A Hybrid AI Framework for DDoS Detection and Mitigation in SDN Environments Using CNN, GAN, and Semi-Supervised Learning

Abdelhakim HADJI, Brahim RAOUYANE
Department of Mathematics and Computer Science-Faculty of Sciences Ain Chock,
Computer Sciences and Systems Laboratory, Hassan II University of Casablanca, Casablanca, Morocco

***Abstract*—The fast technological evolution seen in recent years enhanced the performance and scalability of cloud computing infrastructure and Software-Defined Networking architectures. SDN provides programmability, centralized orchestration, and dynamic resource provisioning, while separating the control and data planes to offer promising architectural paradigm for cloud computing environments. Openness and flexibility expose SDN-based networks to other security concerns, such as large-scale Distributed Denial of Service (DDoS) attacks. This paper introduces a hybrid artificial intelligence (AI) framework for detecting and mitigating DDoS attacks in SDN environments. The framework leverages three complementary approaches: Convolutional Neural Networks (CNN) to capture temporal traffic patterns, Generative Adversarial Networks (GAN) to generate synthetic traffic for dataset augmentation and to enhance anomaly detection, and semi-supervised learning techniques to exploit large amounts of unlabeled traffic data. The proposed system is deployed on a testbed combining OpenDaylight as the SDN controller and Mininet for network emulation, while the AI models are trained and run in Anaconda environment. The network traffic flows are collected, processed into statistical features (i.e., packet rates, entropy values, protocol distribution ratios), and analyzed through the hybrid AI pipeline. Mitigation actions are configured through ODL RESTCONF interface, converting the detection into OpenFlow rules to drop or rate-limit the malicious packets. Experimental evaluation demonstrates that the proposed approach achieves high accuracy detection and robustness to unseen attacks patterns demonstrating the value of applying a hybrid CNN, GAN, Semi-supervised learning approach.**

***Keywords*—SDN; CNN; GAN; DDOS; OpenDaylight; Mininet; semi-supervised learning; hybrid AI framework**

I. Introduction

Over the past ten years, advances in technology significantly improved the performance and scalability of both cloud computing infrastructures and Software-Defined Networking (SDN) architectures. Caller in SDN architecture decouples the control plane from the data plane enabling, programmability, centralized orchestration and agile deployment of services to create a more efficient opportunity over a traditional network. This is the initial method to create a new innovative resource into Network Infrastructure as a key paradigm for the next-generation network that supports cloud-based services. However, the same level of openness and flexibility that provides efficiency and potential for innovation also introduces new vulnerabilities, Distributed Denial of Services (DDoS) attacks which remains one of the most significant security challenges to cloud and SDN/adoption of SDN infrastructures.

Conventional supervised machine learning techniques have achieved excellent performance on known DDoS patterns, but they are limited to known DDoS attacks due to the reliance on labeled datasets. [1]. Recent deliberations detailed in the literature indicate that hybrid models that combine supervised techniques with unsupervised and semi-supervised techniques will be favorable in settings with limited labelled data or high costs of labeling their data. Semi-supervised models have been a great way to take advantage of the ubiquitous unlabeled network traffic and exploit it to improve detection framework robustness and reduce annotation costs [2].

In this regard, Convolutional Neural Networks (CNNs) have emerged as an influential force in the realm of network security.

- Intrusion Detection: CNNs are adept at the detection of complex temporal and spatial patterns in traffic flows and thus can be effectively applied to intrusion detection in the environment of software defined networks (SDNs). For example, a CNN model was able to achieve an accuracy of 99.75% when detecting attacks using SDN–IoT networks [3].
- Feature Extraction: CNNs are capable of automatically extracting complex spatial features from high-dimensional traffic [4] data which is required to distinguish between legitimate and malicious flows [4].

In a similar manner, Generative Adversarial Networks (GANs) have also shown potential having significant ramifications for cybersecurity.

- Anomaly Detection: GANs can produce synthetic traffic that resembles legitimate traffic flows, therefore highlighting subtle deviations that may be indicative of zero-day attacks or progressive malware in cloud systems (L & Kousar, 2024).
- Adversarial Training: GANs produce synthetic adversarial DDoS traffic to increase the resilience of detection systems to advanced style attack strategies and adaptive adversaries [5].

While convolutional neural networks (CNNs) and generative adversarial networks (GANs) offer important advantages in terms of detection accuracy and robustness, the adaptation of these methods to changing threat vectors and the consistency of detection performance across heterogenous cloud-SDN environments presents additional challenges. Hybrid deep learning, adversarial modeling, and semi-supervised algorithms would address resilience, as well as detection accuracy and adaptivity.

