Detection and Mitigation of DDoS Attacks with Machine Learning

Shreya Patil, Snehal Patil, Amruta Patil, Prof.Monica Charate
Computer Science & Technology UMIT, SNDT Mumbai, India

***Abstract*—With the quick development of the Web of Things (IoT), cybersecurity dangers have progressively ended up a major concern, particularly Disseminated Dissent of Benefit (DDoS) assaults. These assaults meddled with organize operations by overpowering them with intemperate activity, driving to disturbances. systems by assaulting them with over the top pernicious activity, which can result in downtime, money related misfortunes, and operational challenges. Later ponders highlight an disturbing increment in modern DDoS assaults particularly focusing on IoT gadgets. Due to their constrained security components, these gadgets are as often as possible abused to make large-scale botnets, such as Mirai, which have been responsible for a few of the foremost troublesome cyberattacks in later a long time. Conventional security measures, counting rule-based interruption location frameworks and manual activity sifting, frequently drop brief in giving real-time reactions, clearing out systems helpless to delayed benefit interferences. To address these challenges, this paper proposes a machine learning-driven DDoS location and computerized moderation framework planned to improve organize security in IoT environments. The framework leverages a crossover irregular timberland demonstrate to examine and classify organize activity, recognizing between authentic and noxious movement with tall precision. Past fundamental assault discovery, the framework classifies DDoS assaults into particular categories—including UDP surge, TCP SYN surge, HTTP surge, and ICMP flood—each of which misuses interesting organize vulnerabilities. UDP surges overpower targets with over the top parcels, TCP SYN surges misuse the TCP handshake prepare, HTTP surges imitate genuine web demands to debilitate server assets, and ICMP surges produce tall volumes of ping demands to stuff systems.**

***Keywords*— DDoS Detection, Machine Learning, Random Forest, Firewall, Network Security, HTTP flood, ICMP flood, TCP SYN flood, UDP flood.**

I. INTRODUCTION

IoT has revolutionized different businesses, counting healthcare, shrewd homes, mechanical robotization, and transportation, by empowering consistent network and computerization. The expanding appropriation of IoT gadgets has encouraged real-time information collection, farther observing, and cleverly decision- making, essentially progressing operational proficiency and client comfort. Be that as it may, this fast extension has moreover driven to a surge in cybersecurity challenges, with Dispersed Refusal of Benefit (DDoS) assaults posturing a major danger to IoT systems. A Disseminated Dissent of Benefit (DDoS) assault may be a cyberattack in which numerous compromised gad- gets, frequently portion of a botnet, send an overpowering volume of activity to a target framework to deplete its assets, rendering it inaccessible to authentic clients [1]. IoT gadgets, frequently characterized by moo handling control, powerless security instruments, and need of legitimate overhauls, are prime targets for such assaults. Once compromised, these gadgets can be enlisted into large-scale botnets—networks of contaminated gadgets that cybercriminals utilize to dispatch high-intensity assaults against businesses, governments, and basic frameworks.

1.1 Understanding DDoS Attacks in IoT

Cybersecurity reports have highlighted a drastic rise in IoT-driven DDoS attacks, with attackers exploiting vulnerabilities such as weak authentication, hardcoded credentials, and outdated firmware [2]. One of the most infamous IoT botnets, Mirai, demonstrated the devastating impact of such attacks, when it infected thou- sands of unsecured IoT devices, launching DDoS at- tacks exceeding 1 terabit per second (Tbps), leading to severe disruptions across major online services and enterprises [3]. A recent study by Cloudflare reported that DDoS attacks have grown by over 200% in frequency and intensity, particularly in network-layer attacks, making

traditional security solutions ineffective against such sophisticated threats [4]. The financial and operational consequences of IoT-based DDoS attacks are significant, affecting not only businesses but also critical services such as healthcare, smart grids, and autonomous transportation systems. Cybercriminals now use multi-vector attack techniques, combining UDP floods, TCP SYN floods, HTTP floods, and ICMP floods to bypass traditional defense mechanisms [5].

