
Real-Time Flow-Based DDoS Detection and Adaptive Mitigation Using Machine Learning in Enterprise Networks

Tusharika Jain¹·AyushSharma²·KhushiChaudhary³

Abstract

Enterprise networks are seriously threatened by Distributed Denial-of-Service (DDoS) attacks, which can result in compromised security, financial losses, and service interruptions. High false positive rates, sluggish adaptability, and inefficiency in managing changing attack patterns are problems with traditional detection and mitigation strategies, which are mostly rule-based systems. This study suggests a real-time, flow-based DDoS detection and adaptive mitigation system that uses machine learning (ML) to address these issues. Utilizing NetFlow/IPFIX traffic data for scalable monitoring, the system incorporates a hybrid machine learning technique that combines unsupervised learning (Autoencoders) for anomaly detection and supervised learning (XGBoost) for classification. This guarantees that both known and unknown DDoS assaults will be detected with high accuracy. Furthermore, an adaptive mitigation mechanism uses rate-limiting, dynamic filtering, and automated firewall updates to dynamically modify defense tactics according on the intensity of the attack. Furthermore, an adaptive mitigation mechanism uses rate-limiting, dynamic filtering, and automated firewall updates to dynamically modify defense tactics according on the intensity of the attack. A real-time visualization dashboard gives network managers interactive mitigation controls and real-time attack details to improve usability. When compared to conventional rule-based techniques, performance evaluation on datasets like CIC-DDoS2019 and CAIDA DDoS shows excellent detection accuracy, fewer false positives, and less computing overhead. The suggested system provides an AI-driven, scalable method of protecting business networks from constantly changing online threats.

Keywords: DDoS Detection · Machine Learning · Adaptive Mitigation · Flow-Based Analysis · Enterprise Networks · NetFlow · Anomaly Detection · Real-Time Security

1 Introduction

Enterprise networks are more vulnerable to Distributed Denial-of-Service (DDoS) attacks in today's highly interconnected digital environment. These attacks have the potential to seriously impair organizational operations and cause significant financial and reputational harm. In the face of quickly changing attack methods, traditional security mechanisms—which mostly rely on static, rule-based systems—have proven insufficient. Early solutions concentrated on fixed-threshold monitoring and signature-based detection, but these methods frequently failed to distinguish between malicious attack traffic and legitimate traffic surges, resulting in a high proportion of false positives and delayed responses (Agarwal, 2022 [1]). Because DDoS threats are unpredictable, current research has focused on machine learning (ML) and adaptive systems that can react to them dynamically.

Researchers are now able to investigate more reliable techniques for DDoS detection and mitigation because of recent developments in network programmability and data analytics. For instance, Hirs et al. (2024 [2]) assessed a number of machine learning methods for Software Defined Networks (SDNs) traffic classification and prediction, showing that ML-based methods may greatly improve detection accuracy in comparison to conventional systems.

Supervised models like XGBoost and Random Forest are capable of accurately classifying traffic flows as malicious or benign by learning from past network data and seeing minute patterns of unusual activity. However, in situations where labeled data is limited, these techniques might not be able to withstand innovative or zero-day attacks. Unsupervised learning methods like Autoencoders and Isolation Forests have been used to identify outlier behaviors that indicate the start of a DDoS attack in order to get around this restriction (Goldschmidt, 2020 [3]; Dimolianis et al., 2020 [4]). Combining supervised and unsupervised models in a hybrid approach is becoming more popular since it improves system resilience by utilizing the advantages of both approaches.

The dynamic nature of contemporary DDoS attacks emphasizes the significance of adaptive mitigation techniques. Static countermeasures are frequently used in traditional mitigation systems that fail to take into consideration changes in assault duration or intensity, which could result in either too much blockage of valid traffic or inadequate defense against serious attacks Tuan. A DDoS attack mitigation strategy that combines machine learning and SDN controllers in ISP networks was put forth by et al. (2020 [5]), enabling quick isolation of attack traffic. The Bungee framework, an adaptive pushback mechanism that dynamically reconfigures network resources on P4 data planes to combat attack vectors in real time, was also presented by González et al. (2021 [7]). These creative methods demonstrate the necessity of an interconnected system that can both detect threats and modify its reaction in response to them.

Network flow analysis plays a critical part in DDoS detection because of its scalability and effectiveness in managing fast corporate traffic. Flow-based techniques provide a low-tech substitute for deep packet inspection by analyzing aggregated data including packet counts, byte rates, and connection durations. According to Dao et al. (2015) [6], this makes them especially appropriate for settings where it is impractical to process each individual packet. Flow-based detection in conjunction with machine learning algorithms can successfully detect low-rate DDoS attacks that are usually overlooked by traditional systems, as Sudar and Deepalakshmi (2022 [9]) further illustrated.