Although the advancement of machine learning and deep learning applications to DDoS detection is increasing, the literature is still limited in ways in which the contributions of the literature can be invoked. A great deal of research relies on the use of fully labeled datasets, which diminishes their ability to generalize and adapt to attacks that are occurring for the first time. Many papers evaluate DDoS detection algorithms in some isolated or simulated environment and often do not deploy them in a controlled environment with a real SDN controller or in some emulated cloud environment. A great deal of research focuses on improving accuracy but does not consider adaptability and real-time mitigation mechanisms to handle DDoS attacks in SDN-enabled cloud environments. Thus, the importance of this research by offering a hybrid AI framework that combines CNNs, GAN, and Semi-supervised learning in an SDN-cloud testbed with OpendDaylight SDN controller and the Mininet emulator, which is capable of enhancing robustness, scalability, and adaptability within hybrid infrastructures where DDoS detection and mitigation can be improved.

In this paper, we present a hybrid AI framework to detect and mitigate distributed denial-of-service (DDoS) attacks in SDN-enabled cloud environments. The framework was implemented on an experimental testbed to represent an SDN-enabled cloud network, integrating OpenDaylight (ODL) as the control implementation and Mininet as the network emulation tool. The proposed method generates a traffic trace dataset that extracts and analyzes statistical features, such as packet rates, entropy measurements, and protocol ratios through the hybrid AI framework. Mitigation actions were dynamically enforced through ODL's RESTCONF API, acting on detection results and mapping them to OpenFlow rules to drop packets or set rates on egress traffic. Our results demonstrate that this hybrid integration enhances detection accuracy, decreases dependence on labeled datasets, and increases resilience against changing and customizing DDoS attack vectors.

II. Related Work

A. Machine Learning for SDN Security

The application of machine learning (ML) in securing Software-Defined Networking (SDN) structures from Distributed Denial of Service (DDoS) attacks has garnered growing attention in the research community. A recent study conducted by Musmuharam and Suharjito (2023) investigates the performance of multiple classification algorithms—specifically Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbors (KNN)—alongside feature selection techniques such as Recursive Feature Elimination (RFE), Principal Component Analysis (PCA), and t-Distributed Stochastic Neighbor Embedding (t-SNE). The authors found that the KNN model in conjunction with RFE produced highly significant results, achieving an accuracy of 99.97%, precision of 99.98%, recall of 99.96%, and F1 score of 99.97% for DDoS detection in an SDN context [6]. This indicates the effectiveness of custom feature engineering in improving the performance of traditional classifiers.

Complementary research [7] proposed a broader ML-based framework for cyber threat detection in SDN.This academic article examines the examination of cyber threats detection in Software-Defined Networks (SDNs) with a framework of machine learning methodologies by utilizing AI-Enabled Servers at the control and application layers to protect the network from them via identification and remediation of threats. The model makes use of six separate classifiers that are trained on differing metric parameters in the network: Random Forest; K-Nearest Neighbor; Support Vector Machine; Naïve Bayes; Decision Tree; and Logistic Regression, whereby analysis of the data supports that the framework is capable of detecting and remediating risks of a cyber nature; and also proposes recommendations for more effective threat detection in the future, and future security controls.

B. CNNs in Network Security

Convolutional Neural Networks (CNNs) have demonstrated utility for intrusion detection and anomaly detection of systems with Software Defined Networking (SDN) properties, primarily due to their ability to automate spatial and temporal feature extraction from challenging data related to network traffic.

Others examined the weakness of CNNs as a means for developing Intrusion Detection Systems (IDS) for SDNs with respect to the overfitting phenomenon that often degrades the performance of deep learning development[8]. By implementing two new approaches based on regularization or uncertainty with their new learning method of CNNs, they demonstrated their improved resilience to unseen attack. Training and testing the learning method on the InSDN benchmark dataset generated higher generalization for the model and better detection accuracy for unknown intrusion events to enhance security for SDN infrastructures against attacks.

In a more recent study, and with a focus on lightweight DDoS detection and mitigation for SDN, [9] a security framework that integrated an anomaly detection and prevention module utilizing a hybrid CNN-MLP model has been proposed. The design leveraged the ability of CNNs to perform feature extraction with the efficiency of multilayer perceptron's (MLPs) since it provided real-time analysis of network traffic; therefore, their system had the ability to identify anomalies, and respond using flow-rule instructions, premised in the SDN controller, to block attacker IP addresses and mitigate malicious traffic. Overall, they were able to demonstrate cost-effective and real-time solutions, thus indicating the feasibility of hybrid CNN architectures to protect against expensive resource DDoS attacks in SDN time-critical infrastructure.

Collectively, these works demonstrate that CNNs play an important role that can significantly bolster security properties for SDN. They further demonstrate that CNNs bearing the

capability of flexibility and when regularized and/or hybridized with other levels of neural architectures, bring robustness and efficiency to the process of identifying and mitigating many classes of cyber threats.

