International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-June-2026, ISSN (Online): 2395-566X

Dos Attack Detection Using Edge Machine Learning

OM Kute[1], Yuvraj Narwade[2], T.B. Faruki[3]
[1,2,3]Department of Computer Engineering, STES'S SAOE , Pune, India

Abstract — Denial of Service (DoS) attacks are one of the most common cyber threats that disrupt network services by overwhelming systems with malicious traffic. Traditional cloud-based detection methods often experience higher latency and increased bandwidth usage, making them less effective for real-time protection. The DoS Attack Detection System Using Edge Machine Learning introduces an intelligent approach that detects malicious network traffic directly at edge devices before it reaches the central server. By leveraging Edge Computing, Machine Learning, and real-time traffic analysis, the system identifies abnormal network behavior with low latency and improved accuracy. This approach reduces server overload, enhances network security, and ensures continuous availability of services while providing a scalable and efficient solution for modern IoT and edge-enabled environments.

Keywords— Denial of Service (DoS), Edge Computing, Edge Machine Learning, Network Security, Intrusion Detection, Traffic Analysis.

I. INTRODUCTION

With the rapid growth of the Internet, cloud computing, and IoT devices, computer networks have become an essential part of everyday life. As the number of connected devices continues to increase, cyber threats such as Denial of Service (DoS) attacks have also become more frequent and sophisticated. A DoS attack attempts to overwhelm a network, server, or application with excessive traffic, making legitimate services unavailable to authorized users. Such attacks can lead to service disruption, financial loss, and reduced user trust.

Traditional intrusion detection systems often rely on cloud-based processing, which may introduce higher latency and increased bandwidth usage. These limitations make it difficult to detect and respond to attacks in real time, especially in edge-enabled and IoT environments. Moreover, many conventional security solutions depend on predefined rules and signatures, making them less effective against evolving attack patterns.

To address these challenges, the DoS Attack Detection System Using Edge Machine Learning applies machine learning techniques at the network edge to identify malicious traffic quickly and accurately. By processing network data closer to the source, the system reduces response time, minimizes unnecessary network traffic, and improves overall security. Using the NSL-KDD dataset, machine learning models are trained to classify network traffic as Normal or DoS Attack based on network traffic features. The proposed system provides an efficient, scalable, and intelligent approach for real-time DoS attack detection while supporting modern edge computing environments.

II. LITERATURE REVIEW

Several researchers have proposed machine learning and deep learning techniques to improve the detection of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks in modern networks.

Traditional Intrusion Detection Systems (IDS) mainly rely on signature-based methods, which are effective for known attacks but often fail to identify new or evolving attack patterns.

Recent studies have shown that Machine Learning (ML) algorithms such as Decision Tree, Random Forest, Support Vector Machine (SVM), and XGBoost can accurately classify normal and malicious network traffic by learning patterns from network datasets like NSL-KDD and CICIDS2017. These approaches improve detection accuracy while reducing false alarm rates.

With the emergence of Edge Computing, researchers have focused on deploying lightweight machine learning models directly on edge devices. This approach enables faster attack detection with lower latency, reduced bandwidth consumption, and quicker response compared to cloud-based detection systems. Edge Machine Learning has become a promising solution for protecting IoT networks and real-time applications.

Although significant progress has been made, challenges such as handling unseen attack patterns, class imbalance, feature selection, model generalization, and maintaining high detection accuracy in real-world environments still remain. Therefore, developing efficient, lightweight, and scalable edge-based DoS detection systems continues to be an active area of research.

Furthermore, the feature engineering and preprocessing pipeline played a significant role in improving the overall performance of the proposed system. Techniques such as label engineering, categorical feature encoding, correlation-based feature selection, feature scaling, and SMOTE helped reduce redundant information, address class imbalance, and improve the learning capability of the machine learning models. Cross-validation and hyperparameter tuning further enhanced model stability and reduced the risk of overfitting, resulting in a classifier that performs consistently on unseen network traffic.

The proposed edge-based architecture also demonstrates practical applicability for real-time network security. By deploying lightweight machine learning models at edge devices, network traffic can be analyzed close to the data source, reducing detection latency, minimizing bandwidth usage, and enabling faster response to DoS attacks. Although the system achieved high detection performance, future improvements can focus on handling zero-day attacks, evaluating the model on more recent cybersecurity datasets such as CICIDS2017 or CSE-CIC-IDS2018, and integrating deep learning techniques for enhanced detection of complex and evolving attack patterns in real-world edge computing environments.

III. METHODOLOGY

1. Dataset

- Publicly available NSL-KDD dataset containing normal and attack network traffic records.
- Dataset includes 41 network traffic features and various attack categories such as DoS, Probe, R2L, and U2R.
- For this project, only Normal and DoS attack records are used for binary classification.
- The dataset is divided into KDD Train+ (training) and KDD Test+ (testing) for model development and evaluation.

2. Preprocessing

- Raw network traffic data is cleaned and prepared for machine learning.
- Label engineering converts multiple attack types into Normal and DoS classes.
- Categorical features are encoded, redundant features are removed, and numerical data is scaled.
- Feature selection and class balancing (SMOTE) are applied to improve model performance.