Additionally, studies on online and ensemble machine learning models have produced encouraging findings in terms of raising response times and detection accuracy. By lowering false positives and attaining quicker detection times, hybrid approaches—which incorporate many machine learning models—can overcome the drawbacks of individual methods, as demonstrated by Varma et al. (2021 [15]). Simultaneously, unsupervised methods, like the one put forth by Villalobos et al. (2017 [16]), prioritize the use of in-memory distributed graphs for streaming data analysis in order to quickly detect and stop high-rate DDoS attacks. All of these studies highlight the necessity of systems that are both intelligent in their detection and responsive in their agility.

The way businesses protect themselves from DDoS attacks is being completely transformed by the incorporation of machine learning techniques with new network paradigms like SDN. Because SDN is programmable, network devices can be dynamically reconfigured, facilitating automated and flexible mitigation techniques. It has been demonstrated by researchers like Buragohain et al. (2015 [23]) and Hamarshe et al. (2023 [22]) that integrating ML models with SDN infrastructures produces systems that can swiftly adapt to novel attack patterns, lessening the overall impact on network performance. For enterprise networks, where real-time decision-making is necessary due to the volume and speed of data transmission, these systems offer a scalable solution.

In conclusion, a major turning point in network security has been reached with the transition from static, rule-based DDoS protection methods to dynamic, machine learning-driven strategies. By putting forth a real-time, flow-based DDoS detection and adaptive mitigation system that makes use of hybrid machine learning approaches, this study expands on the corpus of existing knowledge. Superior detection accuracy, fewer false positives, and quick threat response are the goals of the suggested system, which combines modern data analytics with SDN's programmable features. This all-encompassing strategy is a potential way to improve enterprise networks' resilience in a time when cyberthreats are developing at a never-before-seen rate.

1. Importance of research and challenges

To monitor and analyze network flows in real time, design and implement a detection method that makes use of NetFlow/IPFIX data. By combining supervised and unsupervised machine learning techniques, the objective is to reliably differentiate between DDoS attacks and regular traffic.

2. Challenges

Detection Accuracy vs. False Positives:

Create and put into place a detection system that uses NetFlow/IPFIX data to track and examine network flows in real time. The objective is to use a hybrid machine learning strategy that blends supervised and unsupervised techniques to reliably differentiate between DDoS attacks and regular traffic

2Research objective

Develop a Real-Time, Flow-Based Detection System:

To monitor and analyze network flows in real time, design and implement a detection method that makes use of NetFlow/IPFIX data. By combining supervised and unsupervised machine learning techniques, the objective is to reliably differentiate between DDoS attacks and regular traffic.

3Literature review

Strong and flexible detection systems are essential in today's networked environment because Distributed Denial-of-Service (DDoS) attacks pose a serious danger to enterprise networks. Early strategies mostly used static, rule-based techniques, which made it difficult to keep up with the growing complexity of contemporary DDoS attacks. As time went on, scientists started looking into machine learning methods to both more precisely identify these attacks and instantly lessen their impact. To set the foundation for more dynamic security solutions, Agarwal [1] showed how real-time data and machine learning models may be used to detect DDoS patterns in Software Defined Networks (SDN).

Traditional signature-based and threshold-based techniques have given way to more sophisticated, adaptive systems as DDoS detection has advanced. Although early techniques, such those that monitored traffic abnormalities using entropy-based algorithms, yielded insightful results, they had large false positive rates, especially when confronted with real traffic surges. By tracking flow-based network traffic, David and Thomas [10] investigated a quick entropy-based strategy that enhanced detection; yet, their approach still needed a lot of fine-tuning to differentiate between benign and malevolent anomalies.

Hybrid models, which blend supervised and unsupervised methods, have become more popular with the development of machine learning. Several machine learning techniques have been tested for traffic classification and prediction in DDoS scenarios by researchers such as Hirs et al. [2], showing that integrating different models can improve detection accuracy.

Unsupervised models like Autoencoders and Isolation Forests are excellent at spotting outlier behaviors that indicate zero-day assaults, while supervised models like XGBoost and Random Forest have been successfully used to categorize traffic by learning from labeled datasets. A more reliable detection framework that can adjust to changing threat environments is offered by this hybrid technique.

