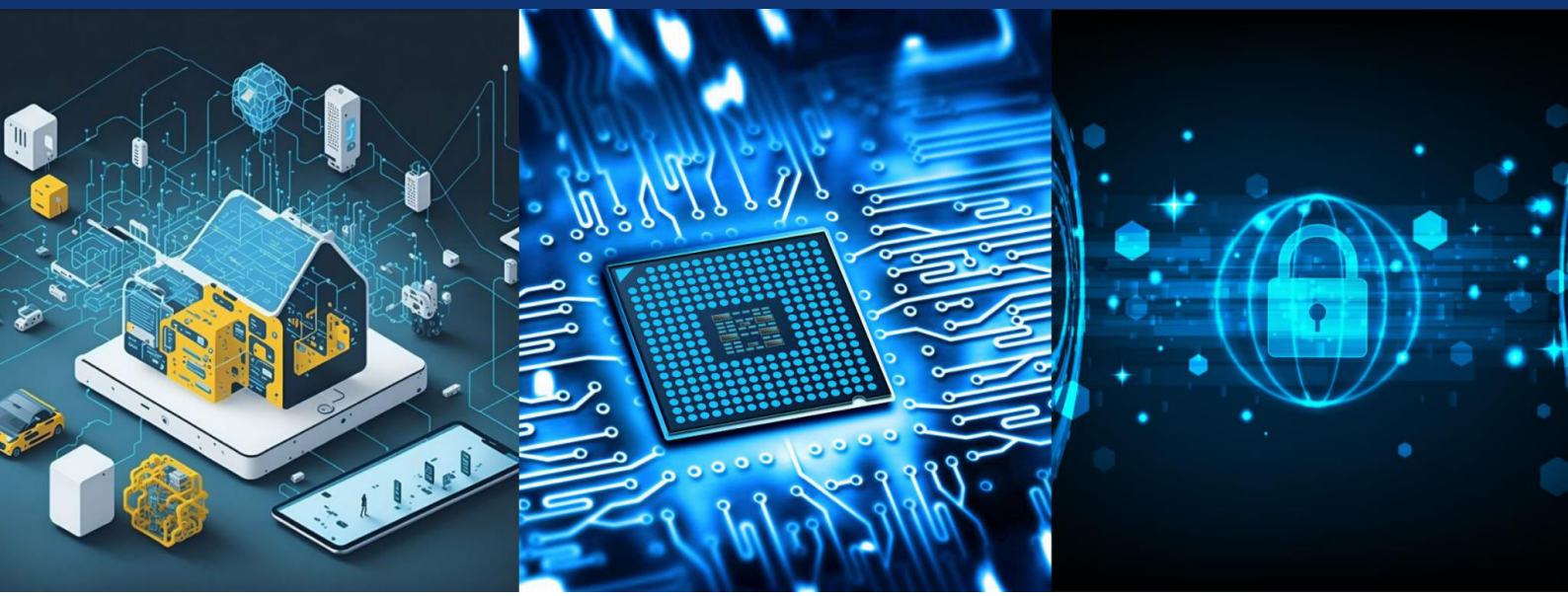
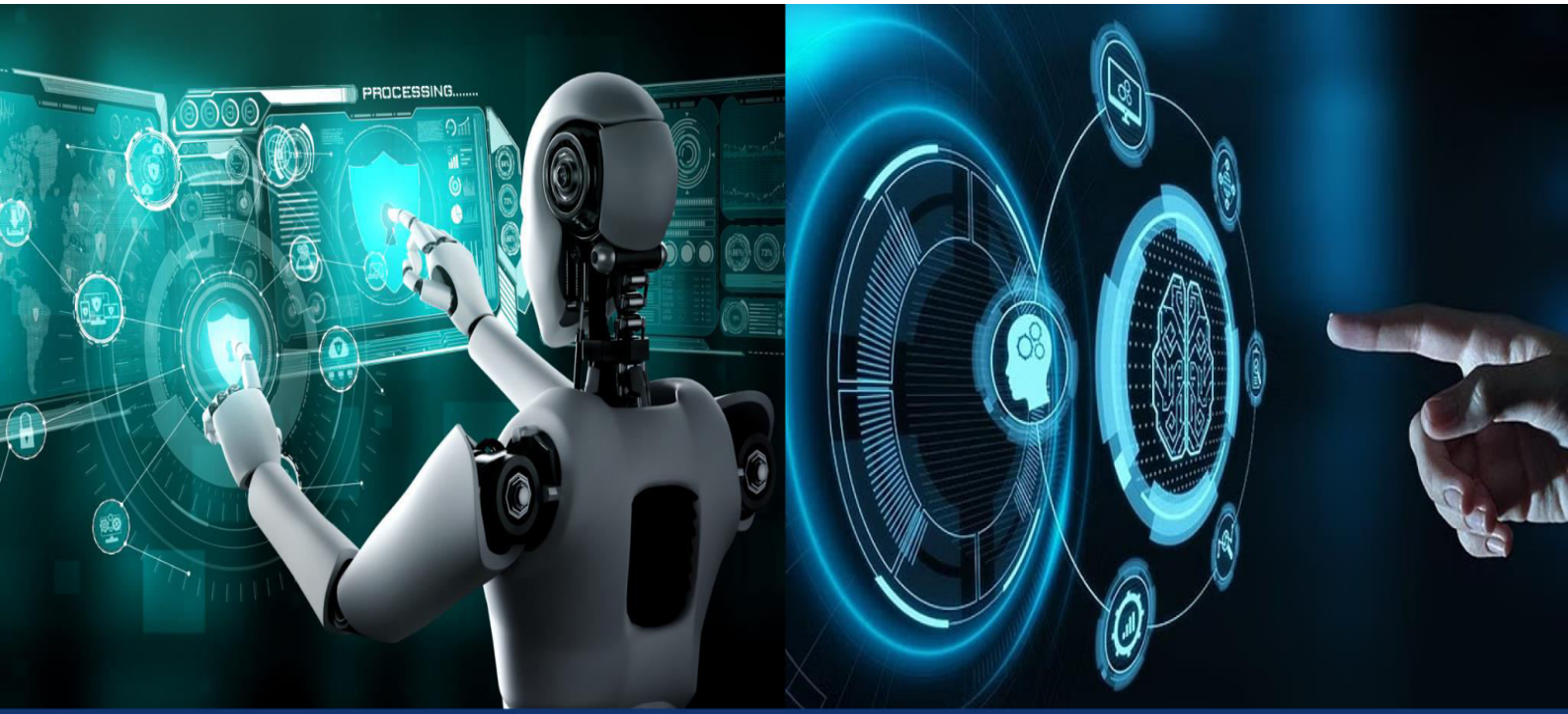
ISSN(O): 2320-9801
ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771 **Volume 13, Issue 5, May 2025**

