IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144107

AI-DRIVEN DDOS ATTACK DETECTION AND MITIGATION IN SDN

Mrs.S.Jancy Sickory Daisy M.Tech.,[1], A.Ponraj[2], K.Ragul[3], V.Surya[4]

Associate Professor, Department Computer Science and Engineering,

Anand Institute of HigherTechnology, Kazhipattur, Chennai

Student, Department Computer Science and Engineering, Anand Institute of HigherTechnology,Kazhipattur, Chennai

Abstract: DDoS attacks pose a significant threat to Software-Defined Networking (SDN) environments, often overwhelming traditional security mechanisms. This work is primarily concerned with designing an AI-driven DDoS detection and mitigation system, which is expected to improve scalability, adaptability, and overall efficiency of network security operations. The system aspires to use AI-based models, including Multi-Armed Bandit, Random Forest, and Online Gradient Boosting, to dynamically detect anomalies, classify attack traffic, and implement intelligent mitigation strategies in real time. A comparative analysis of these models illustrates the benefits of AI technologies in enhancing detection accuracy, reducing false positives, and optimizing network performance. The paper also provides an analysis of the challenges associated with AI-based intrusion prevention and explores various future directions, such as the use of federated learning for collaborative threat intelligence sharing. Through studies on AI-based cyber security solutions, many researchers recognize both the potential and challenges in the deployment of real-time, adaptive DDoS mitigation strategies.

Keywords: DDoS Mitigation, AI-Driven Security, SDN Protection, Multi-Armed Bandit, Online Gradient Boosting, Anomaly Detection, Threat Intelligence.

1. INTRODUCTION

Software-Defined Networking (SDN) is a modern approach to managing computer networks. It separates the network's control functions from the data flow, which allows for easier configuration, centralized decision-making, and flexible traffic handling. This architecture provides better control over network operations, but at the same time, introduces new types of security threats. One major concern is the risk of Distributed Denial of Service (DDoS) attacks, which can severely disrupt network performance.

DDoS attacks happen when a large number of devices send overwhelming amounts of data to a network or server, making it difficult or impossible for legitimate users to access services. In SDN environments, attackers often target the centralized controller, which is responsible for managing all traffic flows. Since SDN networks are programmable and dynamic, they become attractive targets for attackers trying to manipulate or overload network controls.
To deal with these problems, many researchers are turning to Artificial Intelligence (AI) and Machine Learning (ML) techniques These tools are capable of identifying unusual patterns in traffic that might signal a DDoS attack. However, traditional machine learning models often struggle with fast-changing attack methods and may not adapt well to new threats without frequent updates.

This research introduces a smart DDoS detection and response system that uses multiple AI models together. It includes Multi-Armed Bandit (MAB) for decision-making, Random Forest (RF) for classification, and Online Gradient Boosting (OGB) for real-time learning. This combined approach helps the system continuously adjust to new traffic behaviors, detect attacks accurately, and respond effectively.

The proposed method aims to reduce the number of false alarms and improve the speed and accuracy of detection. By learning from live network traffic, the system adapts over time to provide stronger protection against both old and emerging DDoS threats. This paper also discusses the key difficulties in building such systems and outlines possible improvements for the future, including better model training and safer traffic handling methods in SDN networks.

Furthermore, the use of adaptive learning ensures that the system remains effective even in unpredictable traffic conditions. Our approach not only strengthens SDN security but also minimizes the performance impact of detection

DOI: 10.17148/IJARCCE.2025.144107

mechanisms. As AI continues to evolve, its role in securing programmable networks like SDN is expected to grow even more critical.

Another critical advantage of using AI-powered detection systems in SDN is their ability to perform deep traffic inspection and identify low-rate or stealthy DDoS attacks that evade traditional threshold-based mechanisms. These low-rate attacks, which often mimic legitimate traffic patterns, are designed to fly under the radar by consuming server resources gradually over time. The incorporation of

ensemble learning methods, such as combining Random Forest with Online Gradient Boosting, strengthens the model's ability to recognize subtle anomalies.This layered strategy enhances the system's resilience and makes it capable of detecting a wide variety of attack vectors without being limited to predefined rules or historical patterns.