3. Model Development

- Multiple Machine Learning algorithms are trained, including Logistic Regression, Decision Tree, Random Forest, and XG Boost.
- Hyperparameter tuning and cross-validation are performed to improve accuracy and reduce overfitting.
- Models are evaluated using Accuracy, Precision, Recall, F1-Score, ROC-AUC, and Confusion Matrix.
- The best-performing model is selected for deployment.

4. System Architecture

Network Traffic → Data Preprocessing → Feature Engineering → Machine Learning Model → DoS/Normal

Prediction → Edge Device / Stream lit Dashboard

- Incoming traffic is analyzed in real time.
- The trained model classifies traffic as Normal or DoS Attack.
- Results are displayed through a Stream lit dashboard, enabling quick detection and response with low latency.
- The lightweight architecture supports deployment on edge devices for faster and efficient attack detection.

IV. EXPERIMENTAL SETUP

The proposed DoS Attack Detection System Using Edge Machine Learning was evaluated using the NSL-KDD dataset, which contains labeled network traffic records representing both normal and attack activities.

- Dataset: NSL-KDD dataset (KDD Train+ and KDD Test+) containing Normal and DoS attack traffic.
- Preprocessing Tools: Python libraries including Pandas, NumPy, Scikit-learn, Matplotlib, and Seaborn for data cleaning, visualization, feature engineering, encoding, scaling, and SMOTE.
- Model Training: Multiple machine learning models including Logistic Regression, Decision Tree, Random Forest, and XG Boost were trained using hyperparameter tuning and cross-validation.
- Validation: 5-fold Cross-Validation and train-test evaluation were performed to ensure reliable model performance and avoid overfitting.
- Evaluation Metrics: Accuracy, Precision, Recall, F1-Score, ROC-AUC Score, Confusion Matrix, and Detection Time were used to compare models and select the best-performing classifier.

V. RESULT

1. The proposed DoS Attack Detection System
Using Edge Machine Learning achieved strong performance in detecting DoS attacks using the NSL-KDD dataset. Multiple machine learning models were trained and evaluated, with Logistic Regression providing the best overall balance between accuracy, recall, and generalization.

- Best Test Accuracy: 93.16% (Logistic Regression)
- Highest Precision: 98.59%
- Best F1-Score: 91.57%
- Highest ROC-AUC: 98.85% (XG Boost)
- Average Cross-Validation Recall: 99.6%+

The experimental results demonstrate that the proposed system can accurately distinguish Normal and DoS network traffic with high reliability while maintaining good generalization on unseen test data. The lightweight machine learning models are suitable for edge deployment, enabling fast and efficient real-time DoS attack detection with low computational overhead.

VI. DISCUSSION

The experimental results show that Machine Learning combined with Edge Computing is an effective approach for detecting DoS attacks in real time. Among the evaluated models, Logistic Regression achieved the best overall performance with 93.16% test accuracy, while XGBoost provided the highest ROC-AUC score (98.85%), demonstrating strong classification capability.

The system successfully distinguished Normal and DoS network traffic using the NSL-KDD dataset. Applying preprocessing techniques such as label engineering, feature selection, categorical encoding, feature scaling, and SMOTE significantly improved the model's performance and reduced the impact of class imbalance.

Challenges include:

- Detecting previously unseen or zero-day DoS attack patterns.
- Maintaining high accuracy while reducing false alarms.
- Ensuring consistent performance on real-time edge devices with limited resources.
- Improving scalability for large and high-speed network environments.
- Extending the system to support detection of multiple cyberattack categories beyond DoS.
- Overall, the proposed system demonstrates that Edge Machine Learning can provide fast, accurate, and scalable DoS attack detection, making it suitable for modern IoT and edge-based network security applications

VII. CONCLUSION AND FUTURE WORK

Conclusion
The proposed DoS Attack Detection System Using Edge Machine Learning successfully detects malicious network traffic with high accuracy using machine learning techniques. By combining effective data preprocessing, feature selection, and classification models, the system accurately distinguishes Normal and DoS traffic while reducing false detections. Deploying the detection model at the network edge enables faster response, lower latency, and reduced server load, making the solution suitable for modern IoT and edge computing environments.

Future Work

- Integrate Deep Learning models such as CNN and LSTM for improved attack detection.
- Extend the system to detect DDoS, Probe, R2L, and U2R attacks.
- Deploy the model on real edge devices such as Raspberry Pi and IoT gateways.
- Use modern datasets such as CICIDS2017 and CSE-CIC-IDS2018 for better real-world performance.
- Develop an automated real-time alert and response system for faster mitigation of network attacks.

REFERENCES

1. NSL-KDD Dataset, University of New Brunswick. NSL-KDD Data Set for Network Intrusion Detection Research.
2. XG Boost: A Scalable Tree Boosting System, Tianqi Chen and Carlos Guestrin, KDD Conference, 2016.
3. Random Forests, Leo Breiman, Machine Learning Journal, 2001.
4. An Introduction to Statistical Learning, Gareth James, Daniela Witten, Trevor Hastie, and Robert Tibshirani, Springer, 2021.
5. Edge Machine Learning for Intelligent IoT: A Survey, IEEE Communications Surveys & Tutorials, 2022