International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

A Framework for Machine Learning-Based Intrusion Detection to Find Denial of Service Attacks in Network Traffic

K Naresh[1], Bollepalle Jhansi[2]

[1]Assistant Professor, Department of MCA, Annamacharya Institute of Technology and Sciences, Tirupati, Andhra Pradesh, India.

[2]Postgraduate, Department of MCA, Annamacharya Institute of Technology and Sciences, Tirupati, Andhra Pradesh, India.

How to Cite this Article:

Jhansi, B. (2026). A Framework for Machine Learning-Based Intrusion Detection to Find Denial of Service Attacks in Network Traffic. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.059

https://doi.org/10.55041/ijcope.v2i4.059

Abstract

In contemporary network systems, denial of service (DoS) assaults are among the most prevalent and disruptive cyberthreats. By overloading network resources, these attacks seek to prevent genuine users from accessing services. Because of the growing complexity and volume of network traffic, traditional intrusion detection systems frequently fail to detect such attacks. This paper suggests a machine learning-based intrusion detection system intended to successfully identify DoS assaults as a solution to this problem. The suggested approach trains a machine learning model that can differentiate between benign and malicious traffic patterns using network traffic data. To enhance model performance, data preparation methods including feature scaling and feature selection are used.

Real-time traffic analysis and threat detection are made possible by integrating the trained model into a web application created with the Flask framework. To detect possible DoS attacks, the system evaluates network traffic characteristics and categorises them using the taught machine learning model. The suggested method can successfully identify malicious traffic and enhance network security, according to experimental results. In addition to helping network managers monitor and safeguard network infrastructures against cyber threats, the created framework offers a scalable and effective way to detect denial of service attacks.

Keywords

Machine Learning, Intrusion Detection System, Denial of Service Attack, Network Security, Cybersecurity, Flask Web Application

I. Introduction

Network security is now a major worry for both individuals and organisations due to the internet's and digital communication systems' explosive expansion. Many internet services, including cloud computing, e-commerce, online banking, and digital communication platforms, are supported by modern networks, which manage massive amounts of data. Cyber attacks have consequently grown dramatically, putting critical data and network infrastructure at grave risk. Denial of Service (DoS) assaults are regarded as one of the most prevalent and destructive threats that can interfere with network operations.

When an attacker tries to stop a network service by flooding it with too much traffic, this is known as a denial of service attack. By using up network resources like bandwidth, memory, and processing power, this malicious traffic stops authorised customers from using the service. Because attackers are always changing their tactics and patterns, traditional security measures like firewalls and rule-based intrusion detection systems are frequently unable to identify these attacks. Intelligent technologies that can examine network traffic patterns and automatically identify abnormalities are therefore required.

An efficient method for identifying cyberattacks in network environments is machine learning. Machine learning algorithms can identify patterns linked to both benign and malevolent activity by examining past network traffic data. Then, in real time, these models can be used to categorise incoming communications and spot possible threats. Large datasets may be handled by machine learning-based intrusion detection systems, which can also adjust to new attack patterns and increase detection accuracy.

This paper proposes an intrusion detection framework based on machine learning to identify Denial of Service attacks in network data. The system trains a classification model that can recognise harmful activity using characteristics of network traffic. A web-based application created with the Flask framework incorporates the trained model, enabling users to monitor possible threats and analyse network data via an interactive interface. By offering a clever and effective way to identify DoS assaults, the suggested approach seeks to improve network security.

II. Problem Statement

The fast growth of network-based services has led to an increase in the frequency and sophistication of cyberattacks. By flooding servers and network resources with excessive traffic, Denial of Service (DoS) attacks represent a serious danger to network infrastructure. These assaults cause system outages, monetary losses, and diminished confidence in digital platforms by preventing authorised users from accessing services. To detect malicious activity, traditional intrusion detection systems mostly use signature-based techniques and pre-established criteria. However, these methods may lead to significant false positive rates and are frequently ineffectual against novel or unidentified assault types.