In addition, integrating intelligent feedback mechanisms through the Multi-Armed Bandit approach enables the system to learn which model performs best under different network conditions and prioritize it accordingly. This not only optimizes resource usage but also ensures that the system stays robust as traffic behavior evolves. The feedback loop created through real-time learning and model selection allows for quicker adaptation to zero-day attacks—those that exploit previously unknown vulnerabilities. Overall, the synergy between AI models and the flexible SDN infrastructure provides a scalable, adaptive defense solution that evolves in lockstep with the threat landscape, reinforcing the future of secure and intelligent networking.

2. PRELIMINARIES

This section outlines foundational concepts including Software-Defined Networking (SDN), Low-rate DDoS (LDDoS) attacks, Zero-day DDoS threats, Online Machine Learning (OML), and Ensemble Learning techniques.

A. Software-Defined Networks (sdn)

Software-Defined Networking introduces a modernized framework for designing and managing networks. Unlike traditional systems where the control and data planes are tightly coupled within networking devices like routers and switches, SDN separates these planes. This separation enables centralized network management via a controller—commonly referred to as the SDN controller.

SDN is typically organized into three layers: the Application Layer, Control Layer, and Infrastructure Layer. The controller, positioned in the control layer, uses protocols such as OpenFlow to communicate with lower-level devices. It maintains a holistic view of the network, allowing it to make informed, real-time decisions on traffic flow, quality of service (QoS), and security policies. SDN-enabled switches follow instructions from the controller and operate primarily at the data layer. This architecture allows for enhanced flexibility, easier automation, and efficient policy enforcement.

B. Low-Rate Distributed Denial of Service (lDDoS) attacks

Low-rate DDoS attacks are a stealthier variant of traditional DDoS threats. Rather than overwhelming the network with massive traffic volumes, LDDoS attacks slowly drain resources over time by sending intermittent, seemingly legitimate requests.

These types of attacks commonly employ techniques such as Slowloris or RUDY (R-U-Dead-Yet), which exploit connection- handling vulnerabilities in web servers. Bymaintaining many open, low-activity connections, the attacker exhausts the server's capacity to process legitimate user requests. Because of their low traffic footprint, LDDoS attacks are difficult to detect with standard threshold-based defense systems.

C. Zero-Day DDoS Attacks

Zero-day DDoS attacks exploit vulnerabilities that are newly discovered and for which no fix currently exists. These attacks occur on or before the same day the vulnerability becomes publicly known—leaving no time for patching or preventive action.

Detecting zero-day attacks is challenging for traditional machine learning models, which depend on historical data and known threat signatures. Because these threats are novel, they often bypass conventional filters. Additionally, attackers frequently adapt and evolve their tactics, rendering static models less effective. Feature extraction is also problematic,

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144107

as the defining characteristics of zero-day threats may not be clear at the time of the attack.

D. Online Machine Learning (OML)

Online Machine Learning is a subset of ML designed to process data in a continuous and adaptive fashion. Unlike traditional (batch) ML models trained on fixed datasets, OML updates its predictive models as new data arrives—enabling real-time learning and faster adaptation to emerging threats.

This incremental learning approach makes OML particularly suited for cybersecurity tasks such as intrusion detection and DDoS mitigation, where attack patterns evolve rapidly. Its flexibility enables it to adjust to the latest threat landscapes with minimal delay, enhancing both accuracy and response time.

E. Ensemble Machine Learning Model

Ensemble learning combines multiple individual models to build a robust and accurate predictive system. The central idea is to aggregate different learners—each capturing unique patterns in the data—to produce a collective output that is more reliable than any single model.

