An Intelligent Hybrid Machine Learning and Deep Learning–Based Intrusion Detection System for DDoS and Botnet Attacks

Dr. Rengarajan A[1, 2], Dr. Jyoti Sekhar Banerjee[3, 4]

[1] Postdoctoral Scholar, Lincoln University College, Malaysia
[2] Professor, School of Computer Science and IT, Jain (Deemed-to-be) University, Bangalore, India
[3] Lincoln University College, Malaysia
[4] Techno Bengal Institute of Technology, Kolkata, India
Email ID: [1] pdf.rengarajan@lincoln.edu.my / [2] a.rengarajan@jainuniversity.ac.in / [3] pdfsv.jsbanerjee@lincoln.edu.my / [4] jyotisekhar.banerjee@bitcollege.in

Abstract

Intrusion Detection Systems (IDS) play a critical role in protecting modern networks from cyber threats. However, traditional signature-based IDS fail to detect unknown or polymorphic attacks, while anomaly-based approaches often generate high false-positive rates and struggle with scalability. To overcome these limitations, this study proposes an Intelligent Intrusion Detection System (IIDS) that integrates machine learning (ML) and deep learning (DL) techniques for effective detection of Distributed Denial-of-Service (DDoS) and botnet attacks.

The proposed framework employs a hybrid detection architecture combining supervised ML classifiers—Random Forest, Gradient Boosting, and Support Vector Machines—with deep learning models, including Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. Feature selection and dimensionality reduction are performed using Principal Component Analysis (PCA) and autoencoders to reduce noise and improve computational efficiency. The system is trained and evaluated using the CICIDS2017 benchmark dataset, supplemented with simulated attack traffic to enhance realism.

Experimental results demonstrate that the hybrid ensemble model outperforms individual ML and DL models, achieving higher detection accuracy and significantly lower false-positive rates. The IIDS achieves an average accuracy above 98%, with improved recall for low-rate DDoS and botnet traffic. Additionally, explainable AI techniques are incorporated to enhance interpretability and operational trust.

The results confirm that integrating ML and DL within a scalable and adaptive framework significantly improves intrusion detection performance, making the proposed IIDS suitable for real-time deployment in cloud and edge-based network environments.

Keywords

Intrusion Detection System, DDoS, Botnet, Machine Learning, Deep Learning, Network Security

1. Introduction

The primary contributions of this study are threefold. First, it presents a hybrid IDS architecture that effectively detects DDoS and botnet attacks with high accuracy and low false-positive rates. Second, it demonstrates the effectiveness of combining traditional ML and DL models with advanced feature engineering techniques on benchmark and simulated datasets. Third, it incorporates explainability and adaptive feedback mechanisms to bridge the gap between research-level models and practical deployment in cloud and edge computing environments.

2. Literature Survey

The rapid expansion of digital communication networks, cloud computing, and Internet-of-Things (IoT) infrastructures has significantly increased the complexity and scale of modern network environments.

While these advancements have enabled seamless connectivity and data exchange, they have also introduced new vulnerabilities that are increasingly exploited by cyber adversaries [1] [2].

Intrusion Detection Systems (IDS) are a fundamental component of network security architectures, designed to monitor network traffic and detect malicious activities. Traditional IDS approaches are broadly categorized into signature-based and anomaly-based systems [3]. Although they can detect unknown attacks, they often suffer from high false-positive rates, poor scalability, and difficulty in distinguishing between benign anomalies and genuine intrusions [4] [5].

Similarly, botnets exploit compromised devices to launch coordinated attacks that mimic legitimate traffic, further complicating detection. These challenges necessitate the development of more intelligent and scalable intrusion detection mechanisms [6]. However, ML models often rely heavily on handcrafted features and may struggle to capture complex temporal dependencies present in network traffic [7] [8].

Despite their advantages, DL models are computationally intensive and are often criticized for their lack of interpretability, which can hinder trust and adoption in real-world security operations [9] [10].

3. Methodology

3.1 System Architecture Overview

The proposed IIDS is designed as a multi-layered architecture consisting of five core layers: data collection, preprocessing, feature engineering, detection, and response and feedback. This modular design enhances scalability and allows seamless integration into high-throughput network environments such as cloud and edge infrastructures. Each layer performs a specific function while contributing to the overall detection accuracy and robustness of the system.

3.2 Data Collection Layer

The data collection layer serves as the foundation of the IIDS by acquiring raw network traffic from heterogeneous sources. Traffic data is captured from routers, firewalls, enterprise servers, cloud infrastructure logs, and IoT gateways. The collected data includes packet-level and flow-level information such as timestamps, protocol types, source and destination IP addresses, port numbers, packet sizes, and flow durations. Network traffic is stored in standardized formats such as PCAP files or NetFlow records.

