future Work

The proposed system can be further enhanced by integrating deep learning techniques for improved detection of complex attack patterns. Future work may also include real-time deployment in cloud environments, support for encrypted network traffic analysis, and the incorporation of explainable artificial intelligence (XAI) to improve the transparency and interpretability of intrusion detection decisions. Evaluating the model using additional benchmark datasets may further improve its robustness and practical applicability.

References

[1] G. Genuario, G. Santoro, and others, “Machine Learning-Based Methodologies for Cyber-Attacks and Network Traffic Monitoring: A Review,” *Information*, vol. 15, no. 11, 2024.

[2] A. Al-Sharif, “Enhancing Cloud Security: A Study on Ensemble Learning-Based Intrusion Detection Systems,” *IET Communications*, vol. 18, no. 15, pp. 1–16, 2024.

[3] S. M. Nzuva, “A Novel Bagging-XGBoost Ensemble Model for Attaining High Accuracy and Computational Efficiency in Network Intrusion Detection,” SSRN, 2024.

[4] Ismail Bibers, Osvaldo Arreche, and Mustafa Abdallah, “A Comprehensive Comparative Study of Individual ML Models and Ensemble Strategies for Network Intrusion Detection Systems,” 2024.

[5] M. Alamin Talukder, M. Manowarul Islam, and others, “Machine Learning-Based Network Intrusion Detection for Big and Imbalanced Data Using Oversampling, Stacking Feature Embedding and Feature Extraction,” 2024.

[6] “Effective Network Intrusion Detection Using Stacking-Based Ensemble Approach,” *International Journal of Information Security*, Springer, 2023.

[7] Z. Z. Lin, T. D. Pike, M. M. Bailey, and N. D. Bastian, “A Hypergraph-Based Machine Learning Ensemble Network Intrusion Detection System,” 2022.

[8] “Improving Network Intrusion Detection Performance: An Empirical Evaluation Using Extreme Gradient Boosting (XGBoost) with Recursive Feature Elimination,” *2024 IEEE International Conference on AI in Cybersecurity*, 2024.

[9] “Optimizing Network Intrusion Detection Systems Through Ensemble Learning and Feature Selection Using the CIC-IDS2017 Dataset,” *Informatica*, 2025.

[10] “Comparative Evaluation of Ensemble and Tree-Based Machine Learning Algorithms for Network Intrusion Detection,” *Journal of Electronic & Information Systems*, 2025

[11] “Two-Stage Ensemble Machine Learning for Network Intrusion Detection,” *International Journal of Engineering Trends and Technology*, 2026.

[12] “Network Intrusion Classification Using Machine Learning and Clustered Features,” *The Journal of Engineering*, 2026.