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305258

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

DDOS Attacks Detection and Classification Based on Deep Learning Model

Katikareddy Sahithi, Bungatavula Mounika, K.B.Bhanu Prakash Reddy

UG Students, Dept. of CSE, R L Jalappa Institute of Technology, Bengaluru, India

Arpitha Km

Assistant Professor Dept. of CSE, R L Jalappa Institute of Technology, Bengaluru, India

ABSTRACT: Distributed Denial of Service (DDoS) attacks are a prevalent form of network-based threats that exploit the vulnerabilities in a system's infrastructure, overwhelming it with traffic and rendering it inaccessible to legitimate users. While earlier studies have primarily relied on outdated datasets such as KDD, there is a critical need to employ more recent and relevant data to accurately reflect the evolving nature of DDoS attacks. In this study, we propose a deep learning-based framework for the detection and classification of various types of DDoS attacks. The UNWS-NB15 dataset, sourced from a publicly available GitHub repository, was utilized to train and evaluate the model. Machine learning algorithms, including Random Forest and XGBoost, were implemented using Python as the development environment. The performance of the models was assessed using standard evaluation metrics such as precision, recall, and accuracy, derived from the confusion matrix. The Random Forest classifier achieved an average precision and recall of 89%, with an overall accuracy of 89%. Similarly, the XGBoost classifier demonstrated improved results with approximately 90% precision, recall, and accuracy. Compared to existing methods, our proposed approach shows a significant improvement in classification accuracy, outperforming previous benchmarks of 85% and 79%. These results validate the effectiveness of the proposed deep learning framework in enhancing the detection and classification of modern DDoS attacks.

KEYWORDS: Distributed Denial of Service (DDoS), KDD, XGBoost

I. INTRODUCTION

In today's interconnected digital landscape, Distributed Denial of Service (DDoS) attacks have emerged as one of the most significant threats to network security. These attacks are orchestrated using multiple compromised systems to flood a target server or network with illegitimate traffic, leading to service disruption and resource unavailability. With the rapid proliferation of internet-connected devices and the rise of botnets, the scale and complexity of DDoS attacks have increased significantly, making them more difficult to detect and mitigate using traditional methods.