To ensure scalability and real-time processing, the data ingestion process is designed to integrate with distributed streaming platforms such as Apache Kafka or Elasticsearch. This enables continuous monitoring of high-volume network traffic without packet loss, making the system suitable for real-world deployment scenarios.

3.3 Preprocessing Layer

Raw network traffic data often contains noise, redundancy, missing values, and inconsistencies that can negatively affect model performance. The preprocessing layer focuses on improving data quality through several steps. Duplicate packets and irrelevant flows are removed to reduce redundancy. Continuous numerical features, such as packet length and flow duration, are normalized using Min–Max scaling to ensure uniform feature ranges.

Missing values are handled through statistical imputation or removal, depending on their frequency and impact. Categorical features, including protocol types and TCP flags, are transformed using label encoding or one-hot encoding to make them compatible with machine learning algorithms. These preprocessing steps ensure that the dataset is clean, standardized, and suitable for effective feature extraction and model training.

3.4 Feature Engineering Layer

Feature engineering plays a crucial role in improving intrusion detection performance. This layer combines statistical feature selection with deep feature extraction techniques to generate a compact yet informative representation of network traffic. Initially, correlation-based filtering is applied to remove redundant features that exhibit weak relevance to intrusion classes or strong correlation with other features.

Principal Component Analysis (PCA) is then employed to reduce dimensionality while preserving maximum variance in the data. PCA significantly lowers computational complexity and improves model efficiency, particularly for large-scale datasets. In addition, autoencoder networks are trained to learn latent nonlinear representations of traffic patterns. These deep features capture subtle characteristics of malicious behavior that may not be evident in handcrafted features.

The final feature set combines essential statistical attributes, such as packet inter-arrival time, byte rate, and flow duration, with abstract features learned through autoencoders. This hybrid representation enhances the system's ability to detect both known and unknown attack patterns.

3.5 Detection Layer

The detection layer constitutes the core intelligence of the proposed IIDS. A hybrid detection strategy is employed, combining machine learning and deep learning models to leverage their complementary strengths.

Supervised machine learning classifiers, including Random Forest (RF), Gradient Boosting (GB), and Support Vector Machines (SVM), are trained using the engineered feature set. Random Forest provides robustness against noisy features through ensemble learning, while Gradient Boosting improves accuracy by sequentially minimizing classification errors. SVM is utilized for its effectiveness in modeling nonlinear decision boundaries.

In parallel, deep learning models are employed to capture spatial and temporal dependencies in network traffic. Convolutional Neural Networks (CNNs) are used to analyze structured traffic representations, such as flow-based feature matrices, enabling effective spatial feature extraction. Long Short-Term Memory (LSTM) networks are utilized to model sequential traffic behavior and temporal dependencies, which are critical for detecting slow-rate DDoS and botnet activities.

To enhance detection performance, a hybrid ensemble mechanism combines the predictions of ML and DL models using majority voting or weighted averaging. This ensemble approach reduces overfitting, balances precision and recall, and improves generalization across diverse attack scenarios.

3.6 Response and Feedback Layer

The response and feedback layer ensures that detection results lead to actionable outcomes. Upon identifying malicious traffic, the system generates alerts with severity levels to support timely incident response. To address the interpretability challenge of complex models, explainable AI (XAI) techniques such as SHAP and LIME are applied. These methods provide insights into feature contributions, enabling security analysts to understand and trust model decisions.

Furthermore, an adaptive feedback mechanism is incorporated to update model parameters using newly observed traffic patterns. This online learning capability enhances resilience against evolving and zero-day attacks by continuously refining the detection models.

3.7 Experimental Setup and Evaluation Metrics

The IIDS is evaluated using the CICIDS2017 benchmark dataset, which includes realistic normal and attack traffic, particularly DDoS and botnet scenarios. To improve generalization, additional simulated attack traffic is generated in controlled environments. The dataset is divided into training and testing sets to ensure unbiased evaluation.

4. Results and Analysis

This section presents the experimental results and performance analysis of the proposed Intelligent Intrusion Detection System (IIDS). The evaluation focuses on the system's ability to accurately detect DDoS and botnet attacks while maintaining a low false-positive rate. The performance of individual machine learning (ML) models, deep learning (DL) models, and the proposed hybrid ensemble is analyzed and compared.

