IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

REAL TIME DDOS DETECTION AND MITIGATION USING MACHINE LEARNING

[1] Jean R, [2] Marimuthu M, [3] Jeswin Jebasolomon Asir J S A, [4] Mrs. Padma Sundari E

[1]Student, [2] Student, [3] Student, [4] Assistant Professor
[1] Computer Science and Engineering,
[1] Francis Xavier Engineering College, Tirunelveli – Tamil Nadu – India

Abstract:

driven anomaly detection, real-time traffic analysis, and automated response mechanisms. Utilizing XGBoost, MLP, and Random The AI-powered real-time DDoS detection and mitigation system enhances network security by integrating machine learning-Forest, the system efficiently identifies malicious traffic patterns, preventing large-scale attacks before they disrupt network operations. Automated mitigation techniques proactively block suspicious IPs, reducing manual intervention and ensuring minimal downtime. The system features a real-time monitoring dashboard, providing live insights into traffic behavior, attack sources, and mitigation actions. By continuously learning from attack patterns, the system adapts to emerging threats, offering a scalable, proactive, and intelligent defence against DDoS attacks. This approach strengthens network resilience, improves service availability, and optimizes cybersecurity management.

Keywords: DDoS Detection, Machine Learning, Cybersecurity, Anomaly Detection, Network Protection, Real-Time Monitoring, Automated Mitigation.

Introduction:

The increasing frequency and sophistication of Distributed Denial-of-Service (DDoS) attacks pose a major challenge to modern network security, leading to service disruptions, financial losses, and data breaches. The inability of rule-based security systems to keep up with changing attack patterns frequently leads to sluggish responses and extended downtime. To address these issues, this project introduces an AI-powered real-time DDoS detection and mitigation system that leverages machine learning models such as XGBoost, MLP, and Random Forest for enhanced threat detection and prevention.

M, according to R. Masthan and Ravi, malware attacks are becoming increasingly sophisticated, making conventional security approaches ineffective. Our system overcomes these limitations by employing real-time traffic analysis and anomaly detection, ensuring proactive identification of malicious traffic before it causes severe damage. The system is able to apply intelligent rate-limiting, block suspicious IP addresses, enforce adaptive firewall rules, and reduce the need for manual intervention thanks to the integration of automated mitigation mechanisms. Additionally, a real-time security dashboard provides network administrators with attack visualization, traffic analytics, and mitigation insights, enabling efficient cybersecurity management. With its ability to learn from emerging threats and adapt dynamically, this system offers a scalable, proactive, and intelligent defense against modern DDoS attacks. This project significantly enhances cybersecurity infrastructure and robust threat mitigation by ensuring network resilience, reducing operational costs, and maintaining continuous service availability. In addition to real-time threat detection, our system enhances scalability by adapting to varying network loads and attack patterns. The integration of automated responses minimizes human intervention, ensuring a faster and more efficient mitigation process. By continuously learning from new attack strategies, the system evolves to counter even the most sophisticated DDoS threats, providing a robust solution.

AI-driven detection enhances security by classifying network traffic in real time, distinguishing legitimate users from attackers. Using models like XGBoost and MLP, the system adapts to new threats, ensuring minimal false positives and uninterrupted service.

Problems With Centralized DDos Mitigation System

Traditional DDoS mitigation systems often rely on centralized security architectures, which introduce several challenges such as single points of failure, slow response times, and scalability limitations. According to K. Praghash, M. Masthan, and R. Ravi, centralized security systems are more vulnerable to large-scale attacks that can overwhelm a single mitigation point, rendering defenses ineffective. Additionally, these systems often require manual intervention, leading to delayed threat response and increased downtime. The reliance on predefined rules makes them less effective against evolving attack patterns. These challenges highlight the need for an AI-powered, real-time DDoS detection and mitigation system that leverages machine learning for adaptive security, ensuring faster response times, reduced downtime, and enhanced network resilience.

Real Time DDos Detection System:

The real-time DDoS detection system is an AI-driven cybersecurity technology that allows network traffic to be monitored in a secure and tamper-resistant manner. It started out as a way to protect against Distributed Denial-of-Service (DDoS) attacks, but it has since been used for a lot of other cybersecurity applications. In this system, network traffic patterns are recorded across multiple monitoring points in a decentralized and transparent manner. Each traffic log contains an anomaly detection signature linked to previous observations, which creates a continuous security record, hence the name "real-time detection system." This ensures that any attempts to manipulate or disguise malicious traffic will be immediately detected and mitigated by the system.

