IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Detecting DDoS Attacks Through AI driven SDN Intrusion Detection System

[1]Sandesh R, [2]Vinay M, [3]Vivek N P, [4]Suhas P, [5]Priyadarshan H P

[1]Assistant Professor, [2]Student, [3]Student, [4]Student, [5]Student,
[1]Department of Computer science and Engineering,
[1]ATME college of Engineering, Mysuru, India

Abstract: With the increasing prevalence of cyber threats, Distributed Denial-of-Service (DDoS) attacks remain a significant concern for network security. This study introduces an AI-powered DDoS detection system that leverages Machine Learning algorithms, including Random Forest, Logistic Regression, and Neural Networks, to distinguish between legitimate and malicious network traffic in real time. The system is integrated with Software-Defined Networking (SDN) to enable adaptive security measures. A web-based interface, developed using React.js and Tailwind CSS, provides real-time traffic visualization. Experimental evaluations indicate high detection accuracy, reinforcing cybersecurity defenses against evolving attack strategies.

Key word: DDoS Detection, Machine Learning, Software-defined Networking (SDN), Cybersecurity, Real-time Traffic Analysis, Network safety, Web-based Monitoring, Intrusion detection System (IDS).

I. INTRODUCTION

With the increasing threat of cyberattacks, Distributed Denial-of-Service (DDoS) attacks have emerged as a significant challenge, disrupting online services and leading to financial and operational losses. Traditional security approaches, such as rule-based intrusion detection systems and firewalls, often struggle to detect sophisticated DDoS attacks due to their static nature and high false-positive rates. To overcome these limitations, this paper explores AI-driven DDoS detection integrated with Software-Defined Networking (SDN). Machine learning models, including Random Forest, Logistic Regression, and Neural Networks, analyze network traffic in real time to distinguish between legitimate and malicious activity. The use of SDN facilitates dynamic traffic management and automated mitigation, reducing detection time and enhancing response efficiency. Unlike conventional reactive security measures, AI-driven techniques detect anomalies based on behavioral patterns, making them more adaptable to emerging attack tactics. Additionally, SDN integration ensures scalable, real-time mitigation, minimizing service disruptions. This paper examines the effectiveness of AI in detecting DDoS attacks, reviews existing research, and discusses challenges and future directions for strengthening cybersecurity resilience.

II. LITERATURE SURVEY

1. "A Survey on DDoS Attack Detection Techniques in Cloud Computing "

- **Authors:** A. A. Rahman et al.
- **Published in:** 2021

This paper provides a comprehensive survey of DDoS attack detection techniques specifically within cloud computing environments. It categorizes detection methods into signature- based, anomaly-based, and hybrid approaches. The authors highlight the challenges posed by cloud architectures and emphasize the need for scalable, efficient, and adaptive detection mechanisms. The study underscores the potential of machine learning algorithms for enhancing detection accuracy and real-time response to DDoS attacks.

2. "Machine Learning Approaches for DDoS Attack Detection"

- **Authors:** V. K. Jain and S. K. Sharma
- **Published in:** 2020

This survey reviews various machine learning techniques employed in the detection of DDoS attacks. It discusses the advantages and limitations of different algorithms, including Random Forest, Support Vector Machines, and Neural Networks. The authors emphasize the importance of feature selection and dataset quality in improving detection rates. The paper also outlines future research directions to enhance the robustness of DDoS detection systems.

3. "A Survey on Intrusion Detection Systems in Software-Defined Networks"

- **Authors:** F. F. Al-Habsi et al
- **Published in:** 2020

This paper presents a check of intrusion discovery systems designed for Software- Defined Networks (SDN). It discusses the unique security challenges posed by the SDN armature, including the centralization of control and the eventuality for new attack vectors. The authors explore colourful discovery ways, including rule- grounded and machine literacy approaches, pressing their effectiveness in real- time trouble discovery and mitigation within SDN surroundings

4. "AI-Based DDoS Detection in SDN: A Review of Techniques and Applications"

- **Authors:** S. Farahani, A. Saeed
- **Published in:** 2022

This review paper explores AI- grounded ways for detecting DDoS attacks in SDN surroundings. The authors examine colourful machine literacy and deep literacy algorithms used for business analysis, pressing both supervised and unsupervised approaches. The study addresses the challenges of conforming these algorithms to evolving attack patterns and discusses their real- time discovery capabilities within SDN infrastructures.

5. "Detection of DDoS Attacks Using Machine Learning in SDN Environments"

- **Authors:** F. Li, Y. Chen, Z. Liu et al.
- **Published in:** 2021

This paper investigates the operation of machine literacy ways for detecting DDoS attacks in SDN surroundings. The authors review several algorithms, including support vector machines (SVM), decision trees, and arbitrary timbers, and compare their effectiveness in detecting colourful types of DDoS attacks. The paper highlights the significance of real- time discovery and low- quiescence response.