C. GANs in Cybersecurity

Generative Adversarial Networks (GANs) are now increasing attention within cybersecurity, especially in relation to mitigating the limitations of SDN-based infrastructures. Their two-fold potential of generating realistic synthetic traffic and supporting anomalous detection have made GANs valuable in both research and operational defense areas.

A motivating example of GANs used to support SDN-GAN security was presented [10] to introduced one of the early applications of SDN-GAN, a framework that synthesizes cyber-attack scenarios. They illustrated a way that GANs could autonomously synthesize realistic attack signatures based on known patterns. Doing so enables the training of the detection systems in the endless number of possible attack variations. In this regard, the challenge of SDN security is one that is most vulnerable to programmable environments with frequently unknown and adaptive threats.

Another study has recently introduced the LD-BiHGA system [11], a bi-channel hybrid GAN architecture designed for anomaly detection in multi-domain SDN systems. In their model, the two asymmetric GANs were used for independent learning of normal and abnormal traffic, while the bi-channel attention mechanism provided an additional level of feature extraction. By overcoming concerns of real-time, unbalanced traffic data, the LD-BiHGA system improved accuracy in recognition of anomalies over traditional intrusion detection systems, demonstrating the effectiveness of GANs utilized in hybrid models for larger-scale, complex SDN systems. Overall, these contributions signify the journey of GANs in the cyber security space; from synthetically generating attack scenarios, hybridizing with RNNs, and attention mechanisms for anomaly detection. They exemplify not only the capacity for dataset enhancement and classification imbalance for GANs, but also the viability for adaptive engagement and real-time security within SDN infrastructures.

D. Semi-Supervised Learning for SDN Security

In recent years, semi-supervised learning has gained considerable attention as a viable strategy for detecting DDoS attacks in SDN and cloud-based environments, mainly due to the algorithm's capability of utilizing large quantities of unlabeled traffic data. In contrast to purely supervised techniques, which typically depend on having access to large labeled datasets, semi-supervised learning proves a more practical and viable option for real-world implementations.

In addition, a survey of machine learning techniques for intrusion detection in cloud and SDN environments [12]. They found that ML models can detect anomalous traffic related to DDoS attacks and referenced a clear shift towards adaptive rule-based models to increase the security of routing payloads while preserving network privacy.

In IoT-SDN environments, Ravi and Shalinie (2020) introduced the LEDEM mechanism, which acts as a learning-executed detection and mitigation framework. The LEDEM mechanism demonstrated an accuracy of 96.28% for DDoS detection and established the combination of cloud and SDN architecture with learning techniques as successful[13]. This research shows how dynamic and distributive detection models can benefit resource-constrained infrastructures relying on IoT-SDN.

Khamaiseh et al. [2]examined the effectiveness of supervised versus semi-supervised methods for detecting both known and unknown attacks. Their results indicated that supervised methods performed well when encountering previous attack patterns, however, performance suffered against zero-day attacks, demonstrating the limit of these methods. In comparison, semi-supervised methods demonstrated improved adaptability and resilience, and both authors argued for their eventual role in securing DDoS attacks, especially as part of a future SDN security framework. Deka et al. offered a dynamic, range-based anomaly detection method leveraging semi-supervised algorithms[14]. Their work involved the introduction of a density-based approach to handling unlabeled traffic. To that end, semi-supervised classifiers outperformed other standard supervised classifiers in terms of scalability and accuracy offered in fast changing SDN situations.

Overall, these studies contribute to a growing body of studies acknowledging the value of semi-supervised learning method for reducing the number of labeled data needed to detect attacks regardless of their pattern, and combining cost-effective label data and semi-supervised methods will lead to shared improvements to future DDoS detection and security frameworks.

The literature reviewed in this research clearly indicates that there have been significant developments in the detection and prevention of DDoS attacks, especially in SDN and cloud-based contexts, through machine learning (ML) and deep learning (DL) methods. Classical ML approaches, e.g., Random Forest, Support Vector Machine, and K-Nearest Neighbors, achieved relatively high detection accuracy levels when employed with optimally selected features. However, these ML models remain limited by their reliance on labeled datasets and their limited ability to generalize to new or even zero-day attack datasets.

Deep learning methods, namely convolutional long short-term memory (CNN-LSTM), have shown strong performance in automatically extracting important spatial-temporal features from complex traffic data. Regularization methods and hybrid CNN approaches have also shown the ability to improve generalization performance and reduce overfitting levels, which has also made them more robust for designing an intrusion detection task. In a similar vein, GANs have opened important new lines of research into anomaly detection both in isolation and in conjunction with adversarial training. Additionally, GANs can be employed to generate synthetic traffic data that help balance datasets and create realistic attack data that improves performance robustness. Despite these advances, adapting GAN models to solve multi-domain and real-time SDN settings and cloud contexts still presents significant challenges in computational overhead and interpretability.