In DDoS detection scenarios, ensemble methods improve resilience to data imbalance, adapt to network changes, and reduce the risk of false positives. By integrating models like decision trees, random forests, and neural networks, ensemble techniques boost detection accuracy and enhance the system's ability to recognize a wider variety of attack behaviors. These models are well-suited for dynamic environments like SDN, where maintaining continuous protection is critical.

3. RELATED WORK

As Software-Defined Networking (SDN) has become more widely used, securing networks against Distributed Denial of Service (DDoS) attacks has become a key concern.

Traditional security methods, which rely on fixed rulesand traffic thresholds, are often not effective at detecting evolving or low-rate attacks in SDN environments. To overcome these challenges, machine learning (ML) models such as Support Vector Machines (SVM) and Decision Trees have been explored to improve traffic classification. However, these models still face difficulties in adapting to real-time changes.

Recent studies have focused on using ensemble methods like Random Forest (RF) and Gradient Boosting (GB) to enhance detection accuracy. Online learning methods have also been introduced, allowing systems to adjust to dynamic traffic without needing frequent retraining. Additionally, Multi- Armed Bandit (MAB) strategies have been used to optimize defensive decisions by balancing new approaches and existing ones.

Despite these advancements, there are still challenges such as high false positives, real-time adaptability, and scalability. This paper proposes a new AI-based system combining RF, Online Gradient Boosting, and MAB to achieve accurate, adaptive, and scalable DDoS detection and mitigation in SDN networks.

TABLE I. Key Findings and Limitation of ML Algorithm

S.no	ML Algorithm(s)	Key Findings & Limitations
1.	Random Forest, SVM	High detection rate but prone to high FP rates.
2.	Decision Tree, XGBoost	Good accuracy, but lacks real-time processing.
3.	CNN, LSTM	Effective for anomaly detection but requires high computational resources.
4.	KNN, Naïve Bayes	Lightweight but less effective for complex attack types.
5.	Entropy-based ML model	Improved detection accuracy but higher computational cost.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025
DOI: 10.17148/IJARCCE.2025.144107

6.	Optimized AI Model	Achieves balance between performance and processing time.
7.	Online ML Model	Effective for real-time low- rate DDoS detection.

4. PROPOSED SYSTEM

The proposed system aims to create an adaptive and scalablesolution for detecting and mitigating Distributed Denial of Service (DDoS) attacks within Software-Defined Networking (SDN) environments. The system utilizes a combination of AI-based models to dynamically analyze traffic, classify anomalies, and execute real-time mitigation actions. The key components of the system are as follows:

1. Traffic Monitoring and Data Collection

Network Traffic Capture: The system continuously monitors the SDN environment, collecting real-time network traffic data from the SDN controller and switches. This data includes features like packet size, flow rate, source and destination IP addresses, and protocol types.

Preprocessing: Raw traffic data is preprocessed to remove irrelevant information and normalize the features for input into machine learning models. Data is filtered to identify relevant patterns that could indicate attack behavior.

2. AI-based Anomaly Detection Models

Random Forest (RF): RF models are trained on historical network traffic data to identify patterns and classify traffic as normal or malicious. The model uses an ensemble of decision trees to improve accuracy and reduce the likelihood of false positives.

Online Gradient Boosting (OGB): OGB is used to detect sudden shifts or anomalies in network traffic in real time. It allows the system to adapt to dynamic traffic patterns without requiring frequent retraining, making it suitable for SDN environments with constantly changing network conditions.

Multi-Armed Bandit (MAB): The MAB algorithm is incorporated to optimize defense actions by exploring various mitigation strategies. It helps in selecting the best possible defense strategy based on the current attack situation, balancing exploration of new strategies and exploitation of known effective ones.

3. Dynamic Traffic Classification and Attack Detection

Anomaly Detection: The models work together to detect suspicious traffic by comparing incoming traffic against learned patterns. Any significant deviation from normal traffic behavior is flagged as a potential DDoS attack.

Real-Time Classification: The AI models classify network traffic into different categories, such as normal traffic, known attack types, and unknown or emerging attacks. This classification enables the system to respond appropriately to different kinds of threats.