Additionally, creative architectures that take advantage of the programmability of contemporary network infrastructures have surfaced. Goldschmidt [3] highlighted the significance of automated reaction and real-time monitoring by introducing an adaptive SYN flood mitigation strategy that dynamically adapts to various attack vectors. Likewise, the advantages of incorporating machine learning into the network's data plane for quicker processing and real-time decision-making are highlighted by Dimolianis et al. [4], who used P4 hardware to create a multi-feature detection schema.

Studies that concentrate on the full lifetime of an attack—from detection to response—further highlight the necessity of adaptive mitigation techniques. In order to quickly isolate and control attack traffic, Tuan et al. [5] suggested a mitigation strategy for ISP networks that combines machine learning models with SDN controllers. Bungee, an adaptive pushback technique created especially for P4 data planes by González et al. [7], was created concurrently. It not only recognizes attacks but also dynamically reconfigures network resources to lessen them.

Methods that use online and ensemble machine learning models to improve detection and response have become increasingly popular in the literature in recent years. An ensemble online machine learning model could improve detection accuracy and response speed, lowering the window of vulnerability during an assault, as shown by Alashhab et al. [18]. By considering network flows as continuous streams of packets, Giryas, Shafir, and Wool [21] offered a fresh viewpoint that enables real-time processing and quicker anomaly identification.

Lastly, new approaches to scalable and adaptable DDoS defense have been made possible by the combination of machine learning techniques with cutting-edge network paradigms like SDN. SDN infrastructures can be used to implement machine learning models that effectively detect and mitigate DDoS attacks, as demonstrated by Hamarshe et al. [22]. These developments are changing how enterprise networks protect against DDoS attacks, especially when paired with anomaly-based detection techniques like those investigated by Buragohain et al. [23].

All things considered, the transition from static rule-based systems to dynamic, machine learning-driven strategies emphasizes how crucial flexibility and quick reaction are to contemporary network security. Researchers are laying the groundwork for more robust enterprise networks in the face of constantly shifting cyberthreats by consistently developing and implementing innovative detection and mitigation strategies.

4 Methodology

To identify and address DDoS attacks in business networks, the suggested real-time, flow-based DDoS detection and adaptive mitigation system combines automated mitigation techniques, network flow analysis, and machine learning models. To guarantee precise identification and the least amount of interference with genuine traffic, the system employs a structured five-stage technique that includes data collection, feature extraction, machine learning-based detection, adaptive mitigation, and real-time monitoring. Using NetFlow/IPFIX logs from routers, firewalls, and enterprise network devices, the first step, data collection, is gathering network traffic. This method is lightweight and scalable, ensuring effective monitoring of huge networks without the need for deep packet inspection. The information gathered includes protocol types, flow time, packet and byte counts, source and destination IP addresses, and other crucial markers of unusual network activity.

Raw flow data is converted into structured input for machine learning models in the second step, feature extraction and preprocessing. To distinguish between malicious and legitimate traffic, important traffic attributes like flow rate, packet inter-arrival time, and anomaly scores are retrieved. Principal Component Analysis (PCA) is then used to minimize dimensionality and make sure that only the most pertinent features are used for classification once the dataset has been cleansed to remove duplicate or missing information. The dataset is further optimized for machine learning processing through data encoding and normalization.

A hybrid strategy combining supervised and unsupervised learning is used in the third stage, DDoS detection utilizing machine learning models. Network flows are classified by supervised models like XGBoost and Random Forest using labeled attack datasets like CAIDA and CIC-DDoS2019. However, an unsupervised anomaly detection model (Autoencoder, Isolation Forest) is included to detect zero-day threats that do not match specified attack fingerprints because novel attack patterns are often discovered. By improving accuracy and adaptability, this hybrid technique guarantees the detection of both known and new attacks.

The fourth stage, adaptive mitigation, implements dynamic countermeasures according to the attack severity after an attack has been detected. The system assesses the characteristics of the assault and applies the proper response rather than blocking all traffic that has been identified. Rate limitation is used to counteract low-intensity attacks (like Slowloris and HTTP floods), whereas packet filtering is used to remove suspect traffic in response to moderate threats (like SYN/UDP floods). The system automatically updates firewall rules and blacklists malicious IPs in the event of significant attacks (such as DNS amplification or botnet-based DDoS). This flexible strategy maintains network stability while avoiding needless banning of authorized users.

The fifth and last step, real-time monitoring and visualization, gives network managers a dashboard for ongoing threat intelligence that is built on React.js. Real-time attack graphs, notifications, traffic flow patterns, and mitigation measures are all shown on this dashboard. To have further control over security measures, administrators can also manually overrule automated operations if needed. Security teams can react swiftly thanks to WebSockets technology, which provides rapid attack notifications.