1.2 AI-Driven Security Solutions for IoT DDoS Prevention

Conventional security arrangements, such as firewalls, rule-based interruption discovery frameworks (IDS), and signature-based approaches, are deficiently to counter cutting edge DDoS dangers [6]. These ordi- nary strategies depend on predefined rules and inactive marks, making them ineffectual against zero-day as- saults and versatile assault techniques utilized by cyber-criminals. Besides, manual intercession in conventional moderation forms frequently leads to deferred reactions, permitting aggressors to cause noteworthy harm some time recently countermeasures are connected. Given these challenges, analysts have begun "centering on AI-driven security instruments that combine machine learning (ML) and real-time anticipation procedures to upgrade the versatility of IoT systems" [7].

1.3 Key Contributions of This Research

- Development of an automated ML-based model for real-time DDoS attack detection, capable of distinguishing between various DDoS attack types (UDP flood, TCP SYN flood, HTTP flood, ICMP flood).
- Implementation of an automated mitigation mechanism, integrating Windows Firewall activation to dynamically block malicious traffic as soon as an attack is detected.
- Comprehensive analysis of multi-vector DDoS attack techniques and how ML-based detection improves accuracy compared to traditional rule-based security mechanisms.
- Evaluation of the proposed system's effective- ness, demonstrating higher detection accuracy and faster mitigation response times.

Paper Title & Author	Year	Description
Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model - AHMED AHMIM [8]	2023	Hybrid deep learning model using CNN, LSTM, and autoencoders with transfer learning for IoT-based DDoS detection.
Lightweight DDoS Detection Using MobileNet in IoT Environments [9]	2023	Lightweight deep learning models for IoT-based DDoS detection.
Federated Learning for IoT Security [10]	2023	Decentralized ML training to enhance privacy in DDoS detection.
ML-Based Firewall Rule Automation [20]	2022	Real-time attack detection and firewall rule updates.
Blockchain for DDoS Prevention [22]	2023	Decentralized security framework to prevent botnet attacks.
Random Forest Classifier for DDoS Detection [13]	2022	High-accuracy classification of normal and malicious traffic.
CNN and RNN-Based Anomaly Detection [14]	2021	Deep learning approach for real-time anomaly detection.
SDN-Based DDoS Prevention [21]	2021	Dynamic network security using SDN-based policies.
Hybrid Ensemble ML Techniques [5]	2021	Enhanced detection accuracy using multiple classifiers.
Adaptive	2023	Dynamic firewall

Firewall-Based Mitigation [17]		filtering based on real-time traffic analysis.
IDS-IPS Integrated Fire-walls [18]	2021	Improved DDoS mitigation using firewall and IDS-IPS integration.

Table 1: Comparison of DDoS Detection and Mitigation Approaches

II. PROPOSED METHODOLOGY

2.1 Overview of the Model

DDoS assaults posture a basic cybersecurity danger by overpowering arrange frameworks with over the top activity, driving to benefit disturbance. To address this, we created a machine learning-based DDoS discovery and avoidance framework that precisely distinguishes and mitigates malevolent organize action in genuine time. Our model comprises two essential components: a twofold classification show to identify whether activity is ordinary or an assault and a multi-class classification show to recognize the particular sort of DDoS assault. We utilize a Irregular Timberland Classifier, which accomplishes tall exactness in recognizing between kind and noxious activity. The framework is coordinates into a Flask-based web application, empowering clients to analyze organize logs. Upon recognizing an assault, it can consequently enact firewall rules to square pernicious activity, upgrading security. Created utilizing the CIC IoT Dataset 2023, the double classification show accomplished 100 percent accuracy, whereas the multi- class show come to 99 percent accuracy, guaranteeing strong assault location. Future upgrades will center on versatile learning models, real-time gushing examination, and AI-driven risk insights to assist move forward discovery precision and reaction proficiency.

