# CyberGuard IDS: An AI-Powered Multi-Class Botnet and Network Intrusion Detection System Using Random Forest and XGBoost on the CICIDS2017 Dataset

**Dr.M.Navaneetha Krishnan**,
Professor & Head of Department,
Computer Science and Engineering,
St. Joseph College of Engineering, Chennai-602117, Tamil Nadu,
Email Id – mnksjce@gmail.com

**Ms.S.Sathiya Banu**,
Student, Computer Science and Engineering,
St. Joseph College of Engineering, Chennai-602117, Tamil Nadu,
Email Id – sathiyabanus15@gmail.com

## ABSTRACT

The proliferation of sophisticated cyber threats, particularly botnet-based attacks and multi-vector network intrusions, poses critical risks to modern computing infrastructure. Traditional signature-based Intrusion Detection Systems (IDS) are increasingly inadequate against polymorphic malware and zero-day exploits. This paper presents CyberGuard IDS, an AI-powered, multi-class network intrusion detection system engineered to classify network traffic flows into eight distinct categories: BENIGN, DDoS, PortScan, Botnet, BruteForce, WebAttack, Infiltration, and Heartbleed.

The system employs a dual-model machine learning architecture leveraging Random Forest as the primary classifier and XGBoost as a secondary validation model, both trained on the benchmark CICIDS2017 (Canadian Institute for Cybersecurity Intrusion Detection System 2017) dataset. A comprehensive feature engineering pipeline, encompassing data cleaning, class balancing, feature selection via importance ranking, and standardization, is implemented to maximize classification performance. The trained pipeline achieves 99.98% accuracy on the CICIDS2017 test partition, with near-perfect precision, recall, and F1-scores across all eight traffic classes.

A modern, cybersecurity-themed Flask web dashboard provides real-time single-flow prediction via REST API, batch CSV upload processing, feature importance visualization, confusion matrix display, and historical analysis logging with Chart.js-powered live analytics. This paper presents the system architecture, ML pipeline, feature engineering methodology, experimental evaluation, and future enhancement directions for Cyber Guard IDS.

## INTRODUCTION

The contemporary digital ecosystem is under relentless assault from an expanding spectrum of cyber threats. Botnets — coordinated networks of compromised machines controlled by a threat actor via command-and-control (C2) infrastructure — represent one of the most operationally versatile and economically damaging categories of cyber attack. Botnet-enabled campaigns have powered distributed denial-of-service (DDoS) attacks disrupting critical services, credential harvesting campaigns compromising millions of accounts, spam distribution networks, ransomware deployment operations, and cryptocurrency mining botnets consuming victim computational resources. The global annual cost of cybercrime, driven substantially by botnet activity, is projected to exceed $10.5 trillion USD by 2025 [1].

Traditional network security defenses — firewalls, signature-based Intrusion Detection Systems (IDS), and antivirus software — operate on pattern matching against known threat signatures maintained in continuously updated databases. While effective against catalogued attack patterns, these approaches fail fundamentally against polymorphic malware, zero-day vulnerabilities, and novel botnet command protocols that intentionally evade signature detection. Moreover, the sheer volume of modern network traffic — enterprise networks routinely process gigabits per second — renders manual traffic analysis operationally infeasible.

Machine learning (ML) based Intrusion Detection Systems address these limitations by learning statistical patterns that distinguish malicious traffic behavior from benign activity, without relying on explicit attack signatures. Ensemble methods such as Random Forest [2] and gradient boosting frameworks including XGBoost [3] have demonstrated exceptional performance on network traffic classification tasks, combining computational efficiency with high accuracy across multi-class attack taxonomies.

## LITERATURE SURVEY

**1.TITLE**

Network Intrusion Detection Using Random Forest and SHAP on the CICIDS2017 Dataset

**AUTHOR NAME**

Ashwitha C. Shetty

**YEAR**

2026

**ABSTRACT**

This study proposes an explainable intrusion detection framework using Random Forest and SHAP explainability techniques on the CICIDS2017 dataset.

**2.TITLE**

Optimizing Network Intrusion Detection Systems Through Ensemble Learning and Feature Selection Using the CIC-IDS2017 Dataset

**AUTHOR NAME**

Dharmaraj Rajaram Patil

**YEAR**

2025

**ABSTRACT**

The paper evaluates ensemble learning techniques such as Random Forest, XGBoost, LightGBM, AdaBoost, and Extra Trees on the CICIDS2017 dataset. Feature selection methods including

**3.TITLE**

Enhanced Cyber Attack Detection Using Optimized Random Forest with SMOTE-Based Class Balancing and Feature Selection

**AUTHOR NAME**

Jonson Manurung, Adam Mardamsyah, Baringin Sianipar

**YEAR**

2025

**ABSTRACT**

This research develops a Random Forest-based IDS using SMOTE balancing and feature selection techniques on CICIDS2017. The framework improves minority attack detection and handles dataset imbalance effectively.