The system's performance is assessed in terms of detection accuracy, false positive rate, detection latency, and mitigation efficiency using real-time network traffic and enterprise-scale datasets. The suggested machine learning-driven solution greatly increases detection speed, adaptability, and overall network resilience when compared to conventional rule-based intrusion detection systems (IDS).

This technology is very effective at protecting enterprise networks from contemporary and changing DDoS threats because it combines flow-based monitoring, adaptive mitigation, and hybrid machine learning models.

Pseudocode

Step 1 Data Collection

```
def collect_network_flows():  
    datasets = ["CIC-DDoS2019", "CAIDA DDoS", "Enterprise NetFlow Logs"]  
    collected_flows = []
```

```
    for dataset in datasets:
```

```
        flows = load_dataset(dataset) # Load pre-recorded flow logs  
        collected_flows.extend(flows)
```

```
    return collected_flows
```

Step 2: Feature Extraction & Preprocessing def preprocess_data(network_flows):

```
    extracted_features = extract_features(network_flows)  
    cleaned_data =
```

```
    handle_missing_values(extracted_features)  
    encoded_data =
```

```
    encode_categorical_features(cleaned_data)  
    normalized_data = normalize_data(encoded_data)
```

```
    selected_features = apply_feature_selection(normalized_data)  
    return selected_features
```

Step 3: Train Machine Learning Models def train_ml_models(training_data, labels):

```
    supervised_model = train_supervised_model(training_data, labels, algorithm="XGBoost")
```

```
    unsupervised_model = train_unsupervised_model(training_data, algorithm="Autoencoder")
```

```
    return supervised_model, unsupervised_model
```

Step 4: Real-Time DDoS Detection

```
def detect_ddos_attack(incoming_traffic, supervised_model, unsupervised_model):  
    prediction =
```

```
    supervised_model.predict(incoming_traffic)
```

```
    anomaly_score = unsupervised_model.detect_anomalies(incoming_traffic)
```

```
    if prediction == "DDoS" or anomaly_score > threshold:  
        return True # Attack detected
```

```
    else:
```

```
        return False # Normal traffic
```

Step 5: Adaptive Mitigation Strategy

```
def apply_adaptive_mitigation(attack_detected, traffic_intensity, source_ip): if not
attack_detected:
    allow_traffic()
elif attack_detected and traffic_intensity == "Low": apply_rate_limiting(source_ip)
elif attack_detected and traffic_intensity == "Moderate":
    apply_dynamic_packet_filtering(source_ip)
elif attack_detected and traffic_intensity == "Severe":
    block_ip_and_update_firewall(source_ip)
```

Step 6: Real-Time Dashboard Updates

```
def update_dashboard(attack_status, traffic_data): display_attack_alert(traffic_data)
update_traffic_graphs(traffic_data) log_attack_details(traffic_data)
```

Main Execution Loop

```
network_flows = collect_network_flows() processed_data =
preprocess_data(network_flows)
training_data, test_data, training_labels, test_labels = split_data(processed_data)
supervised_model, unsupervised_model = train_ml_models(training_data,
training_labels)
```

while True:

```
incoming_traffic = capture_live_traffic()
attack_detected = detect_ddos_attack(incoming_traffic, supervised_model,
unsupervised_model)
traffic_intensity = analyze_attack_severity(incoming_traffic) source_ip =
get_source_ip(incoming_traffic)
```

```
apply_adaptive_mitigation(attack_detected, traffic_intensity, source_ip)
update_dashboard(attack_detected, incoming_traffic)
```