One of the key benefits of this AI-powered detection system is that it eliminates the need for manual intervention, allowing for automated and adaptive threat mitigation. It also provides a high level of security, transparency, and scalability, making it ideal for applications such as financial services, cloud security, and government agencies. A real-time DDoS detection system is one that keeps track of potential threats and continuously analyzes traffic on digital networks. In this system, each detected threat is represented by a unique identifier called an anomaly signature. This signature is generated using complex machine learning algorithms that are designed to be highly adaptive and resistant to evasion techniques. Once a threat is identified, it is logged and responded to in a linear, Chronological order, forming an automated and adaptive defense system. Attack patterns are validated across multiple network nodes, ensuring accuracy and resistance to manipulation. The attack data is synchronized at each monitoring point for a unified defense. Once a malicious source is detected, it is flagged and blocked instantly. This system creates a secure and scalable cybersecurity solution, protecting banking systems, e-commerce platforms, cloud services, and enterprises from evolving threats.

Encryption System in DDoS System:

Encryption plays a vital role in securing network communications and protecting sensitive data from malicious attacks. In DDoS detection systems, encryption is used to ensure the confidentiality and integrity of network traffic, preventing attackers from intercepting or tampering with critical information. Public-key cryptography provides a secure mechanism for encrypting data transmissions, ensuring that only authorized entities can access network logs and security policies.Additionally, encryption techniques help safeguard communication between the detection system and administrators by preventing unauthorized access to alerts and mitigation actions. Hashing algorithms further enhance security by generating unique identifiers for network packets, making it easier to detect anomalies and prevent data manipulation. By integrating encryption with real-time DDoS detection, the system ensures a more secure and resilient defense against evolving cyber threats.

Machine Learning Model:

Machine learning is used by the real-time DDoS detection system to dynamically monitor network traffic and identify potential threats. It continuously analyzes network packets to detect anomalies, classifying traffic as either normal or malicious. The firewall is automatically updated to block malicious IP addresses after an attack is detected, preventing further threats without user intervention. This AI-driven approach enhances security by adapting to evolving attack patterns in real time. The system employs models like XGBoost, MLP, and Random Forest to improve detection accuracy. It is particularly beneficial for financial institutions, cloud service providers, and enterprise networks, ensuring robust cybersecurity and uninterrupted service availability.

.

The machine learning model for cyber threat detection has gained popularity in recent years due to its focus on automation, accuracy, and adaptability, making it an essential tool for real-time cybersecurity applications. Other than machine learning-based detection, traditional rule-based security systems are also widely used. But there are some differences between both approaches. While traditional systems rely on predefined rules to detect attacks, machine learning models can analyze patterns and adapt to new and evolving threats. Rule-based security methods have limited flexibility, allowing for simple threat detection, whereas machine learning enables complex anomaly detection, making it more effective against sophisticated cyber threats. Additionally, machine learning models can analyze vast amounts of network traffic in real time and reduce false positives compared to rule-based systems

Real Time Threat Detection:

Real-time threat mitigation is a crucial process in the AI-driven DDoS detection system that ensures continuous protection against cyber threats. In this system, threat mitigation refers to the automated response mechanism that identifies, classifies, and neutralizes malicious traffic. When a potential attack is detected, the system instantly analyzes the severity of the threat based on traffic patterns, packet behavior, and historical attack data. Using predefined security policies and adaptive learning, the system determines the best course of action to mitigate the attack. If an attack is confirmed, firewall rules are updated dynamically to block malicious IP addresses and restrict harmful traffic flow. The system logs contain a record of each mitigation step, making it possible for security teams to examine threat patterns and make adjustments in the future. The system continuously reassesses network activity to ensure that the mitigation measures do not disrupt legitimate users. If new attack patterns emerge, the system refines its detection algorithms to enhance its defense mechanisms. Real-time threat mitigation is essential to maintaining network stability, as it enables proactive security responses while preventing service disruptions. This approach ensures that organizations can defend against evolving cyber threats with minimal human intervention..

Supervised Vs Unsupervised Learning:

In machine learning, Supervised Learning and Unsupervised Learning are two distinct approaches used to train models for pattern recognition and decision-making. Labeled datasets are used to train models in Supervised Learning, where each input is paired with an output. The model learns by mapping inputs to correct outputs and improving its predictions over time. This process is computationally efficient and widely used in applications like fraud detection and spam filtering.On the other hand, in Unsupervised Learning, models are provided with unlabeled data and must identify patterns, relationships, or clusters without explicit guidance. This means that the learning process is more exploratory and requires complex algorithms like clustering and anomaly detection. In addition to being effective in discovering hidden patterns, Unsupervised Learning is particularly useful in cybersecurity, as it can detect new attack strategies without prior knowledge.

Supervised Learning is often preferred when labeled data is available, as it ensures higher accuracy. However, it may not be suitable for detecting unknown threats, whereas Unsupervised Learning can identify anomalies in real-time. Overall, while both approaches have their strengths and weaknesses, combining Supervised and Unsupervised Learning creates a more adaptive and efficient machine learning model for cybersecurity.

