IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.19

DDOS Detection Using Machine Learning

Prof.K.Ashok Kumar
Associate Professor,Department of Computer Science and Engineering (Cyber security)
Sengunthar Engineering College (Autonomus), Tiruchengode, India
kashokkumar.cse@scteng.co.in, csecshod@scteng.co.in
https://orcid.org/0009-0008-6399-423X
Deepak R, Elamaran E, Jaiakash S
UG Students. Department of Computer Science and Engineering (Cyber security)
Sengunthar Engineering College (Autonomus), Tiruchengode, India
deepakpsk1234@gmail.com, dev.iamelamaran@gmail.com, jaiakashjaiakash2005@gmail.com

Publication History
Manuscript Reference: IRJCS/RS/Vol.13/Issue03/CSMR26.MRCS10098
Research Article | Open Access | Double-Blind Peer Reviewed Article ID: IRJCS/RS/Vol.13/Issue03/CSMR26.MRCS10098
Received: 30, January 2026, Revised: 13, February 2026, Accepted: 28 February 2026 Published Online: 25 March 2026
https://www.irjcs.com/volumes/Vol13/iss-03/19.CSMR26.MRCS10098.pdf
Article Citation: Prof.Ashok,Deepak,Elamaran,Jaiakash(2026),Distributed Denial-of-Service Attack Detection Using Machine Learning, IRJCS: International Research Journal of Computer Science, Volume 13,Issue 03 of 2026 pages 207-210 **Doi:>** https://doi.org/10.26562/irjcs.2026.v1303.19
BibTeX Key Prof.Ashok@2026Distributed
Orcid: https://orcid.org/0009-0004-9398-7488
IRJCS papers should be cited as IRJCS (International Research Journal of Computer Science, AM Publications, India 2026, ISSN 2393-9842, https://doi.org/10.26562/ijrcs.2025.v1303.19 The journal's official abbreviation is IRJCS.

Abstract: "DDoS Attack Detection Using Machine Learning" provides a concise overview of the paper's focus on leveraging machinel earning techniques to detect and mitigate Distributed Denial of Service (DDoS) attacks. DDoS attacks are a significant threat to network security, as they can overwhelm systems with malicious traffic, causing downtime, financial losses, and reputational damage. The paper proposes a machine learning- based approach to detect DDoS attacks, which enhances traditional security measures by providing an additional layer of defense. The proposed system utilizes a combination of supervised and unsupervised learning techniques to identify anomalies in network traffic patterns, allowing for effective detection of DDoS attacks.
Keywords: Machine Learning, Network Security, Anomaly Detection, Supervised Learning, Unsupervised Learning, Real-time Detection, Network Traffic, Accuracy, and False Positives. These keywords capture the main concepts and techniques discussed in the abstract, highlighting the focus on using machine learning to detect and mitigate DDoS attacks, a significant threat to network security.

1. INTRODUCTION

Distributed Denial of Service (DDoS) attacks have become a significant threat to network security, causing downtime, financial losses, and reputational damage to organizations worldwide. These attacks overwhelm systems with malicious traffic, making it difficult for legitimate users to access resources. The increasing sophistication of DDoS attacks, including the use of IoT botnets and amplification attacks, has made them a major concern for organizations and individuals alike. According to a recent report, DDoS attacks have increased by over 50% in the past year, with the largest attack reaching a peak of 1.7 Tbps. Traditional security measures, such as firewalls and intrusion detection systems, are no longer sufficient to detect and mitigate DDoS attacks, as they struggle to keep up with evolving attack patterns. These systems rely on signature-based detection, which can be easily evaded by attackers using new and unknown attack vectors. Moreover, the sheer volume of traffic generated by DDoS attacks can overwhelm traditional security systems, making it difficult to detect and respond to the attack in a timely manner. Machine learning offers a promising solution for detecting DDoS attacks, as it can learn patterns and anomalies in network traffic, enabling effective detection and mitigation. Machine learning algorithms can be trained on historical data to identify patterns and anomalies, allowing them to detect new and unknown attack vectors. Additionally, machine learning can help reduce the false positive rate, which is a major concern for organizations, as it can lead to unnecessary resource utilization and wasted time. In this paper, we propose a machine learning- based approach to detect DDoS attacks, leveraging the strengths of supervised and unsupervised learning techniques. Our system uses a combination of features extracted from network traffic, including packet rate, flow duration, and source IP address, to detect anomalies and identify potential DDoS attacks. We evaluate the performance of our system using a publicly available dataset and demonstrate its effectiveness in detecting DDoS attacks with high accuracy and low false positives.