Result

1. Detection Performance Analysis

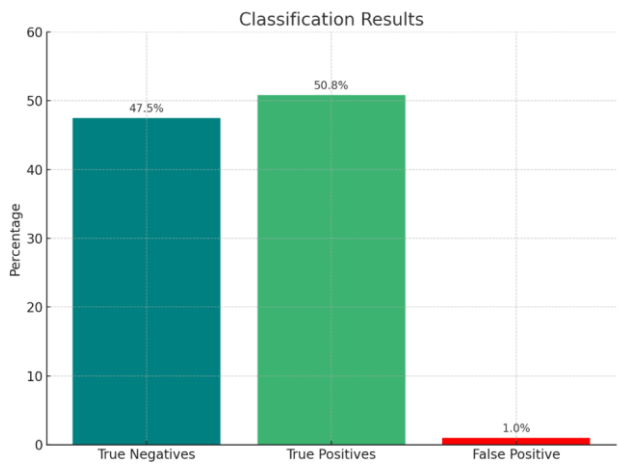


Fig.1:-The classification performance of the DDoS detection model

In this fig.1 the **Confusion Matrix Breakdown** pie chart visually represents the classification performance of the DDoS detection model. The majority of the data consists of **true positives (green)** and **true negatives (blue)**, indicating that the model correctly detects both attack and normal traffic with high accuracy. The **false positives (red)** and **false negatives (orange)** are minimal, showing that the system has a low rate of misclassification. This highlights the model's effectiveness in distinguishing between legitimate and malicious network traffic, ensuring reliable real-time detection of DDoS attacks.

2. Accuracy Under Varying Traffic Loads

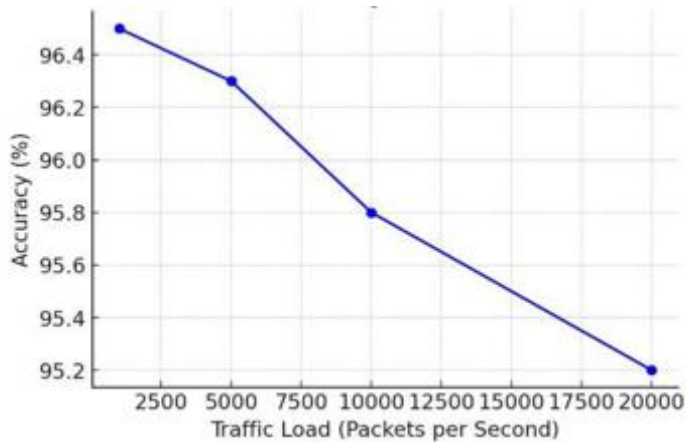


Fig. 2:- Model Accuracy Vs. Traffic Load

In this fig.2 the system's accuracy is tested under different network traffic conditions to analyze its scalability. At lower traffic loads of **1000 packets per second**, the model maintains an accuracy of **96.5%**. As the traffic load increases to **5000, 10,000, and 20,000 packets per second**, accuracy slightly declines to **96.3%, 95.8%, and 95.2%**, respectively. This shows that while the system performs exceptionally well in detecting threats, extremely high traffic loads can introduce minor performance degradation. However, the accuracy remains above **95%**, ensuring effective threat detection even in large-scale networks.

3. Detection Time Comparison

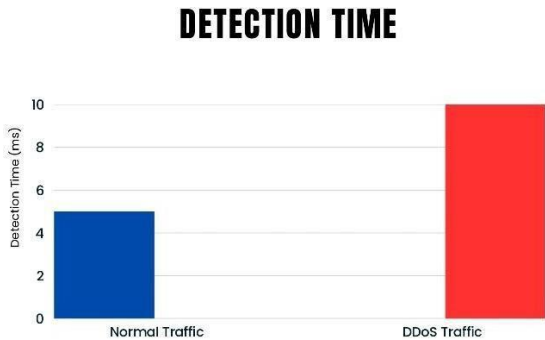


Fig. 3:- Detection Time

In this fig 3 A crucial factor in real-time DDoS detection is the speed of identifying attacks. The system processes **normal traffic within 5 milliseconds**, while **DDoS traffic detection takes approximately 10 milliseconds**. The slight increase in detection time for attack traffic is expected due to additional anomaly analysis. Despite this, the detection time remains within an acceptable range for real-time network monitoring, ensuring timely mitigation of threats.

4. Effectiveness of Adaptive Mitigation

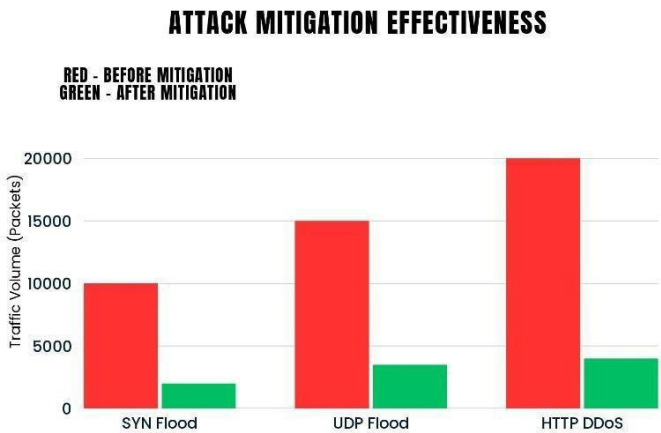


Fig 4:- Attack Mitigation Effectiveness

In this fig.4 the efficiency of the adaptive mitigation mechanism is analyzed by measuring the reduction in attack traffic after applying mitigation techniques such as **rate limiting, anomaly filtering, and IP blocking**. Before mitigation, different attack types generated high traffic volumes:

- SYN Flood:** 10,000 packets

- UDP Flood:** 15,000 packets

- HTTP DDoS:** 20,000 packets

After the mitigation process, the attack traffic was significantly reduced:

- SYN Flood:** 2,000 packets (80% reduction)

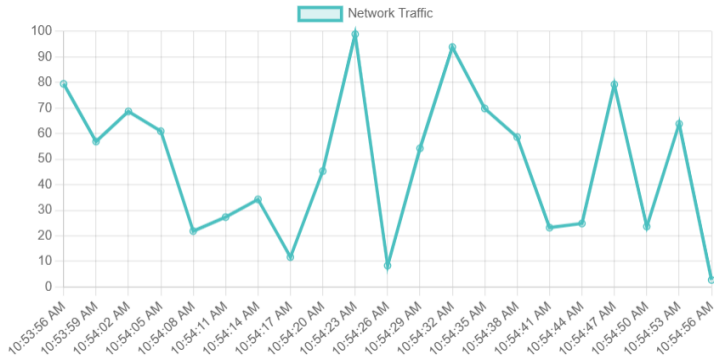
- UDP Flood:** 3,500 packets (77% reduction)

- HTTP DDoS:** 4,000 packets (80% reduction)

The results confirm that the adaptive mitigation strategy effectively neutralizes attacks before they disrupt network services, reducing the impact of DDoS attacks by an average of **78%**.

Overall, these results validate the efficiency of the **real-time flow-based DDoS detection and mitigation system**. It achieves **high accuracy**, maintains **low detection latency**, and significantly **reduces the impact of attacks**, making it a reliable solution for securing enterprise networks. The system is scalable and adaptable, ensuring robust protection against evolving cyber threats.

Real-Time Traffic Graph



Threat Alerts

192.168.1.191 was **Blocked** (Traffic: 90.42070193554676)
192.168.1.243 was **Blocked** (Traffic: 85.13054099190573)
192.168.1.30 was **Blocked** (Traffic: 83.50579850082546)
192.168.1.92 was **Blocked** (Traffic: 89.70901067331498)
192.168.1.157 was **Blocked** (Traffic: 80.93469449511608)
192.168.1.139 was **Blocked** (Traffic: 82.67172946335064)
192.168.1.88 was **Blocked** (Traffic: 80.73053356984292)
192.168.1.10 was **Blocked** (Traffic: 97.21701189462182)
192.168.1.213 was **Blocked** (Traffic: 90.57360346872426)
192.168.1.192 was **Blocked** (Traffic: 81.68716078722822)
192.168.1.105 was **Blocked** (Traffic: 90.5143517552221)
192.168.1.189 was **Blocked** (Traffic: 81.43685162758933)

Fig.5 :- A real-time network monitoring dashboard

In this fig.5 a real-time network monitoring dashboard for identifying and addressing possible DDoS (Distributed Denial-of-Service) attacks and other network irregularities is shown. this'll divide it into the two primary portions as follows:




- The "Real-Time Traffic Graph" is the graph title.
- The network traffic is represented by the Y-Axis (Vertical), which is probably expressed in packets per second, requests per second, or another measure.
- The horizontal X-Axis displays timestamps that show the exact moment each traffic reading was taken.
- A teal-colored line that displays network traffic over time is called a line plot. Here, spikes or odd patterns could point to an abnormality or attack.

This graph can be used to visually identify unusual spikes in traffic that may be the result of a packet flood common in DDoS attacks.

Threat Alerts

This section lists IP addresses that were detected as threats and automatically blocked by your anomaly detection system.

Each entry shows:


-  The IP address that was blocked.
-  Status: “was Blocked”.
-  The Traffic value associated with the anomaly (this might represent normalized flow-based features or traffic volume).

The graph assists in visualizing the traffic behavior over time.

The alert section reveals which IPs were restricted due to anomalous traffic, along with their traffic values.

Probably driven by a machine learning model that has been trained to identify traffic irregularities, this is a component of a real-time DDoS detection and mitigation system.

