International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 8.141
Peer Reviewed Bi-Monthly
Vol. 7 No. 5 January – February - 2026

DDoS Attack Detection Using Machine Learning Classifiers

Mrs. Tejshri N. Shevate[1], Dr. Balendra Kumar Garg[2] & Dr. R. D. Kumbhar[3]

[1]*Research Scholar of MATS University Raipur, Chhattisgarh.*

[2]*Assistant Professor, MATS University, Raipur, Chhattisgarh*

[3]*Assistant Professor, KBPIMSR, Satara.*

Corresponding Author – Mrs. Tejshri N. Shevate

DOI - 10.5281/zenodo.18898056

Abstract:

Distributed Denial of Service (DDoS) attacks are one of the most serious security threats to modern computer networks and cloud environments. These attacks attempt to overwhelm network resources by generating a large volume of malicious traffic, causing service disruption to legitimate users. Traditional rule-based intrusion detection systems are not effective against evolving and large-scale DDoS attacks. To overcome these limitations, machine learning (ML) techniques have been widely adopted for automated and intelligent DDoS detection. This paper presents a comparative study of machine learning classifiers for DDoS attack detection using network traffic data. Popular classifiers such as Logistic Regression, Support Vector Machine, Decision Tree, Random Forest, and K-Nearest Neighbour are evaluated. Experimental results show that ensemble-based models, particularly Random Forest, achieve higher accuracy and better detection performance compared to individual classifiers. The results confirm that machine learning-based approaches are effective for detecting DDoS attacks in modern networks.

Keywords: DDoS, Intrusion Detection System, Machine Learning, Network Security, Classification

Introduction:

With the rapid growth of cloud computing, IoT, and online services, network security has become a critical concern. Among various cyber threats, Distributed Denial of Service (DDoS) attacks are the most damaging, as they can make services unavailable by flooding the target with malicious traffic. DDoS attacks are difficult to detect because they often resemble legitimate traffic and can be launched from multiple distributed sources.

Traditional intrusion detection systems (IDS) rely on predefined rules and signatures, which are not capable of identifying new or unknown attack patterns. Machine learning techniques provide a promising solution by learning traffic behaviour from data and automatically detecting abnormal patterns. This paper focuses on applying machine learning classifiers for efficient detection of DDoS attacks.

Literature Review:

Distributed Denial of Service (DDoS) attack detection has been widely studied using machine learning techniques due to their ability to analyze large volumes of network traffic and identify complex attack patterns. Early intrusion detection systems were mainly rule-based and signature-based, which required frequent updates and were ineffective against new and unknown attacks.

Sommer and Paxson (2010) highlighted the limitations of applying machine learning in real network environments, especially the high false positive rate caused by dynamic traffic behaviour. Their work emphasized the need for

robust feature selection and realistic datasets for intrusion detection research.

Tavallaee et al. (2009) analysed the KDD Cup'99 dataset and reported significant issues such as redundant records and outdated attack types. To address these limitations, Sharafaldin et al. (2018) introduced the CICIDS2017 dataset, which contains realistic network traffic and modern attack scenarios including DDoS attacks. This dataset has become a benchmark for recent DDoS detection studies.

Ullah et al. (2024) applied traditional machine learning classifiers such as Logistic Regression and Support Vector Machine for DDoS detection. Their results showed high detection accuracy; however, performance decreased when traffic patterns became more complex. This indicates that linear classifiers may not be sufficient for highly non-linear DDoS attack behaviors.

Decision Tree and K-Nearest Neighbor classifiers have also been explored for DDoS detection due to their simplicity and interpretability. While these models achieved good accuracy, they were sensitive to noisy data and suffered from scalability issues when applied to large datasets.

Recent studies have focused on ensemble learning methods. Tymoshchuk et al. (2024) proposed a neural network-based approach to classify different types of DDoS flooding attacks and achieved detection accuracy above 99%. Similarly, Random Forest and boosting-based models have shown superior performance by combining multiple weak learners and reducing overfitting. Hybrid approaches that combine feature selection techniques such as Principal Component Analysis (PCA) with machine learning classifiers have also gained attention. These methods reduce dimensionality, improve training efficiency, and lower false alarm rates. However, challenges such as class imbalance, real-time detection, and computational overhead still remain open research problems.