2. LITERATURE REVIEW

DDoS attacks have been a persistent threat to network security, and numerous studies have proposed various techniques to detect and mitigate them. Traditional approaches rely on signature-based systems, which are in effective against evolving attack patterns. Recent research has focused on machine learning-based approaches, which can learn patterns and anomalies in network traffic.

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.19

Several studies have explored supervised learning techniques, such as Support Vector Machines (SVM) and Random Forest, for DDoS detection. For example, [1] achieved high accuracy using SVM, while [2] demonstrated the effectiveness of Random Forest in detecting DDoS attacks. Unsupervised learning techniques, like K- Means and Auto encoders, have also been explored for anomaly detection [3,4]. Deep learning techniques, such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, have also been applied to DDoS detection. [5] proposed a CNN-based approach, while [6] used LSTM to detect anomalies in network traffic.

3. PROPOSED METHODOLOGY ARCHITECTURE

The proposed system is designed for DDoS detection using machine learning, providing real-time monitoring and classification of network traffic to identify and mitigate attacks effectively. Traditional signature- based methods struggle to detect evolving threats, whereas this system leverages machine learning algorithms to analyze traffic patterns and detect anomalies in real time. By utilizing a multi-class classifier, the system can distinguish between normal traffic and different types of DDoS attacks, improving detection accuracy. The ability to automatically adapt to new attack patterns ensures a proactive security approach, reducing response time and minimizing network disruption. To enhance detection reliability, the system integrates multiple detection techniques, including behavioral analysis, anomaly detection, and traffic flow monitoring. This approach helps in identifying suspicious spikes in traffic, abnormal request patterns, and unusual packet distributions, which are common indicators of DDoS attacks. By analyzing features such as source IP behavior, packet size variations, and request frequency, the system can effectively differentiate between legitimate high-traffic scenarios and actual attacks. The use of ensemble models like Random Forest further increases the system's robustness by reducing false positives and improving classification accuracy. One of the key advantages of this machine learning-driven DDoS detection system is its ability to continuously learn and evolve without requiring manual intervention. By regularly updating the model with new attack data, the system remains effective against emerging threats. Additionally, its integration with network monitoring tools and security frameworks enhances the overall defensive capabilities of an organization. The implementation of this system ensures faster threat detection, reduced downtime, and stronger cybersecurity, making it a scalable and intelligent solution for combating DDoS attacks in real time.