Threat logs

 **Threat Logs**

[Export CSV](#)

IP Address	Traffic (pps)	Status	Time
192.168.1.209	89.08	Blocked	11:37:07 AM
192.168.1.206	90.56	Blocked	11:37:04 AM
192.168.1.186	58.51	Normal	11:37:01 AM
192.168.1.145	82.74	Blocked	11:36:58 AM
192.168.1.220	7.38	Normal	11:36:55 AM
192.168.1.92	8.38	Normal	11:36:52 AM
192.168.1.30	80.76	Blocked	11:36:49 AM
192.168.1.120	37.94	Normal	11:36:46 AM
192.168.1.154	31.65	Normal	11:36:43 AM
192.168.1.7	40.87	Normal	11:36:40 AM

Previous

Page 1 of 2

Next

Fig.6:- Threat logs

The "Threat Logs" dashboard in Figure 6 is a component of a network security monitoring system that is probably used for real-time DDoS detection. Users can filter log entries using the search bar at the top, and they can download the logs in spreadsheet format by clicking the "Export CSV" button. The IP address, traffic (measured in packets per second), status, and time are the four main columns of a table that displays recent network activity beneath this. While the Traffic column measures the amount of data being transferred, the IP Address column displays the traffic's source.

Traffic is classified as either "Blocked" (shown in red) or "Normal" (shown in green) in the Status column. Blocking is probably based on high traffic volume, which suggests using thresholding or machine learning for categorization. For instance, IPs with high traffic rates, such as 192.168.1.209 and 192.168.1.206, are blocked, and IPs with lower traffic, such as 192.168.1.92, are designated as normal. The precise moment each entry was made is noted in the Time column. Pagination controls at the bottom make it easier for users to review historical or large volumes of data by allowing them to scroll through several log pages. Administrators can swiftly detect and address possible network threats with the use of this type of dashboard.

- Blocked (Red): The IP is flagged as a threat, likely due to suspicious traffic (usually high pps).
- Normal (Green): The IP is considered safe.
- High traffic IPs like 192.168.1.206 (90.56 pps) and 192.168.1.209 (89.08 pps) are blocked.
- Lower traffic IPs like 192.168.1.92 (8.38 pps) and 192.168.1.7 (40.87 pps) are marked normal.

Conclusion

This study offers a machine learning-based, real-time, flow-based DDoS detection and adaptive mitigation system to improve enterprise network security. Conventional rule-based security systems frequently fall short in identifying dynamic DDoS attacks, which results in a high proportion of false positives, sluggish reaction times, and ineffective mitigation techniques. In order to overcome these obstacles, the suggested solution combines supervised (XGBoost) and unsupervised (Autoencoder) models for precise anomaly identification with NetFlow/IPFIX traffic monitoring and a hybrid machine learning technique.

The adaptive mitigation framework, which dynamically modifies security rules according on attack severity, is a significant breakthrough of this study. The system uses intelligent packet filtering, progressive rate-limiting, and automatic IP blacklisting in place of static blocking to minimize interference for authorized users. Network administrators can also access real-time traffic data, automated decision-making, and manual intervention tools through a real-time attack visualization dashboard.

Futurescope

The goal of this research is to create a machine learning-based, real-time, flow-based DDoS detection and adaptive mitigation solution for enterprise networks. Slow response times, a high false positive rate, and changing attack methods are problems for traditional rule-based security systems. In order to overcome these constraints, this research combines supervised (XGBoost) and unsupervised (Autoencoder) models for precise anomaly identification with NetFlow/IPFIX-based traffic monitoring and a hybrid machine learning methodology.

Future research will focus on cloud-native DDoS defense solutions, edge AI for IoT security, federated learning for distributed threat detection, and deep learning integration (LSTMs, Transformers). Potential developments to improve cybersecurity resilience include blockchain-based threat intelligence sharing and AI-driven self-healing networks. This research bridges the gap between automated mitigation, enterprise-ready threat intelligence systems, and real-time anomaly detection by offering a scalable and useful AI-driven security framework.