2.2 Dataset Selection

To create an proficient DDoS location and anticipation show, we totaled different freely accessible datasets from Kaggle, counting CICDDoS 2023, rather than depending on a single source. This custom dataset improves differences, speaking to a wide run of DDoS assault designs, organize varieties, and real-world pe- culiarities.By joining the most recent assault patterns, our dataset guarantees the demonstrate is prepared on advancing dangers, making strides generalization, pre- disposition lessening, and versatility to inconspicuous assault vectors. This approach essentially improves discovery precision, strength, and real-world appropriate-ness in arrange security.

2.3 Feature Selection

To improveDDoS discovery and moderation, we connected highlight determination methods to hold the foremost basic organize activity properties whereas evacuating insignificant ones. Our dataset incorporates flow-based parameters(length, rate), protocol- related highlights(TCP, UDP, ICMP banners), and measurable markers(add up to measure, standard deviation).Utilizing relationship examination, shared data, and Recursive Include Elimination (RFE), we distinguished the foremost persuasive highlights for precise assault discovery. This optimized highlight determination progresses show proficiency, real-time danger relief, and energetic firewall run the show overhauls, guaranteeing proactive security without influencing genuine arrange activity.

2.4 Model Training and Optimization

To guarantee tall precision, productivity, and versatility, our DDoS location demonstrate takes after a organized preparing and optimization handle. The dataset experiences preprocessing, counting dealing with lost values, encoding categorical highlights, and applying in- clude scaling where vital. It is at that point part into 80% preparing and 20% testing, keeping up a adjusted conveyance of kind and assault activity for successful learning. For double classification (DDoS vs. generous) and multi-class classification (particular assault sorts), we utilize a Irregular Timberland Classifier due to its vigor in dealing with expansive datasets. The demonstrate is prepared whereas persistently observing key execution measurements such as exactness, accuracy, review, and F1-score to guarantee unwavering quality. To optimize demonstrate execution, we apply Lattice Look and Irregular Seek for hyperparameter tuning, re-fining key parameters like n estimators, max features, max samples, and max leaf nodes to adjust complexity and avoid overfitting. Preparing is conducted in a high-performance

computing environment with parallel preparing, making strides proficiency and lessening execution time. Moreover, highlight significance investigation is performed to distinguish basic organize activity parameters impacting assault location, upgrading the model's interpretability and real-world appropriate- ness.