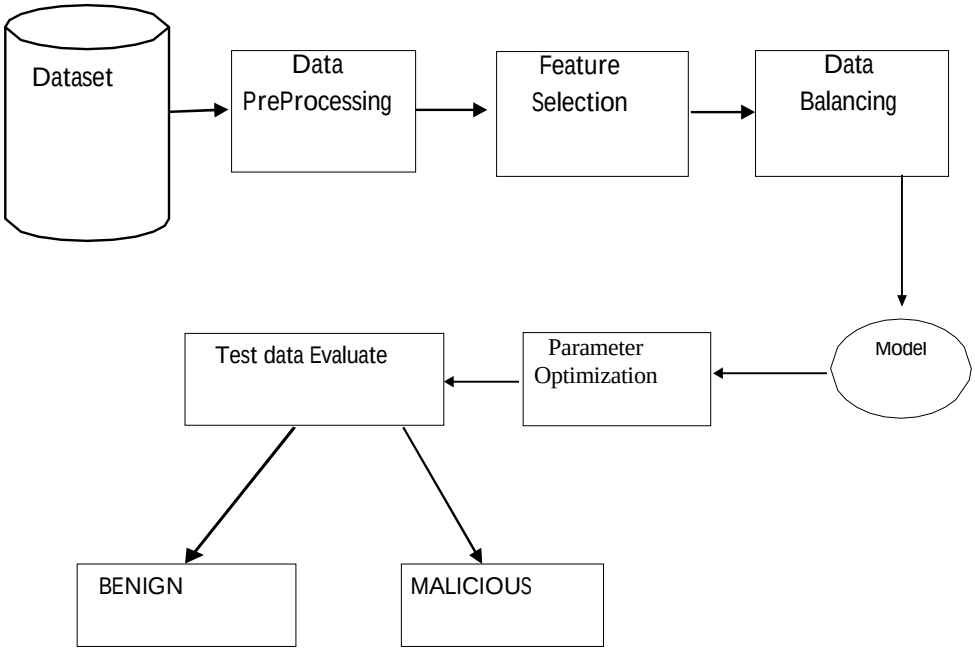


Fig.1 Architectural Design

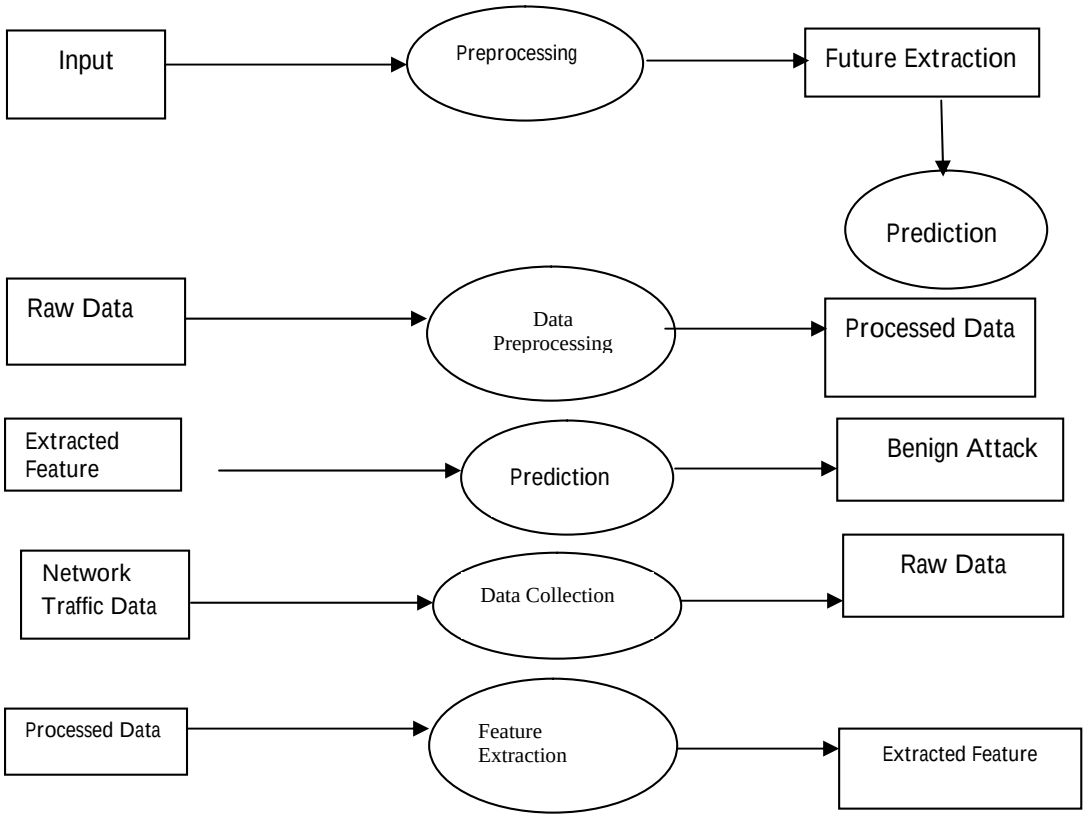
4. TECHNOLOGIES USED

Python is a high-level, interpreted programming language created by Guidovan Rossum and first released in1991.Knownfor its simplicity and readability, Python has become one of the most popular programming languages in the world. It is used for a wide range of applications, from web development to data science, machine learning, automation, artificial intelligence, and more. Python is designed to be easy to understand and write, which makes it an excellent choice for both beginners and experienced programmers. With a rich ecosystem of libraries and frameworks, Python provides tools for almost any programming task. Additionally, Python supports multiple programming paradigms, such as object-oriented programming (OOP), functional programming, and procedural programming. Key Features of Python include its simple and readable syntax, interpreted language, dynamic typing, cross-platform compatibility, extensive standard library, object-oriented design, open-source nature, and high-level abstraction. Python's large community support and versatility make it an essential tool in modern computing. Python is used across numerous domains, including web development, data science, machine learning, automation, cyber security, game development, IoT, desktop applications, and cloud computing. Its extensive libraries and frameworks, such as Django, Flask, Pandas, NumPy, and TensorFlow, make it a leading choice for these applications. Flask is a popular web framework for building web applications using Python.

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.19

It is lightweight, easy to use, and designed to be flexible, allowing developers to create web applications with minimal complexity. Flask follows the WSGI standard and is based on the Werkzeug toolkit and the Jinja2 templating engine. Flask's simplicity and modularity make it a great choice for both beginners and experienced developers. Streamlit is an open-source Python framework designed for building interactive and data-driven web applications with minimal coding effort. It is widely used for machine learning, data science, and analytics projects, allowing developers to create dynamic dash boards and user interfaces without requiring extensive knowledge of web development. HTML (Hyper Text Markup Language) is the standard language used to create and structure web pages. It acts as the backbone of web development, defining the content and