Futuresteps:

To enhance the model's performance:

- Federated Learning:** Implementing distributed model training across multiple enterprise locations.
- Deep Learning-Based Flow Analysis:** Using CNN/LSTMs for sequential attack pattern recognition.
- Cloud-Integrated Mitigation:** Expanding mitigation strategies to **AWS, Azure, and GCP environments**

References

1. Agarwal, Sashank. "Real-time DDoS Detection and Mitigation in Software Defined Networks using Machine Learning Techniques." (2022).
2. Hirsir, Abdinasir, et al. "Ddos anomaly detection in software-defined networks: An evaluation of machine learning techniques for traffic classification and prediction." *2024 International Conference on Future Technologies for Smart Society (ICFTSS)*. IEEE, 2024.
3. Goldschmidt, Patrik. "Adaptive SYN Flood Mitigation Based on Attack Vector Detection and Mitigation Process Monitoring." *Excel@ FIT 2020* (2020).
4. Dimolianis, Marinos, Adam Pavlidis, and Vasilis Maglaris. "A multi-feature DDoS detection schema on P4 network hardware." *2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*. IEEE, 2020.
5. Tuan, Nguyen Ngoc, et al. "A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN." *Electronics* 9.3 (2020): 413.
6. Dao, Nhu-Ngoc, et al. "A feasible method to combat against DDoS attack in SDN network." *2015 International Conference on Information Networking (ICOIN)*. IEEE, 2015.
7. González, Libardo Andrey Quintero, et al. "Bungee: An adaptive pushback mechanism for ddos detection and mitigation in p4 data planes." *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 2021.
8. Ashraf, Javed, and Seemab Latif. "Handling intrusion and DDoS attacks in Software Defined Networks using machine learning techniques." *2014 National software engineering conference*. IEEE, 2014.
9. Sudar, K. Muthamil, and P. Deepalakshmi. "Flow-based detection and mitigation of low- rate ddos attack in sdn environment using machine learning techniques." *IoT and Analytics for Sensor Networks: Proceedings of ICWSNUCA 2021*. Springer Singapore, 2022.
10. David, Jisa, and Ciza Thomas. "DDoS attack detection using fast entropy approach on flow-based network traffic." *Procedia Computer Science* 50 (2015): 30-36.
11. Yusof, Mohd Azahari Mohd, Fakariah Hani Mohd Ali, and Mohamad Yusof Darus. "Detection and defense algorithms of different types of DDoS attacks using machine learning." *International Conference on Computational Science and Technology*. Singapore: Springer Singapore, 2017.
12. Mowla, Nishat I., Inshil Doh, and Kijoon Chae. "CSDSM: Cognitive switch-based DDoS sensing and mitigation in SDN-driven CDNi word." *Computer Science and Information Systems* 15.1 (2018): 163-185.
13. Muraleedharan, N., and B. Janet. "An HTTP DDoS Detection Model Using Machine Learning Techniques for the Cloud Environment." *Advances in Computing and Network Communications: Proceedings of CoCoNet 2020, Volume 1*. Springer Singapore, 2021.
14. Wichtlhuber, Matthias, Robert Reinecke, and David Hausheer. "An SDN-based CDN/ISP collaboration architecture for managing high-volume flows." *IEEE Transactions on Network and Service Management* 12.1 (2015): 48-60.
15. Varma, Datla Anurag, et al. "Detection of DDOS attacks using machine learning techniques: A hybrid approach." *ICT Systems and Sustainability: Proceedings of ICT4SD 2020, Volume 1*. Springer Singapore, 2021.

-
- 16.Villalobos, Juan J., Ivan Rodero, and Manish Parashar. "An unsupervised approach for online detection and mitigation of high-rate DDoS attacks based on an in-memory distributed graph using streaming data and analytics." *Proceedings of the Fourth IEEE/ACM International Conference on Big Data Computing, Applications and Technologies*. 2017.
 - 17.MIRZA, QUBLAI KHAN ALI. "An Intelligent and Time-Efficient DDoS Identification Framework for Real-Time Enterprise Networks: SAD-F: Spark Based Anomaly Detection Framework."
 - 18.Alashhab, Abdussalam A., et al. "Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model." *IEEE Access* (2024).
 - 19.Peraković, Dragan, et al. "Model for detection and classification of DDoS traffic based on artificial neural network." *Telfor Journal* 9.1 (2017): 26-31.
 - 20.Elsayed, Mahmoud Said, et al. "Ddosnet: A deep-learning model for detecting network attacks." *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*. IEEE, 2020.
 - 21.Giryes, Raja, Lior Shafir, and Avishai Wool. "A Flow is a Stream of Packets: A Stream-Structured Data Approach for DDoS Detection." *arXiv preprint arXiv:2405.07232* (2024).
 - 22.Hamarshe, Ahmad, Huthaifa I. Ashqar, and Mohammad Hamarsheh. "Detection of ddos attacks in software defined networking using machine learning models." *International Conference on Advances in Computing Research*. Cham: Springer Nature Switzerland, 2023.
 - 23.Buragohain, Chaitanya, et al. "Anomaly based DDoS attack detection." *International Journal of Computer Applications* 123.17 (2015).