4. Mitigation Strategy Implementation

Intelligent Mitigation: Once an attack is detected, the system immediately triggers mitigation strategies, which could include traffic filtering, rate-limiting, or traffic redirection to minimize the impact of the attack.

Adaptive Defense: The system continuously adjusts mitigation strategies based on feedback from the environment and ongoing attack patterns, ensuring minimal disruption to legitimate traffic while effectively neutralizing threats.

Collaborative Threat Intelligence Sharing: The system incorporates federated learning, where threat data and insights are shared across different SDN environments without compromising privacy. This collaborative approach helps improve detection accuracy and strengthens the overall defense network.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144107

5. Evaluation and Performance Metrics

Accuracy and False Positive Rates: The system's performance is evaluated based on its accuracy in identifying DDoS attacks and minimizing false positives. Performance metrics such as precision, recall, F1-score, and detection time are used to assess the effectiveness of the detection models.

Scalability: The proposed system is designed to scale with increasing network size and complexity, ensuring that it can handle large-scale SDN environments efficiently.

Efficiency: The system evaluates the efficiency of defense actions by measuring the impact on network performance (e.g., latency and throughput) during attack mitigation.

TABLE II. Comparison of Existing Approaches Using ML Algorithms

S.no	Study/ Approach	ML Algorithm(s) Used	Dataset Used	Accuracy
1.	[1] Zhang et al. (2024)	Random Forest, CatBoost	CICDDoS2019	95.6%
2.	[2] Singh & Behal (2020)	Decision Tree, XGBoost	NSL-KDD	93.4%
3.	[3] Alashhab et al. (2021)	CNN, LSTM	Custom Dataset	96.2%
4.	[4] Singh & Bhandari (2020)	KNN, Naïve Bayes	InSDN	91.8%
5.	[5] Al-Dunainawi et al. (2023)	Optimized AI Model	SDN Environment	98.3%
6.	[6] Alashhab et al. (2023)	Online ML Model	Low-rate DDoS (SDN)	97.6%

5. ARCHITECTURAL DESIGN

The architecture of the proposed system consists of various components integrated within the Software- Defined Networking (SDN) environment to detect and mitigate Distributed Denial of Service (DDoS) attacks using machine learning models. The goal is to create an adaptive, efficient, and scalable solution to enhance network security. encompasses three primary modules:

1. Network Infrastructure Layer (SDN Network)

SDN Controller: The central management point for the SDN network that configures and monitors the traffic flow, forwarding rules, and routing in the network.

SDN Switches: Devices that forward data packets based on instructions from the SDN controller. They provide data that the system analyzes in real time for attack detection.

Data Plane: The physical or virtual devices that perform the forwarding of data, continuously transmitting traffic for analysis.

2. Data Collection and Preprocessing Layer

Traffic Monitoring Agent: Deployed on network switches, this component captures and collects real-time traffic data (e.g., packet size, flow rate, IP addresses, etc.) for further analysis.

Preprocessing Unit: This unit performs necessary data cleaning and normalization, filtering the collected traffic to

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144107

extract the key features relevant for machine learning analysis.

3. AI-Driven Detection and Classification Layer

Traffic Classification and Detection Models:

Random Forest (RF): Used to identify patterns from historical data and classify traffic as either benign or malicious.

Online Gradient Boosting (OGB): A real-time model for identifying sudden anomalies and adapting to changes in traffic flow, ensuring rapid detection without the need for frequent retraining.

Multi-Armed Bandit (MAB): This approach optimizes the decision-making process, allowing the system to test different mitigation strategies and choose the best action based on observed attack patterns.

Anomaly Detection: AI models continuously analyze the traffic and detect any deviations from normal behavior, indicating potential DDoS attacks.

4. Mitigation and Response Layer

Mitigation Mechanism: Upon identifying malicious traffic, this layer implements mitigation techniques such as:

Traffic Filtering: Blocking traffic that is identified as part of a DDoS attack.

