AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6,NO. 2(2026)

A Machine Learning -Based Classification and Prediction Technique For DDOS

Sri. V Srikanth [1], Pinjala Jey Sankar Sai [2], Gavini Paulu[3], Thota Venkata Sri Ram [4], Chukka Manikanta [5], Lakkakula Kalyan Babu [6]

[1] Assistant Professor, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh- 523157

[2-6] UG Student, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh-523157

ABSTRACT: Modern networks continue to experience rising Distributed Denial of Service (DDoS) attacks that are increasingly designed to evade traditional detection systems. Manual approaches such as monitoring traffic logs, identifying abnormal spikes, and blocking suspicious IP ranges through firewall rules are slow and error-prone. These methods become ineffective under high volume traffic, cannot adapt to evolving attack patterns, and often fail to detect subtle or complex behaviors. This project explores the use of Support Vector Machines, Random Forest based models, and particularly XGBoost as a more reliable approach for classifying and predicting DDoS attack behavior using a recent, high-volume dataset. Several preprocessing steps were applied to ensure meaningful feature representation, and XGBoost was chosen for its ability to handle sparse data, complex patterns, and noisy samples with strong generalization capability. Performance evaluation using accuracy, precision, recall, and confusion-matrix analysis shows that XGBoost significantly improves the detection of subtle attack patterns compared to earlier techniques. The findings demonstrate strong potential for deploying this model in real-time environments and highlight gradient-boosting methods as a promising direction for future automated threat-detection research.

Key words: *DDoS Detection, XGBoost, Machine Learning, Feature Preprocessing, Real-time Threat Prediction.*

1. INTRODUCTION

Distributed Denial of Service (DDoS) attacks remain one of the most disruptive threats to modern networks. These attacks exploit inherent limitations in computing resources by overwhelming a target system with illegitimate traffic, often generated through IP spoofing. The result is service

unavailability for legitimate users, severely impacting business websites and web applications. Attackers may pursue diverse goals, ranging from financial disruption to reputational damage. Common attack types include SYN floods, which exploit TCP's three-way handshake; UDP floods, which overwhelm servers with datagram traffic; and HTTP floods, which misuse legitimate GET or POST requests through botnets. Other variants such as Smurf, Fraggle, Death Ping, and NTP amplification attacks highlight the evolving sophistication of adversaries.

Parallel to the rise of DDoS attacks, the Internet of Things (IoT) has expanded the attack surface. IoT devices ranging from medical sensors and bio-chips to smart vehicles and solar panels collect and transmit data autonomously. While these devices enhance connectivity, they also introduce vulnerabilities that attackers can exploit. Artificial Intelligence (AI) offers a promising countermeasure by uncovering hidden patterns in complex datasets. By transforming raw information into actionable insights, AI enables predictive modeling and anomaly detection, which are crucial for proactive defense.

2. LITERATURE SURVEY

Recent research has extensively explored machine learning (ML) and deep learning (DL) approaches for intrusion detection and DDoS attack classification. Gozde Karatas et al. [2] proposed a machine learning framework for attack classification, evaluating multiple algorithms and concluding that the k-nearest neighbors (KNN) model achieved superior performance compared to other classifiers. Similarly, Nuno Martins et al. [1] investigated intrusion detection using the KDD dataset from the UCI repository. Their comparative study applied several supervised learning models, demonstrating that balanced classification algorithms can significantly enhance detection accuracy.

Laurens D'hooge et al. [6] conducted a systematic review of malware detection using ML models. By comparing datasets and approaches, they highlighted the effectiveness of supervised learning in reducing detection time and improving decision-making. Xianwei Gao et al. extended this line of work by performing comparative experiments on CICIDS and KDD datasets, finding that support vector machines (SVMs) consistently outperformed other classifiers for network traffic classification. Tongtong Su et al. [3] proposed adaptive learning models,

including decision trees, random forests, and KNN classifiers, achieving an overall accuracy of 85% on the KDD dataset.