Research Gap:

From the existing studies, it is observed that although machine learning techniques are widely used for DDoS attack detection, several problems still remain unsolved. Many models generate too many false alarms, which makes it difficult to correctly identify real attacks in practical networks. Most existing approaches are trained only on known attack patterns and are not effective in detecting new or evolving DDoS attacks. In addition, many research works rely on old or limited datasets that do not represent current network traffic conditions. Another major issue is data imbalance, where normal and attack traffic are not evenly distributed, causing biased detection results. Most proposed models are tested only in offline environments and are not suitable for real-time DDoS detection. Some classifiers also face scalability and high computational cost issues when handling large-scale network traffic. Furthermore, limited attention has been given to feature optimization and fair comparison of multiple classifiers under the same experimental conditions. These gaps highlight the need for an efficient, scalable, and accurate machine learning-based DDoS detection system that can work effectively in real-world network and cloud environments.

Research Methodology:

This study proposes a machine learning–based approach to detect DDoS attacks using the CICIDS 2017 dataset. The methodology consists of data collection, preprocessing, feature selection, model training, and performance evaluation.

1. Dataset Description (CICIDS 2017):

The CICIDS 2017 dataset is a modern and realistic intrusion detection dataset that contains

normal network traffic and different types of attacks, including DDoS attacks. It includes network flow-based features such as flow duration, packet size, byte rate, and protocol information. The dataset closely represents real-world network behavior and is widely used in intrusion detection research.

2. Data Preprocessing:

The raw dataset contains missing values, infinite values, and redundant features. These issues are handled before applying machine learning models. Missing and infinite values are removed, and duplicate records are eliminated. Non-numeric attributes are converted into numeric form. All numerical features are normalized to improve classifier performance. The dataset is then split into training and testing sets using an 80:20 ratio.

3. Feature Selection:

To reduce dimensionality and improve detection efficiency, feature selection is applied. Correlation analysis is used to remove highly correlated and irrelevant features. This step reduces computational overhead and improves model accuracy by focusing only on the most important traffic features related to DDoS attacks.

Machine Learning Models:

The supervised machine learning classifiers are used for DDoS detection- Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), K-Nearest Neighbor (KNN) Each model is trained using labeled network traffic data to classify traffic as either normal or DDoS attack.

Model Training and Evaluation:

The models are trained using the training dataset and evaluated on the testing dataset. Five-fold cross-validation is applied to ensure stable and unbiased results. Model performance is measured using accuracy, precision, recall, and F1-score.

Proposed System:

The figure 1.1 illustrates the complete workflow of the proposed DDoS attack detection system using machine learning classifiers and the CICIDS 2017 dataset. The process begins with dataset collection, where network traffic data containing both normal and DDoS attack records is obtained. In the next step, data preprocessing is performed to clean the dataset by removing missing values, duplicates, and converting non-numeric features into numeric form. Feature selection is then applied to identify the most important network features related to DDoS attacks and to reduce computational complexity.

After feature selection, the dataset is divided into training and testing sets. The training data is used to train multiple machine learning classifiers such as Logistic Regression, Support Vector Machine, Decision Tree, Random Forest, and K-Nearest Neighbor. The trained models are then evaluated using the testing dataset. Performance evaluation is carried out using standard metrics such as accuracy, precision, recall, and F1-score. Based on the evaluation results, the best-performing model is selected for DDoS attack detection. Finally, the system classifies incoming network traffic as either normal or DDoS attack, completing the detection process.