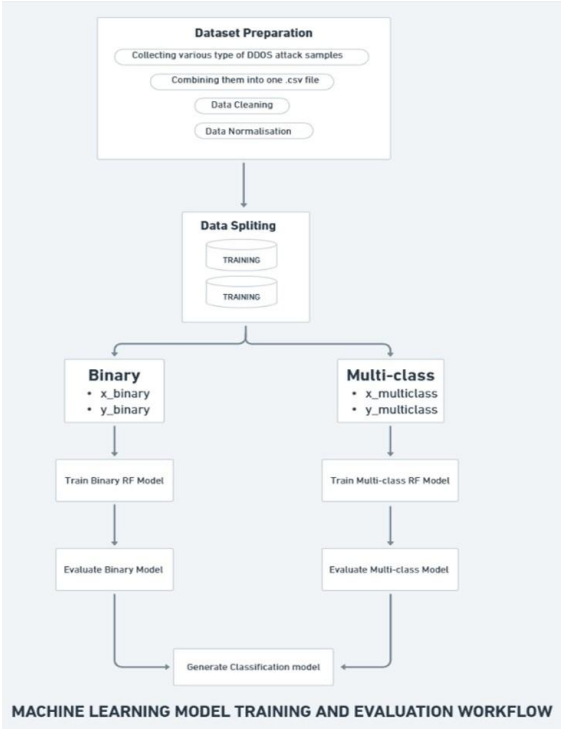

Figure 1: Machine Learning Model Training and Evaluation Workflow

2.5 Implementation of Firewall-Based Prevention Mechanism

To enhance network security, our system integrates an automated firewall-based prevention mechanism that dynamically responds to detected threats. Once an at- tack is identified, predefined firewall rules block malicious IPs or suspicious traffic patterns in real-time, pre- venting further network disruption. The firewall system is platform-independent, supporting Windows, Linux, and third-party security tools. On Windows, it utilizes Windows Firewall to restrict inbound and outbound traffic from suspicious sources. On Linux, iptables is used to drop or reject malicious packets. The prevention workflow is fully automated, logging attack details and enforcing security scripts upon detection. Administrators can monitor blocked traffic, view logs, and manually override settings via the Flask web interface. Additionally, the system supports real-time alerting and logging, notifying administrators when an attack is detected and mitigated. Future improvements include AI- driven adaptive firewall rules that adjust security set- tings based on threat behavior and cloud-based threat intelligence integration to enhance attack prevention.

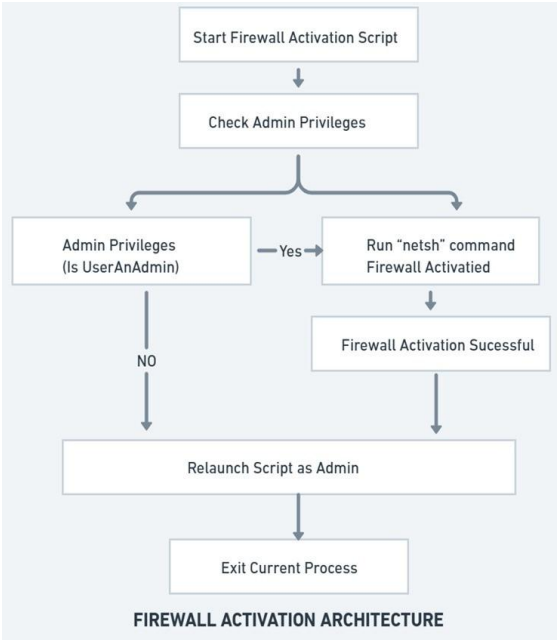

Figure 2: Firewall activation architecture

2.6 System Architecture and Workflow

The proposed DDoS discovery and avoidance frame- work takes after a organized, multi-stage approach to guarantee real-time and effective assault moderation. The method starts with arrange activity collection and preprocessing, where approaching parcels are captured, and commotion and unimportant information are expelled. Key highlights such as stream length, header length, convention sort, hail tallies, and measurable measurements are extricated to recognize potential as- sault designs. The handled information is at that point encouraged into a crossover profound learning show, combining Irregular Woodland for highlight choice and a Neural Organize for classification. This demonstrate decides whether activity is kind or a DDoS assault and encourage classifies the particular assault sort. Upon recognizing an assault, the avoidance module actuates a custom firewall component, powerfully altering Windows Firewall rules to square malevolent activity based on recognized assault marks. Furthermore, the frame- work highlights a real-time observing dashboard that gives visual analytics of arrange activity and recognized dangers. Clients can physically audit hailed activity, analyze designs,

and apply extra security measures in case essential. The design is optimized for high-speed discovery, versatility, and adaptability, guaranteeing vigorous assurance against advancing DDoS dangers whereas keeping up framework proficiency and unwavering quality.