Rate Limiting: Restricting the amount of traffic allowed to flow to the target systems.

Traffic Redirection: Redirecting suspicious traffic to alternative paths to protect critical network segments.

Adaptive Defense: The system adjusts its defense mechanisms based on ongoing traffic patterns and the type of attack detected.

5. Continuous Learning and Feedback Layer

Online Learning Algorithm: The system adapts and improves its detection capabilities by updating its models continuously with new traffic data, ensuring real-time adaptation to evolving threats.

Collaborative Learning: Future upgrades could incorporate federated learning, allowing multiple SDN environments to share threat intelligence without compromising privacy, thus improving detection across a wide network.

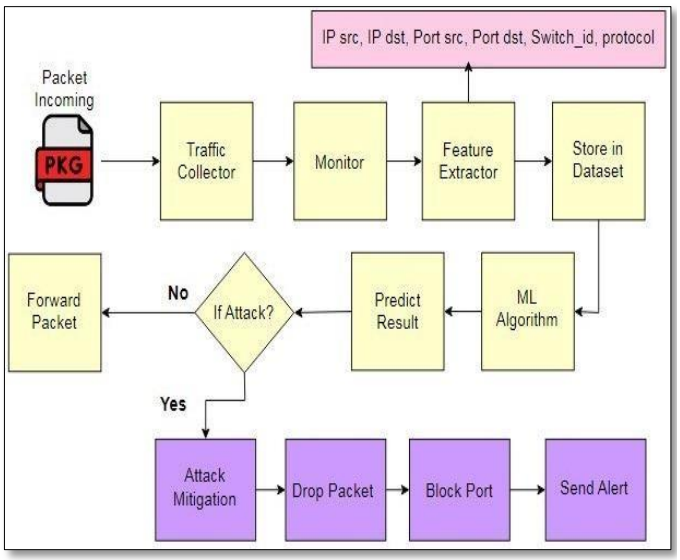

Fig 5.1

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144107

6. EXPERIMENT SETUP

This section describes the experimental setup used to evaluate the AI-driven DDoS detection and mitigation system within a Software-Defined Networking (SDN) environment. The system is designed to improve scalability, adaptability, accuracy, and efficiency in mitigating DDoS attacks.

6.1 Software Setup

The software components of the experiment include the following:

Ryu SDN Controller: The Ryu SDN controller, running on an Ubuntu-based server, is used to manage the SDN network. Itcontrols the virtual switches and interacts with traffic monitoring agents deployed on the switches. Ryu supports OpenFlow and enables the creation of custom network applications for managing SDN traffic.

Mininet Network Simulator: Mininet is used to emulate the SDN topology. It creates a virtual network environment with virtual switches and hosts connected to the Ryu controller. This setup allows the simulation of both normal network traffic and DDoS attack traffic.

Traffic Generation Tools: To simulate DDoS attacks, tools like Hping3 or Ostinato are used to create attack traffic (such as SYN floods, UDP floods, etc.). Normal network traffic is generated using Iperf or NetFlow to simulate real-world conditions.

Machine Learning Models:

Random Forest (RF): This model is used to classify network traffic patterns. It is implemented using Python's scikit-learn library.

Online Gradient Boosting (OGB): This model adapts to real-time traffic changes and is implemented using libraries such as Scikit-Multiflow or Vowpal Wabbit.

Multi-Armed Bandit (MAB): UCB1 (Upper Confidence Bound) and Thompson Sampling algorithms are used to optimize defense decisions by balancing exploration and exploitation.

Mitigation Tools: Mitigation actions are executed using iptables and OpenFlow-based rules in the Ryu controller. These tools filter malicious traffic, apply rate-limiting, or redirect traffic to prevent DDoS impacts.

6.2 Network Configuration

The network setup consists of the following:

SDN Topology: A virtual SDN topology is created using Mininet on Ubuntu. The topology includes multiple virtual switches connected to the Ryu controller. The switches forward traffic according to flow rules set by the controller.