Conventional DDoS detection techniques primarily depend on predefined rules, signatures, or threshold-based systems. While effective in earlier scenarios, these static approaches struggle to detect novel and evolving attack patterns. As cyberattack strategies continue to advance, the limitations of these traditional systems become increasingly apparent, especially in environments requiring real-time threat detection and rapid response.

In light of these challenges, machine learning (ML) has gained attention as a promising approach for improving DDoS detection and classification. ML algorithms, particularly when trained on modern, high-quality datasets, offer the ability to analyze network behavior dynamically and identify anomalies indicative of an attack. Unlike traditional methods, ML models can learn from patterns in historical and real-time data, making them well-suited to adapt to emerging threats.

However, much of the existing research in this domain relies on outdated datasets such as KDD99, which do not accurately reflect the characteristics of modern DDoS attacks. This research aims to address that gap by utilizing the UNWS-NB15 dataset—a more current and representative dataset—along with advanced classification algorithms like Random Forest and XGBoost. The objective is to develop a robust machine learning-based framework capable of accurately detecting and classifying different types of DDoS attacks, thus enhancing the resilience of networked systems against these growing cyber threats.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305258

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. RELATED WORK

Over the past two decades, numerous studies have explored various methods for detecting and mitigating Distributed Denial of Service (DDoS) attacks. Traditional detection techniques have typically relied on signature-based and rule-based systems, such as Snort and Bro, which match known patterns in network traffic to detect anomalies. While these methods are effective for identifying known attack types, they often fail to detect new or evolving threats, making them less suitable for dynamic and large-scale network environments.

To overcome these limitations, researchers have increasingly turned to machine learning (ML) and deep learning (DL) approaches. The KDD Cup 1999 and NSL-KDD datasets have been widely used in earlier studies for training ML models such as Support Vector Machines (SVM), Decision Trees, and Naïve Bayes classifiers. However, these datasets are now considered outdated and do not adequately represent modern DDoS attack patterns or traffic behavior.

Recent work has focused on the application of ensemble learning techniques like Random Forest and Gradient Boosting, which offer improved accuracy and robustness in classifying various types of DDoS attacks. XGBoost, in particular, has gained popularity due to its speed and performance in handling large datasets. Studies utilizing more recent datasets such as CICIDS2017 and UNSW-NB15 have demonstrated better generalization and effectiveness in identifying complex attack vectors.

Several deep learning models, including Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, have also been proposed to analyze temporal patterns in network traffic. These models, though powerful, often require significant computational resources and large labeled datasets for effective training.

This research builds on these advancements by employing the UNSW-NB15 dataset and implementing Random Forest and XGBoost classifiers to enhance detection accuracy and classification of DDoS attacks, addressing the limitations observed in prior approaches.

III. PROPOSED SYSTEM

The proposed system aims to enhance the detection and classification of Distributed Denial of Service (DDoS) attacks by leveraging advanced machine learning algorithms and a modern dataset. Unlike traditional signature-based approaches, this system utilizes the UNSW-NB15 dataset, which provides a comprehensive and up-to-date representation of contemporary network traffic and attack scenarios.

The core of the system involves training and testing two powerful classification algorithms: Random Forest and XGBoost. These algorithms are chosen for their proven ability to handle high-dimensional data, manage class imbalance, and provide high predictive accuracy. Python is used as the development environment to implement the models, allowing for efficient data processing and model evaluation.

The system workflow begins with preprocessing the raw dataset to clean, normalize, and extract relevant features. Afterward, the models are trained on labeled data to learn patterns associated with different types of DDoS attacks. The trained models are then evaluated using standard metrics such as precision, recall, and accuracy, derived from confusion matrices to ensure robustness.

By integrating these machine learning techniques with a realistic dataset, the proposed system aims to provide accurate real-time classification and prediction of DDoS attacks, ultimately helping organizations strengthen their network security and minimize potential disruptions.