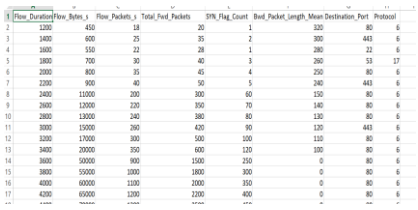
Furthermore, the increasing volume and complexity of network traffic make manual monitoring and rule-based detection systems inadequate for real-time threat identification. As attackers continuously modify their strategies, it becomes difficult for traditional security systems to adapt quickly. Therefore, there is a need for an intelligent and automated system capable of analyzing network traffic patterns and accurately detecting malicious behavior. Machine learning techniques provide an effective solution by learning patterns from historical network data and identifying anomalies that may indicate potential attacks. This research focuses on developing a machine learning-based intrusion detection framework to effectively detect Denial of Service attacks and improve overall network security. Furthermore, rule-based detection systems and human monitoring are insufficient for real-time threat identification due to the growing amount and complexity of network data. Traditional security systems find it challenging to swiftly adjust as attackers constantly alter their tactics. As a result, an automated and intelligent system that can precisely identify fraudulent activity and analyse network traffic patterns is required. By learning patterns from past network data and spotting abnormalities that can point to possible assaults, machine learning techniques offer a practical answer. The goal of this project is to create an intrusion detection system based on machine learning that can efficiently identify Denial of Service attacks and enhance network security in general.

III. Objectives of the Study

The primary goal of this research is to create an intelligent intrusion detection system that uses machine learning techniques to detect Denial of Service assaults. The goal of the study is to examine network traffic data and find trends that set harmful activity apart from legitimate traffic. The device may automatically identify suspicious activity and help network administrators safeguard network resources by using machine learning algorithms. Preprocessing and analysing network traffic characteristics to increase attack detection accuracy is another goal of this research. Additionally, the study focuses on developing and assessing a machine learning model that can distinguish between normal and attack types of network traffic.

Furthermore, a web-based application created with the Flask framework incorporates the taught machine learning model into the suggested system. Through an easy-to-use dashboard, this interface enables users to monitor possible risks and analyse traffic data. The study's overall goal is to improve network security by offering a scalable and effective method for identifying Denial of Service threats.

IV. Dataset:



Flow_Duration	Flow_Bytes_s	Flow_Packets_s	Total_Fwd_Packets	SYN_Flag_Count	Bwd_Packet_Length_Mean	Destination_Port	Protocol
1200	450	18	20	1	320	80	6
1400	600	25	35	2	300	443	6
1600	550	22	28	1	280	22	6
1800	700	30	40	3	260	53	17
2000	800	35	45	4	250	80	6
2200	900	40	50	5	240	443	6
2400	11000	200	300	60	150	80	6
2600	12000	220	350	70	140	80	6
2800	13000	240	380	80	130	80	6
3000	15000	260	420	90	120	443	6
3200	17000	300	500	100	110	80	6
3400	20000	350	600	120	100	80	6
3600	50000	900	1500	250	0	80	6
3800	55000	1000	1800	300	0	80	6
4000	60000	1100	2000	350	0	80	6
4200	69000	1200	2200	400	0	80	6

Fig: Dataset

The study's dataset includes network traffic characteristics that are frequently used to spot unusual network activity and possible Denial of Service (DoS) assaults. These characteristics include protocol information, connection duration, packet counts, and packet sizes, among other aspects of network flows. The machine learning algorithm may identify patterns linked to both harmful and regular traffic by examining these characteristics. Numerous significant network flow

parameters are included in the dataset. A network flow's overall duration is represented by the Flow Duration feature, which aids in spotting abnormally long or short connections that can point to questionable activity. The data transmission rate within the flow is indicated by Flow Bytes per Second (Flow_Bytes_s), which is helpful for identifying high traffic volumes commonly linked to DoS attempts.

Similar to this, Flow Packets per Second (Flow_Packets_s) counts the number of packets sent in a second and aids in spotting unusual packet transmission rates.

Total Forward Packets, which shows how many packets are sent from the source to the destination during a network session, is another significant feature in the dataset. Abnormal traffic behaviour may be indicated by an abrupt increase in this figure. The SYN Flag Count function keeps track of how many SYN packets are transmitted while establishing a connection. This feature is essential for identifying SYN flood attacks since many DoS attacks take advantage of the TCP handshake procedure by sending an excessive number of SYN requests.

Additionally, Backward Packet Length Mean (Bwd_Packet_Length_Mean), which shows the average packet size in the opposite direction of the communication flow, is included in the dataset. This facilitates the analysis of the server's response behaviour during a connection. Furthermore, Destination Port determines the network communication's target port, which might highlight trends associated with attacks against particular services like HTTP or HTTPS. The Protocol feature helps differentiate between various kinds of network traffic by indicating the type of network protocol that is being used, such as TCP or UDP.

The machine learning model can efficiently analyse traffic behaviour and categorise it as either harmful or normal by using these network traffic properties. The suggested intrusion detection system can more accurately identify possible DoS assaults because to the dataset's structured representation of network flow characteristics.