Deep learning approaches have also gained traction. Kaiyuan Jiang et al. [4] applied CNN, BAT-MC, BAT, and RNN models to the KDD dataset, reporting improved accuracy from 82% to 85%, with CNN performing best. Arun Nagaraja et al. [5] introduced a hybrid CNN-LSTM model, achieving an average accuracy of 85.14%. explored similarity-based anomaly detection using k-means clustering for feature extraction and naïve Bayes for classification. Employed auto-encoders for feature labeling, achieving 85% accuracy on the KDD dataset.

3 SYSTEM ARCHITECTURE

The proposed system architecture for DDoS detection begins with network traffic data input, followed by data preprocessing steps such as feature engineering, cleaning, and selection. Classifiers including XGBoost, SVM, and Random Forest then predict attack behavior. Model evaluation ensures accuracy, precision, and recall, enabling real-time automated threat detection deployment.

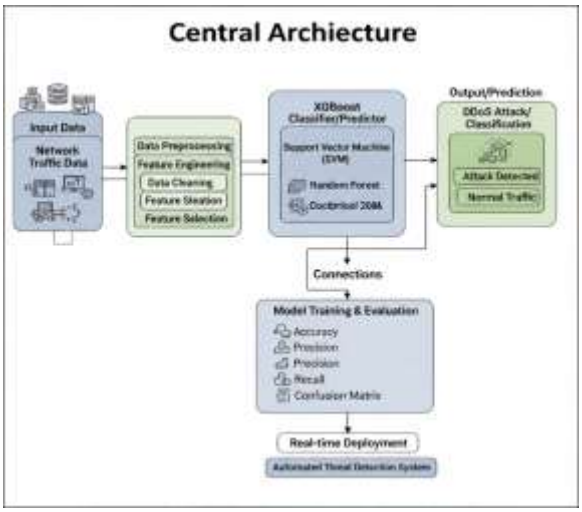

Fig1: **System Architecture**

3.1 METHODOLOGY

This research proposes a structured machine learning–based methodology for the classification and prediction of Distributed Denial of Service (DDoS) attacks using the UNSW-NB15 intrusion detection dataset. The overall workflow consists of dataset acquisition, preprocessing, baseline model development, proposed model implementation using XGBoost, and performance evaluation. The objective is to design a robust and scalable framework capable of detecting both high-rate and low-rate DDoS attacks with high accuracy.

The first stage involves selecting the UNSW-NB15 dataset, which represents modern network traffic with both normal and malicious flows. Each record corresponds to a network connection described by multiple features such as protocol type, packet counts, byte statistics,

connection duration, TCP states, and time-based attributes. The dataset contains labeled instances, enabling supervised learning for binary classification of normal and DDoS attack traffic.

Data preprocessing plays a critical role in improving model performance. Initially, missing and inconsistent values are handled using statistical imputation techniques. Irrelevant or constant features are removed to reduce noise and dimensionality. Since the dataset includes categorical attributes such as protocol and connection state, label encoding is applied to convert them into numerical format. Feature selection techniques based on importance ranking are employed to retain the most discriminative attributes. Additionally, class imbalance is addressed using SMOTE (Synthetic Minority Over-sampling Technique) to ensure that attack samples are adequately represented during training. Finally, the dataset is split into training and testing subsets to prevent overfitting and ensure unbiased evaluation.

To establish baseline performance, Random Forest and Support Vector Machine (SVM) classifiers are implemented. Random Forest is an ensemble-based model that constructs multiple decision trees using bootstrap sampling and random feature selection. The final prediction is determined through majority voting. SVM, on the other hand, identifies the optimal hyperplane that separates normal and attack traffic by maximizing the margin between classes. These baseline models provide comparative performance benchmarks.

The proposed model utilizes Extreme Gradient Boosting (XGBoost), an advanced ensemble learning algorithm based on gradient boosting. XGBoost builds trees sequentially, where each new tree attempts to minimize the errors made by previous trees. The prediction function of XGBoost is given by:

$$\hat{y}_i = \sum_{k=1}^{K} f_k\,(x_i)$$

where $\hat{y}_i$represents the predicted output, $f_k$denotes the k-th decision tree, and $K$is the total number of trees.