Traffic Monitoring Agents: These agents are deployed on Mininet switches to capture real-time traffic data, which is analyzed to detect anomalies indicative of DDoS attacks. This data is fed into the machine learning models for traffic classification and attack detection.

6.3 Experimental Procedure

The following steps outline the experimental procedure:

Network Initialization: The Ryu SDN controller is initialized, and the Mininet network topology is set up. Traffic monitoring agents are deployed on the switches to collect traffic data.

Model Training: The machine learning models (Random

Forest, Online Gradient Boosting, and Multi-Armed Bandit) are trained using historical traffic data. These models are designed to identify attack traffic and classify it appropriately.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144107

Traffic Simulation: Attack traffic is simulated using tools such as Hping3 or Ostinato, while Iperf or NetFlow generates legitimate traffic. This simulation is used to test the system's ability to detect and mitigate DDoS attacks.

Attack Detection and Mitigation: Once an attack is detected, the machine learning models (RF, OGB, MAB) classify the traffic. The Ryu controller then applies mitigation actions such as filtering, rate-limiting, or rerouting traffic to manage the attack.

Continuous Learning: The Online Gradient Boosting model is updated with new data in real-time, allowing it to adapt to evolving attack patterns. The Multi-Armed Bandit model optimizes the mitigation strategies dynamically by balancing exploration (testing new actions) and exploitation (using the best-known actions).

7. RESULTS AND DISCUSSION

To evaluate the ensemble model's performance, which incorporates Multi-Armed Bandit, Random Forest, and Online Gradient Boosting on the acquired dataset, we employ key performance indicators: accuracy, precision, recall, F1-score, and false alarm rate. These metrics rely on values derived from true positives, true negatives, false positives, and false negatives. The goal of the proposed model is to achieve high detection accuracy while minimizing false positives.

A. EVALUATION METRICS OF THE DETECTION PHASE

1) Prediction Accuracy

The ensemble model demonstrates superior performance, surpassing individual classifiers with an accuracy of **0.9926**, confirming its effectiveness in detecting DDoS attacks. The comparative analysis of classifier accuracy highlights the advantages of combining multiple ML algorithms.

2) Precision

Precision evaluates the model's ability to minimize false positives. The ensemble model achieves a precision of 0.9910, indicating its effectiveness in reducing incorrect attack classifications.

3) Recall

Recall measures the model's success in identifying actual attacks. The ensemble model attains a recall of 0.9962, demonstrating high sensitivity in capturing DDoS threats.

4) F1 Score

The F1 score balances precision and recall, providing a comprehensive assessment of the model's detection capability. The ensemble model achieves an F1-score of 0.9817, reinforcing its robustness.False Alarm Rate
A key objective is to minimize false alarms. The ensemble model records a false alarm rate of 0.025, ensuring minimal disruption to normal network traffic.

5) Evaluation on Benchmark Datasets

The model was tested on CICIDS2019, InSDN, and slow read-DDoS-attack-in-SDN datasets. It achieved high accuracy across all datasets, confirming its adaptability to diverse attack scenarios

TABLE III. Performance of the Proposed Method on Different Datasets.

Dataset	Accuracy	Precision	Recall	F1-Score	False Positive
CICID S2019	98.70%	99.78%	98.81%	98.78%	18.5%
InSDN	98.20%	97.51%	97.93%	98.27%	18%

DOI: 10.17148/IJARCCE.2025.144107

Slow- read-DDoS-attack	98.88%	96.80%	95.90%	96.27%	3.65%
Custom Dataset	99.26%	99.10%	99.60%	98.17%	2.25%

8. FUTURE ENHANCEMENT

Future research will focus on deploying the model in real- world network infrastructures to evaluate its performance in dynamic, live environments. Additionally, there will be exploration of deep learning-based enhancements to further improve the detection accuracy and ability to recognize complex attack patterns. Validation of the system's performance in large-scale environments, including testing its scalability and robustness in high-traffic networks, will be a key area of focus.