V. Proposed System Architecture

The suggested solution uses an intrusion detection framework based on machine learning to identify and counteract Denial of Service threats. The architecture is made up of a number of parts that cooperate to examine network data, spot malicious activity, and stop questionable activity. Network traffic data, which includes a variety of characteristics like packet rate, packet size, protocol type, destination port, and SYN flag count, is first

collected by the system. The machine learning model uses these characteristics as inputs.

Data cleaning, feature extraction, and feature scaling are carried out at the preprocessing stage of the network traffic data collection. Before the data is utilised for model training, this phase makes sure that it is correctly prepared and normalised.

To train the machine learning classifier, the dataset is split into training and testing sets after preprocessing. The trained model creates a predictive model that can recognise unusual network activity by learning patterns linked to both attack and normal traffic. Following training, the model is included into a web application built on Flask that enables real-time network traffic monitoring. After receiving network traffic data, the web application sends it to a machine learning model that has been trained for classification. The system logs the attack information and bans the attacker IP address right away if the model detects abnormal activity, such as a possible DoS attempt. Additionally, the system keeps threat data in a database for later examination.

Fig: Architecture

The suggested framework offers an interactive dashboard with real-time threat logs, blacklisted IP addresses, and attack data. This architecture increases the overall security of the network infrastructure by enabling network administrators to keep an eye on network activity and react swiftly to possible attacks.

VI. Experimental Results and Analysis

The network traffic dataset was used in a number of experiments to assess the efficacy of the suggested machine learning-based intrusion detection system. Numerous network flow characteristics, including flow time, packet rate, packet size, protocol type, and SYN flag count—all crucial markers for spotting unusual network activity—were included in the dataset. These characteristics were used to train the machine learning model to identify malicious or benign network traffic.

To assess the model's performance, the dataset was split into training and testing subsets during the training phase. To increase the machine learning algorithm's accuracy, data preprocessing methods including feature scaling and normalisation were used.

Following training, the model was able to identify denial-of-service attack patterns and differentiate them from typical traffic flows.

To conduct real-time traffic analysis, the trained model was included into the Flask-based NetGuard IDS web application. The model evaluates the input features and forecasts if the traffic indicates a possible attack when fresh network traffic data is entered into the system. When an attack is identified, the system automatically blocks the associated IP address and logs the incident in the threat log.

The experimental findings show that both DoS and DDoS attacks can be successfully detected by the suggested method. Numerous statistics are shown on the monitoring dashboard, such as the total number of threats identified, the quantity of DoS attacks, DDoS attacks, and blacklisted IP addresses.

Each detected assault's source IP address, protocol, destination port, attack type, confidence score, and throughput are all documented in the threat log. These findings show that the machine learning model effectively detects questionable network activity and contributes to enhancing network infrastructure security.

VII. Discussion

By examining a variety of network traffic characteristics, the suggested machine learning-based intrusion detection system successfully detects denial of service assaults. By identifying patterns in the dataset, the system is able to differentiate between malicious and legitimate traffic flows. Real-time monitoring and visualisation of attack events are made possible by the model's interaction with the NetGuard IDS dashboard. Important information is recorded by the system, including the attack category, protocol type, source IP address, and confidence score. This enables network managers to promptly comprehend attack behaviour and take appropriate action. The machine learning approach enhances detection capability and

adaptability as compared to conventional rule-based systems. However, by using sophisticated algorithms and training the model on bigger datasets, more advancements can be made.

VIII. Conclusion

A machine learning-based intrusion detection system for identifying denial-of-service attacks in network data was reported in this paper. The system uses a trained machine learning model to classify traffic after analysing different aspects of network flow. A Flask-based web application that offers a real-time monitoring dashboard for examining assault events is integrated with the model. The technology can effectively identify DoS and DDoS attacks and automatically block malicious IP addresses, according to experimental data. By facilitating quicker and more precise attack detection, the suggested framework enhances network security. Future research can concentrate on enhancing the system's ability to identify various cyberattacks and applying deep learning methods to boost efficiency.

References

[1] C. F. Tsai, Y. F. Hsu, C. Y. Lin, and W. Y. Lin, “Intrusion Detection by Machine Learning: A Review,” Expert Systems with Applications, vol. 36, no. 10, pp. 11994–12000, 2009.

[2] R. Sommer and V. Paxson, “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,” in Proceedings of the IEEE Symposium on Security and Privacy, 2010, pp. 305–316.

[3] A. L. Buczak and E. Guven, “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.

[4] G. Kim, S. Lee, and S. Kim, “A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection,” Expert Systems with Applications, vol. 41, no. 4, pp. 1690–1700, 2014.

[5] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly Detection: A Survey,” ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, 2009.