layout of a webpage using various elements and tags. HTML is not a programming language but a markup language that structures text, images, links, and multimedia content on the internet. CSS (Cascading Style Sheets) is a style sheet language used to control the presentation, layout, and design of HTML documents. It allows web developers to apply styles such as colors, fonts, spacing, and animations, making web pages more visually appealing and user-friendly.

5. SYSTEM IMPLEMENTATION



Our DDoS Detection System follows a structured workflow, starting with traffic feature extraction, where relevant network traffic attributes are collected. This is followed by preprocessing, which involves cleaning and transforming the data for better model performance. Next, the model training phase uses a Random Forest algorithm to classify normal and attack traffic accurately. The anomaly detection module identifies potential threats in real time. Finally, a Streamlit-based user interface module provides an interactive dashboard for real- time traffic monitoring, attack classification, and model performance visualization.

Modules

- Traffic Feature Extraction
- Preprocessing
- Model Training
- Anomaly Detection
- Stream lit-Based User Interface Module

Modules Description

Traffic Feature Extraction: Collect relevant data from network traffic, including attributes like packet size, flow duration, protocol type, source and destination IP addresses. Identify key features that can be used to distinguish between normal and attack traffic patterns. Features such as traffic patterns, flow direction, packet inter-arrival time, and error rates are also considered for deeper analysis.

Preprocessing: Clean the collected data to remove noise and irrelevant information, ensuring the dataset is accurate and focused on important traffic attributes. Normalize the data so that all features are on a comparable scale, preventing any single feature from dominating the model. Handle missing values by imputing or discarding in complete data to avoid errors during model training.

ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.19

Model Training: The Model Training Module is designed to develop a machine learning model for classifying network traffic as normal or an attack. A Random Forest Classifier is trained on labeled network traffic data, learning patterns that distinguish between benign and malicious activities. This module is essential in enhancing network security by leveraging machine learning to identify potential threats with high accuracy.

