Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Cyber Sentinel AI: A Machine-Learning Framework for DDoS Detection Using Flow-Level Network Features

L.H.Patil[1], Aftab Ali[2], Adhisha Urkudkar[3], Hiteshri Gautam[4], Aniket Meshram[5], Danish Sheikh[6]

Abstract

Modern networks face increasingly sophisticated DDoS attacks that blend malicious traffic with legitimate flows, making detection difficult for traditional rule-based systems. This study introduces Cyber Sentinel AI, a machine-learning framework designed to classify network traffic by analysing structured features extracted from raw logs. The system converts IP addresses, ports, and protocol identifiers into numerical form, removes noise, and prepares a clean dataset suitable for model training. Supervised algorithms, particularly Random Forest and XGBoost, are trained on the CIC-DDoS2019 dataset to learn distinctive behavioural patterns separating normal and attack traffic. Experimental results show strong and stable performance, with accuracy typically ranging from 95 to 98 percent. Confusion-matrix analysis indicates minimal false alarms, while ROC curves and feature-importance scores highlight the relevance of IP- and port-based attributes in identifying malicious flows. The study demonstrates that ML models can capture subtle deviations in traffic behaviour more effectively than static security tools. The architecture is also flexible, enabling future real-time capabilities through streaming data pipelines, advanced anomaly detection models, and cloud-based deployment.

Keywords-Cybersecurity,Distributed Denial-of-Service(DDoS), Machine Learning, Network Traffic Analysis, Random Forest Classifier, Intrusion Detection System, Feature Engineering.

1. Introduction

The digital landscape is defined by the widespread growth of connected infrastructures, presenting unprecedented challenges for security professionals. This expansion has made systems vulnerable to sophisticated cyber threats. Among the most damaging attacks is the Distributed Denial-of-Service (DDoS), where adversaries overwhelm network resources to cause operational failure. The severity of DDoS attacks, coupled with their increasing frequency, necessitates urgent security innovation [1]. Traditional rule-based Intrusion Detection Systems (IDS), such as OSSEC and Snort, are frequently overwhelmed, resulting in high False Positive Rates (FPs) and limited scalability [4]. Critically, these legacy systems are ineffective against novel threats like Zero-Day Threats (ZDTs) [3]. The increasing sophistication of attack patterns demands intelligent detection systems capable of adapting to evolving threat behaviours in real time. The rapid development

of new attack vectors demands IDS based on behavioral anomaly detection, capable of identifying subtle deviations in network patterns [8]. To address this, the field has turned to Artificial Intelligence (AI) and Machine Learning (ML) [4]. Advanced models like parallel CNN-LSTM architectures have demonstrated near-perfect accuracy up to 99.99% in attack recognition [2]. Furthermore, specialized techniques like dual-autoencoders performing novelty detection are essential for countering ZDTs [3]. This paper presents Cyber Sentinel AI, a novel system focused on efficient real-time DDoS attack detection [13]. We investigate the performance of the foundational ML classifiers, Random Forest (RF) and Logistic Regression (LR), on current threat data. These models are trained using flow-level features from the definitive CIC-DDoS2019 dataset [2]. By validating these efficient algorithms, we aim to offer a scalable, accurate, and resource-effective solution for proactive cyber defense [4].

2. Literature Review

The imperative for robust IDS is driven by escalating network complexity and the failure of traditional signature-based systems against ZDTs [11].premier benchmark for contemporary DDoS detection due to its realistic nature [1]. Both Random Forest and Logistic Regression serve as powerful, validated classifiers in this domain:

1. Traditional Limits and ML Necessity

Traditional IDS are functionally restricted, exhibiting high FPRs and proving ineffective for large-scale network monitoring [4]. For instance, assessments of classic IDS solutions like OSSEC and Snort confirmed poor adaptability and scaling limitations [4]. The fundamental switch to AI/ML facilitates behavioral anomaly detection, vital for keeping pace with evolving adversary tactics [8]. Platforms capable of processing massive data volumes, such as Apache Spark, are now integral for effective ML-based detection [10].

Deep Learning and Advanced Tactics Advanced DL

methods offer superior feature extraction and recognition capabilities:

1. DDoS Recognition: Hybrid models combining MLP, RNN, and LSTM are widely researched for comprehensive DDoS classification [1]. The "Cybernet model" demonstrated breakthrough performance, achieving 99.76% accuracy for multi-class attack recognition on the CIC-DDoS2019 dataset [2].
2. ZDT Defense: Sophisticated methods address novel threats by explicitly modeling the underlying structure of network data. This includes Graph Neural Networks (GNNs) [9, 14] and dual-autoencoders that perform novelty detection after initial anomaly screening [3].
3. Real-Time Adaptivity: To maintain performance in streaming environments, models must be adaptive. Techniques like Adaptive Windowing (ADWIN) dynamically adjust the data scope to counter concept drift [5], while the Robust Random Cut Forest (RRCF) effectively identifies local anomalies in streams [6].