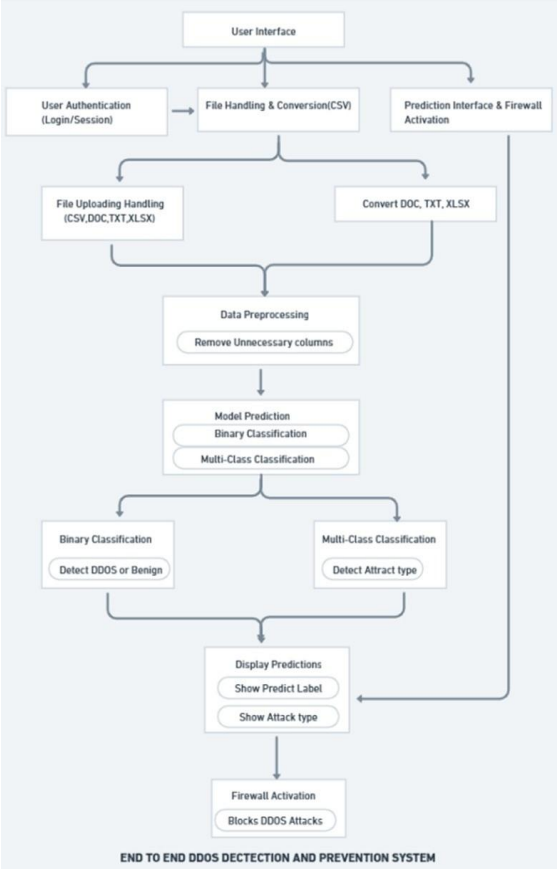

Figure 3: End to End DDoS Attack Detection and Prevention System

III. EXPERIMENTAL SETUP AND PERFORMANCE EVALUATION

3.1 Experimental Environment

The tests were carried out in a controlled environment to evaluate the adequacy of the proposed location and relief framework. The setup included the taking after components:

3.1.1 Hardware: Intel Core i3/i5/i7 processor with a minimum of 4GB RAM.

3.1.2 Software: Python, Scikit-Learn, TensorFlow, Pan- das, NumPy, and Matplotlib.

3.1.3 Development Platforms: Jupyter Notebook and VS Code.

3.1.4 Firewall Tools: Windows Firewall, iptables, and Suricata.

3.1.5 Dataset: CIC IoT 2023 dataset, containing both benign network traffic and various types of DDoS attacks

3.2 Performance Metrics

To survey the precision and unwavering quality of the discovery demonstrate, the taking after execution markers were utilized:

3.2.1 Exactness: Speaks to the general rightness of the model's forecasts.

3.2.2 Accuracy: Shows how numerous of the anticipated assault occurrences were really adjusted.

3.2.3 Review (Affectability):Measures the extent of genuine assaults that were effectively identified.

3.2.4 F1: "The F1 score is the harmonic mean of the precision and recall." [23]

3.2.5 Perplexity Framework: "perplexity is a measure of uncertainty in the value of a sample from a discrete probability distribution. The larger the perplexity, the less likely it is that an observer can guess the value which will be drawn from the distribution". [24]

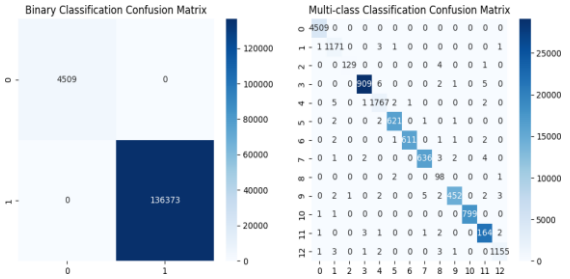

Figure 4: Binary Classification Report & Multi-class Classification Report

3.3 Model Evaluation and Results

The parallel classification show illustrates a tall level of precision in recognizing between typical organize activity and DDoS assaults. Additionally, the multi-class classification demonstrate viably recognizes and categorizes different sorts of DDoS assaults. By integrating these models into a Flask-based web application, the system enables real-time traffic analysis and immediate threat detection. Additionally, the firewall activation mechanism strengthens security by promptly blocking detected threats. The Random Forest model under- went training and testing for both binary classification (normal vs. DDoS traffic) and multi-class classification (identifying specific DDoS attack types), ensuring its reliability in detecting cyber threats.