III. PREREQUISITES

1. Understanding DDoS Attacks

DDoS (Distributed Denial-of-Service) attacks can be categorized into different types:
Volumetric Attacks: Overwhelm network bandwidth using high traffic (e.g., UDP flood, ICMP flood).
Protocol Attacks: Exploit vulnerabilities in network protocols (e.g., SYN flood, TCP reset attack).
Application-Layer Attacks: Target application services (e.g., HTTP flood, Slowloris).
Impact on Network Security:
DDoS attacks disrupt service availability, lead to financial losses, and pose risks to critical infrastructure.

2. Basics of Software-Defined Networking (SDN)

SDN Architecture:
Control Plane: Manages network traffic and makes routing decisions centrally.
Data Plane: Handles packet forwarding based on control plane directives.
Northbound & Southbound APIs: Facilitate communication between network devices and SDN controllers.
Security Benefits of SDN:
Centralized management allows real-time monitoring, efficient threat detection, and dynamic response to attacks.

3. Machine Learning in Cybersecurity

Supervised Learning: Uses labeled datasets for training models such as Random Forest and Logistic Regression.
Unsupervised Learning: Identifies anomalies in network traffic without predefined labels.
Feature Engineering: Selects critical parameters like packet size and flow duration to enhance detection accuracy.

4. Datasets for DDoS Detection

CIC-DDoS2019: Contains real-world traffic data with labeled DDoS attacks.
CAIDA DDoS Dataset: Provides large-scale attack patterns for research.
NSL-KDD: Commonly used for anomaly detection in cybersecurity applications.

5. AI-Driven Detection and Mitigation

Classification Models for DDoS Detection:
Random Forest: Highly accurate and robust in identifying attack patterns.
Logistic Regression: Lightweight model suitable for quick classification tasks.
Neural Networks: Capable of recognizing complex patterns in network traffic.
This structured foundation enables effective implementation of AI-driven intrusion detection and mitigation strategies.

IV. CONCLUSION

The AI-driven SDN Intrusion Detection System effectively enhances network security by leveraging Various Machine Algorithm for real-time DDoS detection. The system ensures high accuracy, low latency, and seamless integration with SDN, making it adaptable to dynamic network environments.

This research highlights the potential of AI in cybersecurity, addressing challenges like false negatives and high-volume traffic management. Future improvements include advanced attack detection, adaptive learning models, and automated threat response, reinforcing AI's role in strengthening cybersecurity defences against evolving threats

REFERENCES

[1] **Al-Razib, M., & Islam, S.** (2020). A Survey of DDoS Attack Detection Methods in SDN: Challenges and Future Directions. Journal of Computer Networks and Communications

[2] . **Wang, T., & Wang, J.** (2019). DDoS Attack Detection Using Machine Learning in SDN: A Survey. International Journal of Computer Science and Network Security, 19(2), 12-19.

[3] **Rashid, A., & Islam, M. R.** (2021). A Hybrid Deep Learning Model for DDoS Attack Detection in Software Defined Networks. Journal of Network and Computer Applications, 79, 102880.

[4] **Hussein, A. M., & Saeed, A. H.** (2020). DDoS Detection in SDN-Based Networks Using Machine Learning Algorithms. Proceedings of the International Conference on Networking and Communications Systems, 98-104.

[5] **Sharma, V., & Sharma, S.** (2021). Real-Time DDoS Attack Detection and Mitigation in SDN Using AI Techniques. Journal of Cyber Security Technology, 5(3), 156-173.

[6] **Nguyen, D. C., & Zhang, Y.** (2021). Deep Learning-Based Intrusion Detection System for SDN Against DDoS Attacks. IEEE Transactions on Network and Service Management, 18(4), 3456-3470.

[7] **Yang, Y., & Li, X.** (2020). Detection of DDoS Attacks in SDN Using Machine Learning-Based Intrusion Detection Systems. International Journal of Information Security, 20(1), 1-16.

[8] **Li, X., & Wang, X.** (2020). An Adaptive DDoS Attack Detection Framework in SDN Using Ensemble Learning Techniques. Journal of Cyber Security and Privacy, 1(3), 178-192.

[9] **Farahani, F., & Saeed, A.** (2022). AI-Based DDoS Detection in SDN: A Review of Techniques and Applications. International Journal of Artificial Intelligence and Networks, 2(2), 88-104.

[10] **Li, J., & Zhang, J.** (2021). DDoS Attack Detection in SDN Using Random Forest and Neural Networks. Proceedings of the IEEE International Conference on Cloud Computing, 380-387.