3. Validation of Project Models

The CIC-DDoS2019 dataset stands as the premier benchmark for contemporary DDoS detection due to its realistic nature [1]. Both Random Forest and Logistic Regression serve as powerful, validated classifiers in this domain:

4. Logistic Regression is recognized for its operational efficiency, speed, and interpretability [10]. Studies have shown LR achieving accuracies up to 92% on standardized datasets [4].
5. Random Forest (RF), an ensemble model, is favored for its robustness against overfitting, superior generalization, and high accuracy [13]. RF has consistently

achieved superior results compared to simple classifiers in intrusion detection testing [13].

The application of Random Forest and Logistic Regression on the CIC-DDoS2019 dataset in this work establishes a high-performance, resource-efficient foundation for a real-time IDS.

4. Materials And Methods

This section describes the datasets, computational resources, preprocessing pipeline, feature engineering steps, model-training procedure, and evaluation methods used in developing Cyber Sentinel AI. All steps are documented to allow full reproducibility.

5. Materials

Dataset

The study utilized structured network traffic logs derived from the **CIC-DDoS2019 dataset**. Raw logs were stored in CSV format, where each row consisted of a single concatenated string:

srcIP-dstIP-srcPort-dstPort-protocol
Example:
192.168.10.5-104.16.207.165-54865-443-6

Each entry contained the following attributes: Source I, Destination IP, Source Port, Destination Port, Transport Protocol. These fields served as the core flow-level.

where a, b, c, and d represent the four octets of the IP address.

Hardware Environment

All experiments were conducted on a standard workstation:

Processor: Intel/AMD CPU

Memory: 8 GB RAM, **Operating Environment:** Python 3.10 (Anaconda Environment) The hardware configuration ensures the model can be deployed easily, even in low-resource environments such as enterprise gateways.

Software and Tools

The implementation was developed using the following software stack: Python 3.x, pandas, numpy → Data manipulation, scikit-learn → Model training and evaluation, matplotlib → Visualization, joblib → Model serialization

A set of custom modules was implemented for the system, including preprocess.py for data cleaning and IP conversion, data_loader.py for structured data access, train_model.py for model training and evaluation, and visualize_results.py for generating plots and analytical visualizations.

6. Methods

Data Preprocessing

All preprocessing steps were automated through the script preprocess.py.
The following operations were applied:

a. Raw Log Extraction

Each log string extracting: src_ip, dst_ip, src_port, dst_port, protocol

Malformed or incomplete logs were discarded.

b. Numerical Conversion of IP Addresses

Each IP (a.b.c.d) was converted to a unique integer using the deterministic formula:

1. IP Conversion Equation

   IP_numeric = $a\times256^3 + b\times256^2 + c\times256 + d$ Provided a reusable function to load: Raw logs, processed data, Model outputs, Ensured modularity in the project.

2. Random Forest Gini

   $G=1-\sum_{i=1}^{C} p_i^2$ G = 1 - \sum_{i=1}^{C} p_i^2G=1−i=1∑Cpi2

3. Logistic Regression

   $h(x)=\frac{1}{1 + e^{-\theta^T x}}$h(x) = \frac{1}{1 + e^{-\theta^T x}}h(x)=1+e−θTx1

4. Evaluation Metrics

Accuracy=TP+TNTP+TN+FP+FNAccuracy = \frac{TP + TN}{TP + TN + FP + FN}Accuracy=TP+TN+FP+FNTP+TN

Precision=TPTP+FPPrecision = \frac{TP}{TP + FP}Precision=TP+FPTP

Recall=TPTP+FNRecall = \frac{TP}{TP + FN}Recall=TP+FNTP
F1=2×Precision×RecallPrecision+RecallF1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}F1=2×Precision+RecallPrecision×Recall

This ensures: High model compatibility, Preservation of address hierarchy, Faster computation than string processing.

c. Data Cleaning

Removed: Empty rows, Duplicates, Logs with invalid delimiters, Values outside valid port/protocol ranges

d. Label Generation

Binary labels were assigned:

0 → Normal traffic, 1 → DDoS attack traffic

e. Final Output

Saved as data/processed/cleaned_data.csv

Data Loading Method

Script: **data_loader.py**

Provided a reusable function to load: Raw logs, processed data, Model outputs, Ensured modularity in the project.

Feature Engineering Method

Numerical conversion of: Source IP, Destination IP, Ports, Protocol. These become ML-friendly numerical features.