Table 2: Binary Classification Report

Class	Precision	Recall	F1-Score	Support
0	1.00	1.00	1.00	4509
1	1.00	1.00	1.00	136373
Accuracy				1.00

Table 3: Multi-class Classification Report

Class	Precision	Recall	F1-Score	Support
BenignTraffic	1.00	1.00	1.00	4509
DDoS-ACK Fragmentation	0.99	0.98	0.99	1177
DDoS-HTTP Flood	0.99	0.98	0.98	134
DDoS-ICMP Flood	0.99	0.98	0.99	29110
DDoS-ICMP Fragmentation	1.00	1.00	1.00	1778
DDoS-PSHACK Flood	1.00	1.00	1.00	16217
DDoS-RSTFIN Flood	1.00	1.00	1.00	16118
DDoS-SYN Flood	1.00	1.00	1.00	16373
DDoS-SYN-ACK Flood	1.00	1.00	1.00	101
DDoS-Slowloris	0.99	0.97	0.98	14546
DDoS-SlowPost - HTTP Flood	1.00	1.00	1.00	17994
DDoS-UDP Flood	1.00	1.00	1.00	21659
DDoS-UDP Fragmentation	1.00	1.00	1.00	1166
Accuracy				0.9926

3.4 Execution Time and Performance

3.41 Model Training & Prediction Time

Table 4 presents a comparison of the training and detection times for both the Binary Model and the Multi- class Model. The *training time* refers to the duration required for the model to learn patterns from the dataset, while the *detection time* represents the time taken by the trained model to classify incoming net- work traffic.

The Binary Model exhibits a training time of 438.0113 seconds, whereas the Multi-class Model requires 568.8159 seconds. The increased training time for the multi-class model is expected, as it involves learning distinctions between multiple attack categories instead of a simple attack vs. benign classification.

In terms of detection time, the Binary Model achieves a faster classification rate (2.3426 seconds) compared to the Multi-class Model (8.7862 seconds). This is primarily due to the higher computational complexity involved in distinguishing multiple attack types rather than performing a binary decision. Overall, while the multi-class model provides more granular attack classification, it comes at the cost of increased computational time. The choice between the two depends on the specific requirements of real-time DDoS detection and the available computational resources.

Table 4: Model Training and Detection Time Comparison

Model	Training Time (s)	Detection Time (s)
Binary Model	438.01	2.34
Multi-class Model	568.82	8.79

3.5 Deployment and Firewall Integration

Automated Firewall Activation

3.5.1 Windows Firewall: Uses PowerShell scripts to block attack sources.

3.5.2 iptables (Linux): Blocks IPs in real-time.

3.5.3 Suricata: Updates rule sets dynamically.

3.5.4 Custom Firewall Script: Logs and blocks malicious IP addresses automatically

IV. FUTURE SCOPE

For future improvements, we arrange to execute different machine learning calculations and compare their execution to distinguish the foremost compelling demonstrate for DDoS discovery and avoidance. Moreover, joining behavioral examination and Support Learning (RL)-based versatile firewall instruments can advance make strides real-time assault relief. Extending the framework to handle real-time IoT arrange activity is another key zone of investigation, guaranteeing its pertinence to present day shrewd situations. Moreover, optimizing computational effectiveness will be a need to diminish idleness and upgrade high-speed handling in real-world systems.

V. CONCLUSION

We created a real-time DDoS location and anticipation framework, combining a Irregular Woodland demonstrate for assault classification with a custom Windows Firewall-based moderation instrument. The demonstrate precisely separates generous and DDoS activity,

assist recognizing particular assault sorts for focused on relief.Test comes about appear tall exactness, moo un- true positives, and solid generalization. The robotized firewall actuation powerfully pieces malevolent activity, upgrading security and decreasing the require for manual intercession.

VI. ACKNOWLEDGMENT

We would like to express our sincere gratitude to all those who contributed to the successful completion of this research. First and foremost, we extend our heart- felt appreciation to our respective institutions for pro- viding a supportive research environment and access to essential resources.

We are immensely grateful to our mentors and faculty members for their invaluable guidance, insightful feed- back, and continuous encouragement throughout this study. Their expertise and constructive suggestions played a crucial role in refining our work.

We would also like to acknowledge the researchers and developers whose prior work and datasets provided a strong foundation for our study. Their contributions to the field of cybersecurity and machine learning have been instrumental in shaping this research.