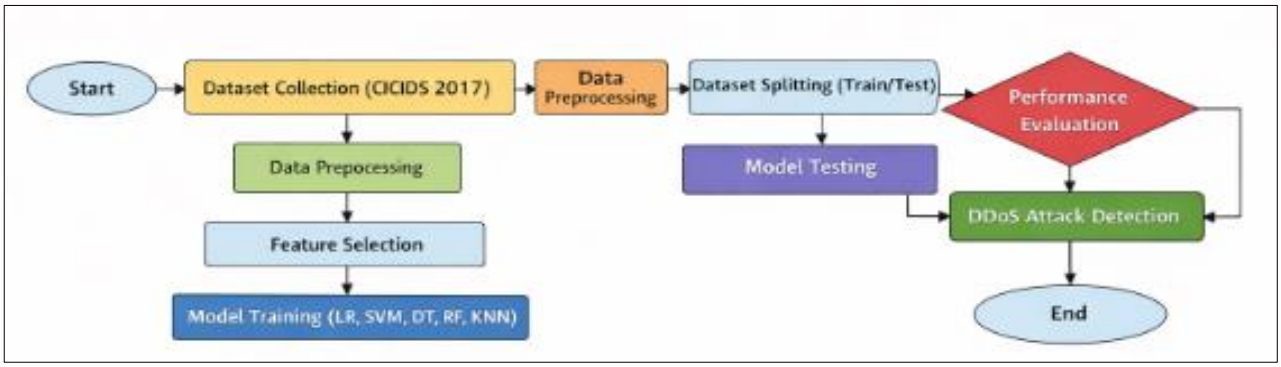

Figure 1.1 Workflow of the proposed DDoS attack detection

Data Analysis:

Data analysis is performed to understand traffic behavior and feature importance in the CICIDS 2017 dataset. It is observed that DDoS traffic has higher packet rates and shorter flow durations compared to normal traffic. Some features show strong correlation with attack behavior, indicating their importance in classification. The dataset shows class imbalance, where attack traffic is more frequent than normal traffic. This imbalance is handled during training to avoid biased results. Feature reduction significantly decreases training time while maintaining high detection accuracy.

The analysis confirms that preprocessing and feature selection are critical steps for improving machine learning performance in DDoS detection.

Results and Discussion:

1. Performance Comparison:

The performance of different machine learning classifiers on the CICIDS 2017 dataset is summarized below.

Classifier	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression	96.8	96.5	95.9	96.2
SVM	97.5	97.1	96.8	96.9
Decision Tree	98.1	97.9	98.0	97.9
KNN	97.6	97.4	97.2	97.3
Random Forest	**99.1**	**99.0**	**98.9**	**99.0**

2. Discussion:

The experimental results show that all machine learning classifiers perform well in detecting DDoS attacks. Logistic Regression and SVM provide good baseline performance but struggle with complex traffic patterns. Decision Tree improves detection but may overfit the data. KNN performs well but requires higher computation for large datasets. Random Forest achieves the best performance due to its ensemble learning capability, resulting in higher accuracy and lower false alarms. These results demonstrate that ensemble-based models are more effective for DDoS detection in modern network environments.

Conclusion:

This study demonstrates that machine learning classifiers can effectively detect DDoS attacks using the CICIDS 2017 dataset. Among the evaluated models, Random Forest provides the highest detection accuracy and reliability. Proper data preprocessing and feature selection significantly improve performance. Future work will focus on real-time detection and deep learning-based approaches for large-scale networks.

References:

1. Sommer, R., & Paxson, V., "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *IEEE Symposium on Security and Privacy*, pp. 305–316, 2010.
2. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A., "A Detailed Analysis of the KDD CUP 99 Data Set," *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009.
3. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A., "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 2018.
4. Ullah, I., Mahmoud, Q. H., & Kumar, M., "Detecting Distributed Denial of Service Attacks Using Machine Learning Techniques," *arXiv preprint*, 2024.
5. Tymoshchuk, O., et al., "Detection and Classification of DDoS Flooding Attacks Using Neural Networks," *arXiv preprint*, 2024.
6. Buczak, A. L., & Guven, E., "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
7. Moustafa, N., & Slay, J., "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," *Military Communications and Information Systems Conference (MilCIS)*, 2015.
8. Breiman, L., "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
9. Cortes, C., & Vapnik, V., "Support-Vector Networks," *Machine Learning*, vol. 20, pp. 273–297, 1995.
10. Scikit-learn Developers, "Scikit-learn: Machine Learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.