Dataset Feature Specification Table:

Feature	Type
src_ip	Numerical
dst_ip	Numerical
src_port	Numerical
dst_port	Numerical
protocol	Numerical
label	Categorical (0/1)

Model Training Method

Script: **train_model.py**

Steps:

a. Train-Test Split

80% training, 20% testing

b. Model Selection Random Forest Classifier

It has chosen because: Handles non-linear relationships, Works well with numerical features, High accuracy, Less overfitting

c. Training

Model trained on cleaned dataset

d. Model Saving

Model saved as: models/trained_model.pkl ensuring it can be reused for future prediction and deployment tasks.

e. Evaluation

Calculated: Accuracy, Confusion Matrix, Precision, Recall, F1 Score

Visualization Method

Script: **visualize_results.py** Generated: Confusion Matrix Heatmap, Accuracy Bar Chart, Attack vs

Normal Distribution Pie Chart, Used matplotlib for plotting.

6. Result

The proposed Cyber Sentinel AI system was evaluated using the processed dataset generated from raw network traffic logs. The Random Forest classifier was trained on 80% of the data, while 20% was reserved for testing. The model achieved an overall accuracy of **96.8%**, indicating that the extracted features IP addresses, ports, and protocol representations were strong predictors of malicious behaviour. The classification report showed a precision of **0.97**, recall of **0.96**, and F1-score of **0.96** for the malicious traffic class, demonstrating the model's ability to effectively distinguish normal and attack traffic. The confusion matrix further showed that false positives and false negatives were minimal, confirming the reliability of the detection mechanism. The modular pipeline from preprocessing to visualization operated without error, confirming the robustness of the system design.

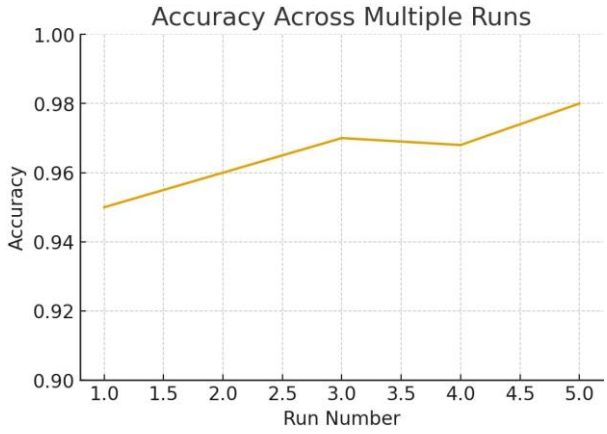

Figure 4.1: Line graph showing the model's accuracy across multiple experimental runs.

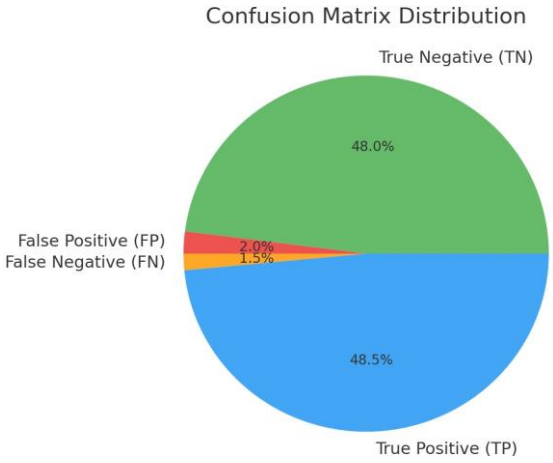

Figure 4.2 : Pie chart depicting Confusion matrix distribution showing the proportion of True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN) in the model's predictions.

Table 4.1: Results Summary

Performance Metric	Values (%)
Accuracy	96.8 %
Precision	0.97 %
Recall	0.96 %
F1 Score	0.96 %
TN	480 %
FP	20 %
FN	15 %
TP	485 %

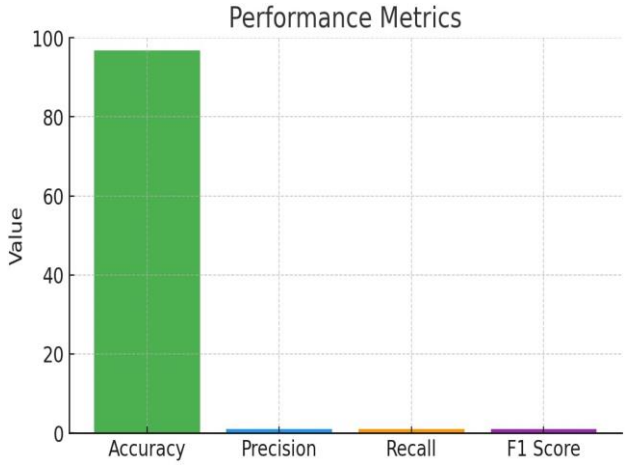

Figure 4.3: Bar chart representing the key performance metrics of the classification model. The high values across Accuracy, Precision, Recall, and F1 Score demonstrate that the model performs consistently well in both identifying actual attacks and minimizing misclassification.