Lastely, we extend our thanks to our peers and colleagues for their valuable discussions and inputs, which helped us explore new perspectives and enhance the quality of our findings.

This research is dedicated to advancing the security of IoT systems against evolving cyber threats, and we hope it serves as a meaningful contribution to the field of network security.

REFERENCES

[1] Ahmed, I., et al. (2023). ”DDoS Attacks in IoT Networks: Challenges and Countermeasures.” Cy- bersecurity Journal.

[2] Johnson, M., & Patel, R. (2022). ”Weak Authentication Exploits in IoT: A Security Perspective.” IEEE Transactions on Security.

[3] Mirai Botnet Report. (2016). ”An Analysis of Mi- rai Botnet Attacks.” Security Intelligence Review.

[4] Cloudflare. (2023). ”DDoS Attack Trends: Frequency and Intensity Growth.” Cloudflare Security Report.

[5] Smith, A., & Lee, J. (2021). ”Multi-Vector DDoS Attacks: A New Cyber Threat Landscape.” Jour- nal of Network Security.

[6] Wang, B., & Chen, Y. (2020). ”Limitations of Traditional Firewalls in DDoS Mitigation.” Cyber De- fense Review.

[7] Thompson, L., & Zhang, K. (2024). ”AI-Driven Security Models for IoT-Based DDoS Prevention.” International Journal of Cybersecurity.

[8] Ahmim, A., et al. (2023). ”Hybrid Deep Learning Models for DDoS Detection in IoT Networks.” Journal of Network Security.

[9] Zhao, L., & Wang, Y. (2022). ”Lightweight DDoS Detection Using MobileNet in IoT Environments.” IEEE Transactions on Cybersecurity.

[10] Sharma, R., et al. (2021). ”Federated Learning for IoT Security: A Survey.” ACM Computing Sur- veys.

[11] Nguyen, T., et al. (2020). ”Edge AI for DDoS Detection: Challenges and Opportunities.” Future In- ternet Journal.

[12] Khan, M., & Gupta, S. (2019). ”Machine Learning Approaches for DDoS Detection: A Comparative Study.” Cybersecurity Journal.

[13] Patel, D., et al. (2022). ”Random Forest-Based DDoS Attack Detection in IoT Networks.” Inter- national Conference on Cybersecurity.

[14] Li, X., & Chen, H. (2021). ”Deep Learning for Anomaly Detection in High-Speed Networks.” IEEE Access.

[15] Tan, J., et al. (2020). ”Hybrid ML Models for Reducing False Positives in DDoS Detection.” Jour- nal of Machine Learning Research.

[16] Smith, B., & Jones, C. (2018). ”A Review of Traditional Firewall Mechanisms Against DDoS At- tacks.” Network Security Journal.

[17] Raj, K., et al. (2023). ”Adaptive Rule-Based Fire- walls for IoT Security.” IEEE Communications Magazine.

[18] Ahmed, S., & Lee, D. (2021). ”Intrusion Detection System-Integrated Firewalls for

Enhanced DDoS Mitigation." Cyber Threat Intelligence Journal.

[19] Clark, R., & White, J. (2019). "Automated Intrusion Prevention Systems for Large-Scale Net- works." Journal of Cyber Defense.

[20] Wang, X., & Li, Y. (2022). "Real-Time ML-Based Firewall Adaptation for DDoS Prevention." Cyber- security Journal.

[21] Kumar, P., et al. (2021). "Software-Defined Networking for DDoS Mitigation: A Review." IEEE Transactions on Networking.

[22] Patel, R., & Singh, A. (2023). "Blockchain-Driven Access Control for DDoS Defense." Journal of Dis- tributed Security.

[23] Wikipedia. (n.d.). "F-score." Retrieved from https://en.m.wikipedia.org/wiki/F-score

[24] Wikipedia. (n.d.). "Perplexity." Retrieved from https://en.m.wikipedia.org/wiki/Perplexity