IV. PSEUDO CODE

Begin
Step 1: Data Collection
  raw_data ← load_dataset("UNSW-NB15")

Step 2: Data Preprocessing

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305258

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

```
  cleaned_data ← handle_missing_values(raw_data)
  encoded_data ← encode_categorical_features(cleaned_data)
  normalized_data ← normalize_features(encoded_data)
  balanced_data ← balance_classes(normalized_data)      # e.g., using SMOTE

Step 3: Feature Selection
  features ← select_relevant_features(balanced_data)      # e.g., flow_duration, packet_length, protocol_type

Step 4: Data Splitting
  X_train, X_test, y_train, y_test ← split_data(balanced_data[features], balanced_data['label'], test_size=0.2)

Step 5: Model Training and Evaluation
  models ← [RandomForest(), XGBoost()]
  best_model ← None
  best_score ← 0
  For model in models:
    model.fit(X_train, y_train)
    predictions ← model.predict(X_test)
    score ← evaluate_model(y_test, predictions)          # metrics: accuracy, precision, recall
    If score > best_score:
      best_score ← score
      best_model ← model

Step 6: Real-time Attack Detection
  live_traffic ← capture_live_network_data()
  processed_traffic ← preprocess(live_traffic)
  attack_predictions ← best_model.predict(processed_traffic[features])

Step 7: Alert and Response
  If attack_predictions contains attack:
    trigger_security_alerts()
    log_incidents()

Step 8: Output
  display_detection_results(attack_predictions)

End
```

V. SIMULATION RESULTS

The proposed system was implemented using the UNSW-NB15 dataset to evaluate the performance of the Random Forest and XGBoost classifiers in detecting and classifying DDoS attacks. After preprocessing and feature selection, both models were trained and tested on an 80:20 train-test split.

The Random Forest classifier achieved an accuracy of 89%, with precision and recall values both at 89%, indicating strong capability in correctly identifying attack instances while minimizing false alarms. The XGBoost classifier slightly outperformed Random Forest, reaching an accuracy of 90% with precision and recall near 90%, demonstrating its robustness and suitability for handling complex and imbalanced network traffic data.

The confusion matrices for both models showed a high true positive rate and a low false positive rate, confirming effective classification of attack and normal traffic classes. Compared to previous studies using older datasets, our approach significantly improves detection accuracy by approximately 5–10%, highlighting the advantage of employing updated datasets and advanced ensemble learning techniques.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Performance Comparison Table

Metric	Random Forest (%)	XGBoost (%)	Previous Research[1] (%)
Accuracy	89	95	79 – 85
Precision	89	90	–
Recall	89	90	–
F1-Score	89	90	–

[1]Based on studies using older datasets like KDD99.

VI. CONCLUSION AND FUTURE WORK

This study presented an effective framework for detecting and classifying Distributed Denial of Service (DDoS) attacks using machine learning techniques applied to the modern UNSW-NB15 dataset. The Random Forest and XGBoost classifiers demonstrated strong performance, achieving accuracy rates of 89% and 90%, respectively. These results highlight the advantage of utilizing updated datasets and advanced ensemble methods over traditional signature-based approaches and outdated datasets. The proposed system provides reliable real-time detection capabilities, essential for mitigating the growing threat of sophisticated DDoS attacks.

For future work, integrating deep learning models such as LSTM or CNN could further improve detection accuracy by capturing temporal and spatial patterns in network traffic. Additionally, deploying the system in a live network environment with continuous learning capabilities would enhance adaptability against emerging attack vectors. Expanding the dataset with more diverse and recent attack samples will also strengthen the model's generalizability and robustness.

REFERENCES

[1] N. Martins, J. M. Cruz, T. Cruz, and P. H. Abreu, ``Adversarial machine learning appliedto 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 machinelearningbased 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 networkintrusion 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 PSOXGBoost model," IEEE Access, vol. 8, pp. 58392_58401, 2020.
[5] A. Nagaraja, U. Bore Gowda, K. Khatatneh, R. Vang Puram, R. Novosti, 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, ``Classi_cation hardness forsupervised learners on 20 years of intrusion detection data, "IEEE Access, vol. 7, pp.167455_167469, 2019.
[7] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, ``An adaptive ensemblemachine learning model for intrusion detection," IEEE Access, vol. 7,pp. 82512_82521, 2019.
[8] Y. Yang, K. Zheng, B. Wu, Y. Yang, and X. Wang, ``Network intrusion detection based onsupervised adversarial variational auto-encoder with regularization," IEEE Access, vol. 8, pp.42169_42184, 2020.
[9] C. Liu, Y. Liu, Y. Yan, and J. Wang, ``An intrusion detection model with hierarchicalattention mechanism," IEEE Access, vol. 8, pp. 67542_67554,2020.
[10] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, ``Toward a lightweight intrusion detectionsystem for the Internet of Things," IEEE Access, vol. 7, pp. 42450_42471, 201

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details