Further, the integration of advanced threat intelligence systems, such as integrating AI-driven anomaly detection mechanisms, could significantly enhance the system's ability to detect emerging, unknown attack vectors. The model's capabilities will also be extended to cloud-based SDN frameworks to provide a comprehensive, multi- layered cybersecurity solution that addresses the unique challenges of cloud infrastructure. Moreover, integrating this system with automated mitigation protocols could help improve response times and reduce the manual intervention required during attack events, making the overall system more efficient and reliable.

9. CONCLUSION

The proposed model, integrating Multi-Armed Bandit, Random Forest, and Online Gradient Boosting, presents a robust and adaptive framework for DDoS attack detection and mitigation in SDN networks. This architecture effectively handles both low-rate and high-rate DDoS incidents, demonstrating superior adaptability and precision. The ensemble approach enhances detection accuracy by dynamically selecting the most effective model based on real-time network conditions, achieving detection and legitimate traffic rates exceeding 99%.

The Multi-Armed Bandit algorithm optimizes decision-making in real-time by dynamically selecting the most suitable classifier for incoming traffic. Random Forest enhances feature selection and classification accuracy, ensuring a reliable detection mechanism. Online Gradient Boosting enables continuous learning and adaptation to evolving attack patterns, significantly improving the system's resilience against zero-day threats. Integration with SDN controllers ensures scalability and flexibility across various network environments. The modular design of the proposed system allows independent enhancements to each component, ensuring long-term adaptability and optimization

REFERENCES

[1] Zhang, Y., Wang, L., & Zhao, M. (2024). Ensemble-based DDoS detection using CICDDoS2019 in SDN. Journal of Cybersecurity and Privacy, 4(1), 1–15.

[2] J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions," *Comput. Sci. Rev.*, vol. 37, Aug. 2020, Art. no. 100279.

[3] A. A. Alashhab, M. S. M. Zahid, A. A. Barka, and A. M. Albaboh, "Experimenting and evaluating the impact of DoS attacks on different SDN controllers," in *Proc. IEEE 1st Int. Maghreb Meeting Conf. Sci. Techn. Autom. Control Comput. Eng. (MI-STA)*, May 2021, pp. 722–727.

[4] M. P. Singh and A. Bhandari, "New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges," *Comput. Commun.*, vol. 154, pp. 509–527, Mar. 2020.

[5] M. Chhabra and B. B. Gupta, "An efficient scheme to prevent DDoS flooding attacks in mobile ad-hoc network (MANET)," *Res. J. Appl. Sci., Eng. Technol.*, vol. 7, no. 10, pp. 2033–2039, Mar. 2014.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144107

[6] A. Mishra, N. Gupta, and B. B. Gupta, "Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller," *Telecommun. Syst.*, vol. 77, no. 1, pp. 47–62, May 2021.

[7] Y. Al-Dunainawi, B. R. Al-Kaseem, and H. S. Al- Raweshidy, "Optimized artificial intelligence model for DDoS detection in SDN environment," *IEEE Access*, vol. 11, pp. 106733–106748, 2023.

[8] Q. Li, H. Huang, R. Li, J. Lv, Z. Yuan, L. Ma, Y. Han, and Y. Jiang, "A comprehensive survey on DDoS defense systems: New trends and challenges," *Comput. Netw.*, vol. 233, Sep. 2023, Art. no. 109895.

[9] A. Bhardwaj, V. Mangat, R. Vig, S. Halder, and M. Conti, "Distributed denial of service attacks in cloud: State- of-the-art of scientific and commercial solutions," *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100332.

[10] A. A. Alashhab, M. S. M. Zahid, M. Abdullahi, and M. S. Rahman, "Real-time detection of low-rate DDoS attacks in SDN-based networks using online machine learning model," in *Proc. 7th Cyber Secur. Netw. Conf. (CSNet)*, Oct. 2023, pp. 95–101.