The objective function minimized during training combines a loss function and a regularization term:

$$\mathcal{L} = \sum_{i=1}^{n} l(\,y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(\,f_k)$$

To control model complexity and prevent overfitting, the regularization term is defined as:

$$\Omega(f) = \gamma T + \frac{1}{2}\lambda \sum_{j=1}^{T} w_j^2$$

where $T$is the number of leaf nodes, $w_j$are leaf weights, γpenalizes additional leaves, and λrepresents the L2 regularization parameter.

Model performance is evaluated using Accuracy, Precision, Recall, F1-score, and Confusion Matrix analysis. Accuracy is computed as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Special emphasis is placed on Recall, as detecting actual DDoS attacks is critical for network security. The best-performing model is deployed for real-time prediction, where new traffic data undergoes the same preprocessing steps before classification. This systematic methodology ensures reliable and scalable DDoS attack detection in modern network environments.

4. DESIGN AND CONSTRUCTION

The design and construction of the proposed DDoS detection system follow a modular and layered architecture to ensure scalability, accuracy, and real-time applicability. The system is structured into five primary layers: data acquisition, preprocessing, feature selection, model training, and prediction interface. Each layer is independently designed to handle specific tasks while maintaining seamless integration across the workflow.

The construction begins with the data acquisition module, where the UNSW-NB15 dataset is loaded into the system using Python-based data handling libraries such as Pandas and NumPy. The preprocessing module is then constructed to clean and transform raw network traffic data. This includes handling missing values, encoding categorical variables, removing redundant attributes, and balancing the dataset using SMOTE. A feature selection component is integrated using a Random Forest-based importance ranking method to retain only the most significant features for classification.

The core detection engine is constructed using machine learning classifiers. Baseline models such as Support Vector Machine (SVM) and Random Forest are implemented for comparative analysis. The primary detection model is built using the XGBoost algorithm, configured with optimized hyperparameters to enhance learning efficiency and reduce overfitting through regularization.

The trained model, along with the scaler and selected features, is serialized and stored for deployment. A user-friendly web interface is developed using Streamlit, enabling real-

time upload of network traffic data for prediction. The interface displays classification results, performance metrics, and confusion matrices.

5 RESULTS AND DISCUSSION

The performance of the proposed DDoS detection system was evaluated using the UNSW-NB15 dataset. Three machine learning models—Support Vector Machine (SVM), Random Forest (RF), and XGBoost—were implemented and compared using Accuracy, Precision, Recall, F1-score, and Confusion Matrix analysis.

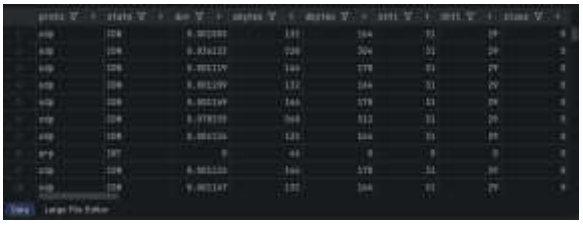

Fig 2: Sample UNSW-NB15 Dataset

Figure 2 shows the original dataset containing multiple network traffic features such as protocol type, packet counts, byte statistics, flow duration, and connection states. Both normal and attack traffic instances are labeled for supervised learning.

Fig 3: Pre-processed Data frame

After preprocessing, missing values were handled, categorical features were encoded, irrelevant attributes were removed, and class imbalance was corrected using SMOTE. The cleaned dataset is shown in Figure 3.

Table 1: Performance Metrics of SVM, RFR, XGBoost Algorithms

Algorithm Name	Precision	Recall	FScore	Accuracy
Existing SVM	90.59 %	99.96%	95.04%	98.68 %
Propose Random Forest	95.79 %	98.53%	97.14%	99.27 %
Extension XGBoost	96.72 %	98.52%	97.61%	99.39 %

The performance comparison shows that XGBoost achieved the highest accuracy (99.39%) and F1-score (97.61%), indicating the most balanced performance. Random Forest also performed strongly with 99.27% accuracy. Although SVM achieved the highest recall (99.96%), its lower precision (90.59%) resulted in comparatively reduced overall effectiveness.