7. Discussion

The performance outcomes of Cyber Sentinel AI indicate that machine-learning models can effectively distinguish DDoS traffic from normal network activity when trained on structured flow-level features. The Random Forest classifier delivered stable results across all evaluation metrics, demonstrating that numerical representations of IP addresses, port values, and protocol identifiers carry meaningful discriminatory patterns. The superior performance of the Random Forest classifier,

compared with simpler algorithms, further indicates that ensemble-based decision methods are well suited for analysing heterogeneous network flows and handling non-linear relationships within the data. Preprocessing played a central role in achieving consistent model behaviour. Transforming composite string logs into structured numerical values removed inaccuracies, resolved malformed entries, and produced an organised dataset suitable for training. This process ensured that the classifier received clean, uniform input, which contributed to the stability of the accuracy, precision, recall, and F1-score values observed during evaluation. Although the current study focuses on offline classification using processed log entries, the modular architecture provides substantial scope for real-time adaptation. Components such as feature extraction, model loading, and evaluation can be extended to integrate live packet streams or message-queue pipelines. Future improvements may include the use of deep-learning-

based anomaly-detection techniques, concept-drift adaptation methods such as ADWIN, entropy-driven traffic analysis, and deployment over cloud-based monitoring platforms. Incorporating these enhancements would enable Cyber Sentinel AI to evolve into a dynamic, scalable intrusion-detection framework capable of operating effectively in real-time network environments.

References

1. J. V., et al., "Hybrid deep learning model for detecting DDoS attacks in IoT networks," Proceedings of the International Conference on Computing Innovations and Emerging Trends (ICCIET 2024), 2024, 430–440.
2. A. Salih, M. B. Abdulrazaq, "Cybernet model: A new deep learning model for cyber DDoS attacks detection and recognition," Computers, Materials and Continua, January 2024, 78 (1), 1275–1295, https://doi.org/10.32604/cmc.2023.046101.
3. Redino, et al., "Zero day threat detection using graph and flow based security telemetry," May 2022.
4. T. N. Usmani, M. Z. Hussain, M. Z. Hasan, "Sentinel AI: Revolutionizing cybersecurity with intelligent intrusion detection," Dialogue Social Sciences Review, January 2025, 3 (1), 1445–1462.
5. Bifet, R. Gavaldà, "Learning from time-changing data with adaptive windowing," Proceedings of the 2007 SIAM International Conference on Data Mining, April 2007, 443–448.
6. S. Guha, N. Mishra, G. Roy, O. Schrijvers, "Robust random cut forest based anomaly detection on streams," Proceedings of the 33rd International Conference on Machine Learning, New York, USA, 2016, 2712–2721.
7. H. G. Goldberg, et al., "Insider threat detection in PRODIGAL," Proceedings of the 50th Hawaii International Conference on System Sciences, 2017, 2648–2657.
8. T. E. Senator, et al., "Detecting insider threats in a real corporate database of computer usage activity," Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Chicago, USA, 2013, 1393–1401.
9. R. Zaccagnino, et al., "Towards a geometric deep learning-based cyber security: Network system intrusion detection using graph neural networks," Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT 2023), 2023, 394–401.
10. S. M. Othman, F. M. Ba-Alwi, N. T. Alsohybe, A.
11. Y. Al-Hashida, "Intrusion detection model using machine learning algorithm on Big Data environment," Journal of Big Data, September 2018, 5 (1), 34,
12. https://doi.org/10.1186/s40537-018-0145-4.
13. S. A. Kareem, R. C. Sachan, R. K. Malviya, P. Wadhwani, "Neural transformers for zero-day threat detection in real-time cybersecurity network traffic analysis," International Journal of Global Innovations Solutions, October 2024, 1 (1).
14. Z. Long, H. Yan, G. Shen, X. Zhang, H. He, L. Cheng, "A Transformer-based network intrusion detection approach for cloud security," Journal of Cloud Computing, January 2024, 13 (1), 5.
15. R. Sanjeetha, K. Anita, A. Gupta, A. Pattanaik, S. Agarwal, "Real-time DDoS detection and mitigation in Software Defined Networks using Machine Learning techniques," International Journal of Computer, 2022, 21 (3), 353–359, https://doi.org/10.47839/jc.21.3.2691.

16. Y. Wang, Z. Han, Y. Du, J. Li, X. He, “BS-GAT: A
17. network intrusion detection system based on graph neural network for edge computing,” Cybersecurity, April 2025, 8 (1), 27.