4.1 Overall Detection Performance

The first set of experiments evaluates the classification performance of individual ML and DL models as well as the hybrid ensemble approach. Table 1 summarizes the results in terms of accuracy, precision, recall, and F1-score. These metrics collectively reflect detection effectiveness, robustness, and balance between false alarms and missed attacks.

Table 1: Performance Comparison of Detection Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	96.8	95.9	96.2	96.0
Gradient Boosting	97.4	96.8	97.1	97.0
SVM	95.6	94.3	95.0	94.6
CNN	97.9	97.2	97.6	97.4
LSTM	98.2	97.8	98.0	97.9
Hybrid Ensemble	**98.7**	**98.3**	**98.5**	**98.4**

The results indicate that deep learning models outperform traditional ML classifiers due to their ability to capture complex spatial and temporal patterns in network traffic. Among DL models, LSTM achieves superior recall, highlighting its effectiveness in detecting sequential and slow-rate attack behaviors. The proposed hybrid ensemble model achieves the highest overall performance, demonstrating that combining ML and DL predictions improves generalization and reduces misclassification.

4.2 False Positive Rate and Robustness Analysis

In practical intrusion detection systems, minimizing false positives is critical to avoid alert fatigue and unnecessary intervention. Table 2 presents the False Positive Rate (FPR) and AUC-ROC values for the evaluated models.

Table 2: False Positive Rate and AUC-ROC Comparison

Model	False Positive Rate (%)	AUC-ROC
Random Forest	3.4	0.971
Gradient Boosting	2.8	0.976
SVM	4.1	0.962
CNN	2.3	0.982
LSTM	1.9	0.986
Hybrid Ensemble	**1.4**	**0.991**

The hybrid ensemble model achieves the lowest false positive rate, indicating its ability to accurately distinguish between benign and malicious traffic. The high AUC-ROC value further confirms the model's strong discriminatory capability across varying decision thresholds. The reduction in false positives can be attributed to ensemble voting, which mitigates individual model biases and stabilizes predictions.

5. Conclusion

This research presented an Intelligent Intrusion Detection System (IIDS) that integrates machine learning and deep learning techniques to effectively detect Distributed Denial-of-Service (DDoS) and botnet attacks in modern network environments. Traditional intrusion detection approaches often struggle with evolving attack patterns, high false-positive rates, and scalability limitations. To address these challenges, the proposed framework adopts a hybrid architecture that combines statistical learning models with deep neural networks, supported by advanced feature engineering and explainability mechanisms.

Overall, the results confirm that intelligent hybrid intrusion detection systems offer a practical and scalable solution for defending against sophisticated cyber threats. Future work will focus on extending the framework to handle encrypted traffic, incorporating unsupervised and federated learning for privacy preservation, and deploying the system in real-time cloud and edge environments to further validate its effectiveness under dynamic network conditions.

References

1. A. Albulayhi, A. J. Alzahrani, and M. A. Khan, "A hybrid ensemble model for detecting DDoS attacks in cloud computing," *IEEE Access*, vol. 9, pp. 45174–45185, 2021.
2. S. Shafiq, M. S. Farooq, and M. A. Shah, "Comparative analysis of classification algorithms for DDoS detection in cloud environment," *IEEE Access*, vol. 8, pp. 134527–134539, 2020.
3. M. Adil, N. Javaid, and Z. Rehman, "Feature selection using statistical methods for botnet detection," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 1, pp. 105–116, Mar. 2021.
4. I. D. Thaseen and C. A. Kumar, "An efficient feature selection algorithm for network intrusion detection using PCA," *Comput. Electr. Eng.*, vol. 89, p. 106886, 2021.
5. R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Applying deep learning approaches for network traffic classification and intrusion detection," *ProcediaComput. Sci.*, vol. 132, pp. 1668–1677, 2020.
6. S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *J. Comput. Sci.*, vol. 25, pp. 152–160, 2020.
7. H. He, Y. Zeng, and J. Wang, "Real-time botnet detection using LSTM and traffic flow features," *IEEE Access*, vol. 8, pp. 217905–217915, 2020.
8. B. Sharma, M. Gupta, and A. Saxena, "DDoS attack detection using CNN in SDN," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 3, pp. 1475–1485, Sep. 2020.
9. Y. Wang, Y. Li, and X. Guo, "A transformer-based approach for network intrusion detection," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3276–3285, Mar. 2021.
10. A. Hafeez, M. A. Jan, and Y. Cao, "Autoencoder-based hybrid intrusion detection system in IoT," *IEEE Access*, vol. 8, pp. 119821–119829, 2020.