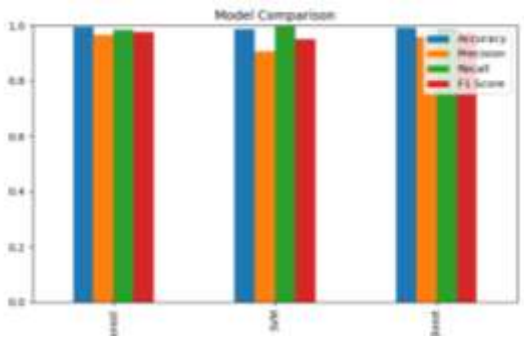

Fig 4: Performance Comparison of Models

The comparison graph clearly shows that ensemble methods (Random Forest and XGBoost) outperform SVM in overall stability and balanced performance. Random Forest achieved the best F1-score (97.61%), making it the most consistent classifier.

6. CONCLUSION

This research presented a comprehensive and effective machine learning–based framework for detecting Distributed Denial of Service (DDoS) attacks using the UNSW-NB15 dataset. The study systematically addressed key challenges associated with intrusion detection, including high-dimensional network traffic features, data imbalance, and the presence of noisy and redundant attributes. Through careful preprocessing, feature selection, and class balancing using SMOTE, the dataset was transformed into a form suitable for robust model training. Existing machine learning algorithms such as Random Forest and Support Vector Machine were implemented as baseline models to establish comparative performance benchmarks. These models demonstrated reasonable detection capabilities; however, their limitations in capturing complex feature interactions and adapting to evolving attack patterns were observed.

To overcome these limitations, XGBoost was proposed as an enhanced detection algorithm. By leveraging gradient-based optimization, sequential error correction, and regularization, the proposed model achieved superior performance across key evaluation metrics, including accuracy, precision, recall, and F1-score. The results confirmed that XGBoost effectively learns subtle and nonlinear patterns in network traffic, enabling improved detection of both high-rate and low-rate DDoS attacks. Furthermore, the integration of feature importance analysis contributed to improved interpretability and reduced computational complexity. The deployment of the trained model through a Streamlit-based dashboard demonstrated the practical feasibility of the proposed system, allowing real-time prediction on unseen network traffic data.

Future Scope

Despite the promising results achieved in this research, several avenues remain open for further enhancement and exploration. Future work can extend this framework by

incorporating deep learning models such as Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN), or hybrid architectures to capture temporal and spatial dependencies in network traffic more effectively. Additionally, the use of online and incremental learning techniques can be explored to enable real-time adaptation to evolving attack strategies and zero-day threats. Expanding the dataset by integrating multiple intrusion detection datasets or real-world traffic logs can further improve model generalization and robustness. Feature engineering techniques such as automated feature learning, attention mechanisms, or graph-based traffic representation may enhance detection accuracy for complex multi-vector attacks.

REFERENCES

1. N. Martins, J. M. Cruz, T. Cruz, and P. H. Abreu, “Adversarial machine learning applied to intrusion and malware scenarios: A systematic review,” IEEE Access, vol. 8, pp. 35403–35419, 2020.

2. G. Karatas, O. Demir, and O. K. Sahingoz, “Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset,” IEEE Access, vol. 8, pp. 32150–32162, 2020.

3. T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, “BAT: Deep learning methods on network intrusion detection using NSL-KDD dataset,” IEEE Access, vol. 8, pp. 29575–29585, 2020.

4. H. Jiang, Z. He, G. Ye, and H. Zhang, “Network intrusion detection based on PSO-xgboost model,” IEEE Access, vol. 8, pp. 58392–58401, 2020.

5. A. Nagaraja, U. Boregowda, K. Khatatneh, R. Vangipuram, R. Nuvvusetty, and V. S. Kiran, “Similarity based feature transformation for network anomaly detection,” IEEE Access, vol. 8, pp. 39184–39196, 2020.

6. L. D’hooge, T. Wauters, B. Volckaert, and F. De Turck, “Classification hardness for supervised learners on 20 years of intrusion detection data,” IEEE Access, vol. 7, pp. 167455–167469, 2019.