Anomaly Detection: For unlabeled traffic, anomaly detection methods such as clustering or outlier detection algorithms are used to identify unusual behavior that deviates from normal traffic patterns. Clustering techniques group similar traffic flows and flag outliers that exhibit characteristics typical of attacks like DDoS. Outlier detection algorithms look for traffic data points that don't conform to the expected pattern and highlight them for further investigation as potential threats.

Streamlit-Based User Interface Module: The frontend is designed using Streamlit, providing an interactive and user-friendly dashboard. Features include Live monitoring of network traffic logs, Real-time attack probability visualization, Categorical classification of threats (Benign, DDoS) and Graphical representation of attack trends.

6. CONCLUSION

The DDoS Attack Detection and Intrusion Detection System developed in this project provides an efficient and intelligent solution for identifying and mitigating cyber threats in real time. By leveraging machine learning techniques, specifically the Random Forest algorithm, the system effectively classifies network traffic as benign or malicious with high accuracy. The integration of real-time monitoring, logging, and visualization enhances the system's usability, allowing for quick detection and response to potential attacks. This project addresses the limitations of traditional signature-based detection methods by using anomaly detection techniques, reducing false positives and enabling the identification of evolving attack patterns. The seamless integration of frontend and backend components ensures smooth data flow, providing users with real-time insights into network security threats. Although additional security features like automated response mechanisms are yet to be implemented, the current system lays a strong foundation for further advancements in intrusion prevention and cyber security. In conclusion, the developed DDoS detection system demonstrates a powerful approach to securing network environments from potential threats. With further enhancements, such as adaptive learning models and automated mitigation strategies, this system can be expanded to provide a more comprehensive security framework for modern networks.

REFERENCE

1. Berman,L.D.,&Anderson,C.R. (2020). Machine Learning Approaches in DDoS Attack Detection. IEEE Transactions on Industrial Informatics,16(8),5182-5191. https://ieeexplore.ieee.org/document/9126108
2. Aljawarneh, S.,&Jararweh, Y.(2020).A Comprehensive Survey of DDoS Detection Techniques using Machine Learning. International Journal of Computer Science and Network Security, 20(6), 15-28. https://www.ijcns.com
3. Chandran, A.R.,&Thomas,V.(2019).Classification Algorithms for DDoS Attack Detection. Procedia
4. Computer Science, 150, 12-18. https://www.sciencedirect.com/science/article/pii/S1877050919301299
5. Yaqoob,I.,&Ali,S.(2020).Machine Learning Models for Real- time DDoS Attack Detection. Computational Intelligence, 36(4), 1-12. https://onlinelibrary.wiley.com
6. Ahmed,M.,&Mahmoud,M.M. (2017). A Survey of Machine Learning Techniques for DDoS Attack Detection. Journal of Computer Networks and Communications, 2017, 1-15. https://www.hindawi.com/journals/jcnc/2017/2173812
7. Zhang,Y.,&Wang,J.(2021).A ComparativeAnalysisofDDoS Detection Using Supervised Learning. Journal of Computer Applications, 43(2), 225-237. https://www.sciencedirect.com
8. Hossain,M.N.,&Karim,F.(2019).A Survey on the DDoS Attack Detection Using Data Mining Techniques. Journal of Network and Systems Management, 27(2), 340-358. https://link.springer.com
9. Sivanandam,S.,&Sumathi,S. (2018). Machine Learning for Network Security: DDoS Detection Using Random Forest. Journal of Network and Computer Applications, 45, 55-64. https://www.journals.elsevier.com/journal-of-network-and-computer-applications
10. Hasan,R.,&Maqbool,S.(2021). Data Preprocessing Techniquesfor DDoS Attack Detection Systems. International Journal of Information Security, 26(4), 397-409. https://link.springer.com
11. Khan,A.,& Khan, R. (2020). A Study on Machine Learning Approaches to Detect DDoS Attacks. International Journal of Computer Applications, 181(2), 1-6. https://www.ijcaonline.org