Why Real Time DDos Detection:

Real-time DDoS detection systems offer significant benefits over traditional security methods. They provide instant threat identification, allowing organizations to mitigate attacks before services are disrupted. Instead of relying on manual intervention, these systems continuously monitor network traffic for proactive defense.

By distinguishing between legitimate users and malicious bots, machine learning models improve accuracy and reduce false positives. These systems can grow with the amount of traffic on the network and new ways to attack. M, according to R. Masthan and Ravi, traditional security struggles against sophisticated DDoS attacks [6]. Overall, real-time DDoS detection ensures reliable cybersecurity and uninterrupted services.

.

Automated Threat Detection:

Real-time DDoS detection systems offer significant benefits over traditional security methods. They provide instant threat identification, allowing organizations to mitigate attacks before services are disrupted. Instead of relying on manual intervention, these systems continuously monitor network traffic for proactive defense.

By distinguishing between legitimate users and malicious bots, machine learning models improve accuracy and reduce false positives. These systems can grow with the amount of traffic on the network and new ways to attack. M, according to R. Masthan and Ravi, traditional security struggles against sophisticated DDoS attacks [6]. Overall, real-time DDoS detection ensures reliable cybersecurity and uninterrupted services.

Methodology:

The system captures live network traffic and analyzes patterns using machine learning models like XGBoost, MLP, and Random Forest. Automatic firewall updates to prevent malicious IPs are initiated when threats are detected. Accuracy is enhanced by decentralized monitoring, which ensures synchronized security across nodes.

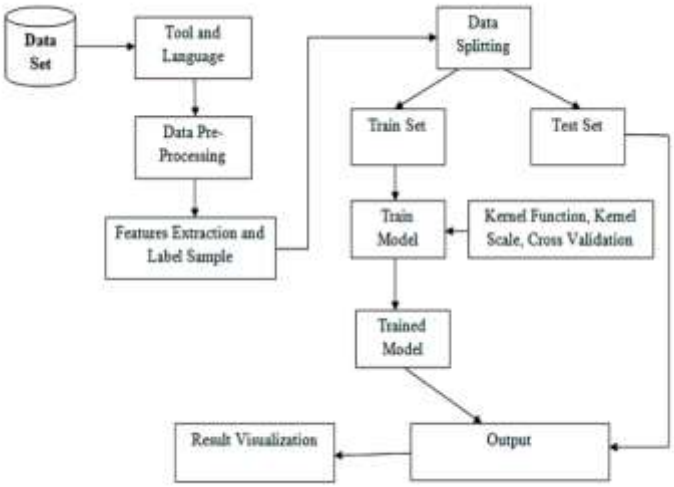
The real-time DDoS detection system's installation is an essential step toward securing the network. This system integrates machine learning models such as XGBoost, Multi-Layer Perceptron (MLP), and Random Forest to analyze live network traffic and detect malicious activities in real-time. The primary objective of the deployment is to monitor incoming IP address logs, classify network requests, and mitigate potential DDoS attacks efficiently.

The process begins with the training of machine learning models using a dataset containing both normal and attack traffic patterns. These models learn to differentiate between legitimate and malicious requests based on multiple network parameters. The models are put on a live server after they have been trained, where they process network traffic in real time for anomaly detection. To capture live traffic, the system utilizes packet sniffing tools that collect and log network activity. The pre-processed network packets are then fed into the trained models, which classify the traffic as either safe or suspicious. The system immediately updates firewall rules to block the identified IP addresses whenever it detects a potential attack. This automated mitigation prevents the escalation of DDoS attacks and ensures continuous protection.

Furthermore, the system is designed to be adaptive, allowing for continuous learning and updates based on emerging attack patterns. The real-time nature of this deployment enhances the overall resilience and scalability of cybersecurity defenses, making it an effective solution for organizations handling large volumes of online traffic.

To improve user accessibility, a Django-based web dashboardis integrated, providing a real-time visual representation of detected threats. This dashboard allows security analysts to monitor live traffic, view blocked IPs, analyze attack trends, and manually override decisions if necessary. By combining machine learning models with an interactive dashboard, the system enhances both automation and human intervention in cybersecurity operations.