## PROPOSED WORK

CyberGuard IDS integrates these ML advances into a production-ready system comprising a robust training pipeline, a dual-model inference architecture, and a real-time web dashboard. Trained on the CICIDS2017 dataset [4] — the most comprehensively labeled publicly available network intrusion dataset — CyberGuard IDS achieves 99.98% multi-class classification accuracy while providing actionable threat intelligence through its interactive web interface.

The primary contributions of this paper are:

(1) a complete ML pipeline for multi-class network intrusion detection including preprocessing, feature engineering, class balancing, and dual-model training.

(2) a dual-model architecture combining Random Forest and XGBoost with prediction confidence scoring.

(3) a cybersecurity-themed real-time web dashboard supporting single-flow and batch CSV prediction modes with live Chart.js analytics.

(4) a comprehensive system evaluation on the CICIDS2017 dataset.

(5) an analysis of feature importance rankings providing explainability for security analyst decision support.

## CONCLUSION

This paper has presented CyberGuard IDS, a comprehensive AI-powered multi-class botnet and network intrusion detection system achieving 99.98% classification accuracy on the CICIDS2017 benchmark dataset. By combining a dual-model architecture of Random Forest and XGBoost classifiers with a rigorous feature engineering pipeline addressing class imbalance, dimensionality reduction, and feature standardization, CyberGuard IDS delivers reliable detection across eight distinct traffic categories including BENIGN, DDoS, PortScan, Botnet, BruteForce, WebAttack, Infiltration, and Heartbleed.

Future enhancements including deep learning integration, real-time CICFlowMeter pipeline coupling, SIEM integration, federated learning for privacy preservation, and SHAP-based per-prediction explainability will expand CyberGuard IDS into a comprehensive, enterprise-grade network security platform. The modular codebase establishes a robust foundation for these extensions, positioning CyberGuard IDS as a scalable, long-term contribution to the open-source cybersecurity tool ecosystem**.**

## REFERENCE

[1] Cybersecurity Ventures. (2023). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. Available: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[2] Breiman, L. (2001). Random Forests. Machine Learning, 45(1), 5–32. doi:10.1023/A:1010933404324

[3] Chen, T., & Guestrin, C. (2016). XGBoost: A Scalable Tree Boosting System. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 785–794.

[4] Sharafaldin, I., Habibi Lashkari, A., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), 108–116.

[5] Roesch, M. (1999). Snort—Lightweight Intrusion Detection for Networks. Proceedings of the 13th USENIX Conference on System Administration (LISA), 229–238.

[6] Bace, R., & Mell, P. (2001). NIST Special Publication on Intrusion Detection Systems. National Institute of Standards and Technology (NIST SP 800-31).

[7] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A Detailed Analysis of the KDD CUP 99 Data Set. Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 1–6.

[8] Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, 5, 21954–21961.

[9] Farnaaz, N., & Jabbar, M. A. (2016). Random Forest Modeling for Network Intrusion Detection System. Procedia Computer Science, 89, 213–217.

[10] Zhang, H., Li, J. L., Liu, X. M., & Dong, C. (2021). Multi-Dimensional Feature Fusion and Stacking Ensemble Mechanism for Network Intrusion Detection. Future Generation Computer Systems, 122, 130–143.

[11] Dong, B., & Wang, X. (2016). Comparison Deep Learning Method to Traditional Methods Using for Network Intrusion Detection. Proceedings of the 8th IEEE International Conference on Communication Software and Networks (ICCSN), 581–585.

[12] Sharafaldin, I., Habibi Lashkari, A., Hakak, S., & Ghorbani, A. A. (2019). Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. Proceedings of the 53rd IEEE International Carnahan Conference on Security Technology (ICCST), 1–8.

[13] Alrawashdeh, K., & Purdy, C. (2016). Toward an Online Anomaly Intrusion Detection System Based on Deep Learning. Proceedings of the 15th IEEE International Conference on Machine Learning and Applications (ICMLA), 195–200.

[14] Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., Celik, Z. B., & Swami, A. (2016). The Limitations of Deep Learning in Adversarial Settings. Proceedings of the 1st IEEE European Symposium on Security and Privacy (EuroS&P), 372–387.

[15] Lundberg, S. M., & Lee, S. I. (2017). A Unified Approach to Interpreting Model Predictions. Advances in Neural Information Processing Systems, 30, 4765–4774.

[16] Scikit-learn Documentation. (2024). Ensemble Methods: Random Forests. Available: https://scikit-learn.org/stable/modules/ensemble.html

[17]XGBoost Documentation. (2024). XGBoost Parameters. Available: https://xgboost.readthedocs.io/en/stable/parameter.html

[18] Flask Documentation. (2024). Flask 3.x Web Framework. Available: https://flask.palletsprojects.com