Architecture Diagram:



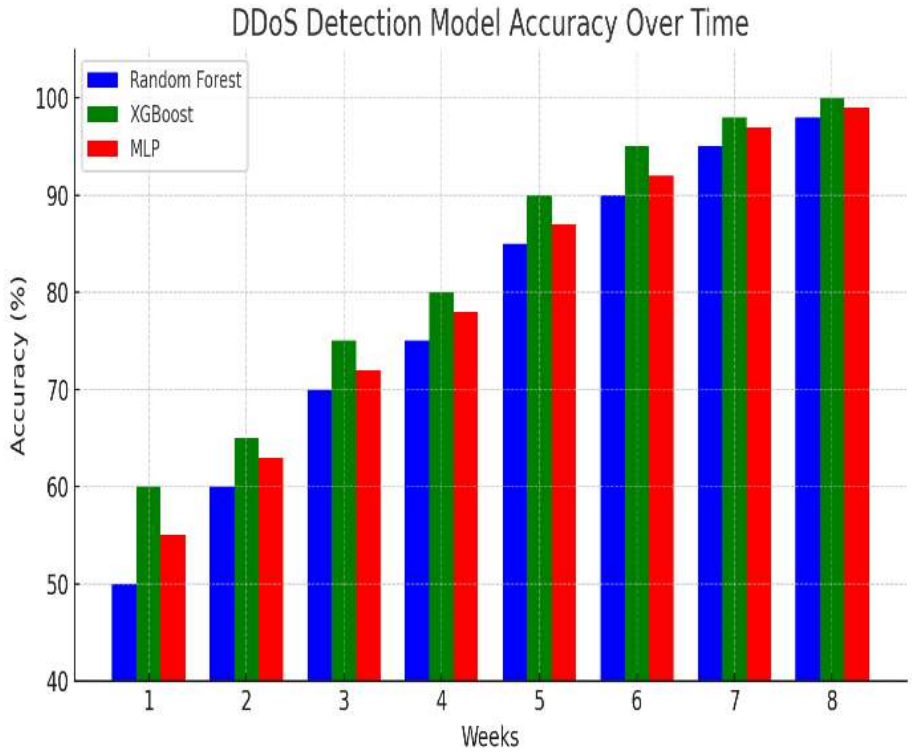
This figure describes the overall process of the platform.

Results:

This above Picture shows the suer interface after login

This Above picture shows the Ouput after choosing and uploading files to detect attacks and block Ips.

Graph:



Conclusion:

The real-time DDoS detection system has been successfully deployed. By leveraging XGBoost, MLP, and Random Forest, the system effectively analyzes network traffic and detects threats.

With live packet monitoring and a Django-based efficiently, ensuring network security.The deployment of the real-time DDoS detection system using XGBoost, MLP, and Random Forest has enabled effective live threat monitoring. By integrating the system with a Django-based web application, network traffic is continuously analyzed to detect and mitigate malicious attacks.This project has provided valuable insights into cybersecurity and machine learning, showcasing the potential of AI-driven security solutions. Overall, this system enhances network protection and ensures proactive defense against cyber threats, contributing to a safer digitalenvironment.

References:

[1] J. Hou, P. Fu, Z. Cao and A. Xu, "Machine Learning Based DDos Detection Through NetFlow Analysis Conference (MILCOM), Los Angeles, CA,
2018, pp. 1-6.
[2] S. Das, A. M. Mahfouz, D. Venugopal and S. Shiva, "DDoS IntrusionDetection Through Machine Learning Ensemble," 2019 IEEE 19thInternational Conference on Software Quality, Reliability and Security Companion (QRS-C), Sofia, Bulgaria, 2019, pp. 471-477.
[3] U. Dincalp, M. S. Güzel, O. Sevine, E. Bostanci and I. Askerzade, "Anomaly Based Distributed Denial of Service Attack Detection and Prevention with Machine Learning," 2018 2nd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, 2018, pp. 1-4.
[4] R. Doshi, N. Apthorpe and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, 2018, pp. 29-35.
[5] Z. He, T. Zhang and R. B. Lee, "Machine Learning Based DDoS Attack Detection from Source Side in Cloud," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, 2017, pp. 114-120.
[6] B. Zhang, T. Zhang and Z. Yu, "DDoS detection and prevention based on artificial intelligence techniques," 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, 2017, pp. 1276-1280
[7] B. Zhou, J. Li, J. Wu, S. Guo, Y. Gu and Z. Li, "Machine-LearningBased Online Distributed Denial-of-Service Attack Detection Using Spark Streaming," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, 2018, pp. 1-6.
[8] O. Rahman, M. A. G. Quraishi and C. Lung, "DDoS Attacks Detection and Mitigation in SDN Using Machine Learning," 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 2019, pp. 184-189.
[9] K. Verma and A. K. Ghosh (eds.), Computational Intelligence:Theories,Applications and Future Directions—Volume I, Advances in Intelligent Systems and Computing 798 © Springer Nature Singapore Pte Ltd. 2019
[10] P. Khuphiran, P. Leelaprute, P. Uthayopas, K.Ichikawa and W. Watanakeesuntorn, "Performance Comparison of Machine Learning Models for DDoS Attacks Detection," 2018 22nd International Computer Science and Engineering Conference (ICSEC), Chiang Mai, Thailand, 2018, pp. 1-4