Semi-supervised learning has emerged as an exciting alternative to address one of the central challenges of SDN security: the limited/missing labeled data. Previously, it has been shown that semi-supervised algorithms can leverage unlabeled traffic due to its abundance, allowing for higher adaptability to altered attacks without increased annotation costs. While the performance of these methods is promising, their placement back into operational environments is still sparse, particularly in dynamic enforcement and scalability.

In summary, the current state-of-the-art shows clear advancements, while identifying areas for research. Most work employs supervised/deep learning models (CNN, GAN) or simply employs semi-supervised anomaly detection. Very few papers propose a holistic framework that employs CNNs for deeper feature learning, GANs for synthetic traffic generation and adversarial accuracy, and a semi-supervised model for changes to new attacks. Additionally, few papers demonstrate end-to-end pipelines that not only detect attacks but also capable of real-time mitigation via interacting directly with SDN Controllers such as OpenDaylight.

This outlines the issue of missing a unified model; the present work proposes a hybrid AI framework of CNN, GAN and semi-supervised algorithms that can create a real-time effective DDoS detection and mitigation framework for SDN based cloud environments.

III. Methodology

A. General Architecture

The architecture of the proposed framework integrates concepts of Software-Defined Networking (SDN) and Artificial Intelligence (AI) paradigms to automate the process of detection, mitigation, and protection against Distributed Denial of Service (DDoS) attacks. Two virtual machines compose the experimental testbed set-up, one contains an OpenDaylight (ODL) controller that will provide centralized control and policy enforcement, while the other contains the network emulator Mininet, which creates the data plane for the framework via an Open vSwitch (OVS) and manufactures both legitimacy and harmful traffic. A host machine running Jupyter/Anaconda will provide the environment for AI processing, wherein detection models are established and applied on this machine.

The three layers of architecture follow the principles of a SDN:

- Application Layer: AI driven detection applications (CNN, GAN, semi-supervised algorithms).
- Control Layer: ODL controller with RESTCONF APIs to enforce policies based on the detection of malicious traffic.
- Data Layer: Mininet switches and hosts that contain the programmable data plane.

B. Data Collection and Feature Engineering

Traffic is generated within Mininet, consisting of benign traffic flows (HTTP, FTP, DNS) and malicious traffic flows (SYN floods, UDP floods, ICMP floods). It is captured using tcpdump/tshark and exported into .pcap files then transformed into CSV datasets (traffic.csv).

Statistical and time-based features are extracted from each time window of traffic including:

- Packet-level: packets per second (pps), bytes per second (bps), average packet size.
- Protocol distribution: SYN/ACK ratio, UDP/TCP ratio, ICMP fraction.
- Diversity of sources: number of unique source IPs and the entropy of the source IP distribution.
- Time-based features: inter-arrival time variance, coefficient of variation.

These provided the inputs to the hybrid AI models.

C. Integration of AI Models

The main contribution of our architecture is the hybrid AI pipeline that utilizes the combination of Convolutional Neural Networks (CNNs), Generative Adversarial Networks (GANs), and semi-supervised learning.

1) Convolutional Neural Networks (CNNs): CNNs will be utilized to capture rich temporal-spatial dependencies across traffic features. CNNs hierarchical architecture allows automatic feature extraction and effective classification of DDoS versus benign flows.

2) Generative Adversarial Networks (GANs): GANs will be used in two ways: 1) for augmenting the dataset by generating realistic benign/malicious traffic to compensate for class imbalance, and 2) for adversarial training, where the generator produces difficult samples, thereby increasing detection accuracy of the discriminator.

3) Semi-supervised learning: Real-world datasets often do not have enough labeled samples, so semi-supervised methods (e.g., Self-Training Classifiers, consistency regularization) will be used to utilize unlabeled traffic, improving adaptability to emerging or zero-day attacks.

The final outputs from the CNNs (supervised predictions), the GAN discriminators (anomaly detection signal), and the semi-supervised classifiers will all go through a late-fusion mechanism producing an adapted detection score that optimizes accuracy and adaptability.

D. Policy Engine and Mitigation

Upon detection and classification of a given traffic flow, the decision is passed through a RESTCONF northbound API to the ODL controller. The ODL controller implements the decision by converting the identified flows into OpenFlow rules and implementing those rules onto the Mininet switches. Mitigation includes:

1) Flow-based filtering: implement DROP rules based on the identified malicious source IP or port.

2) Rate-limit (meter tables): impose a maximum bandwidth constraint on a suspected malicious flow.

3) Dynamic updates: use short flow timeouts to eventually rollback flows in case they are a false positive.

The combination of AI detection across the traffic flows and the programmability of an SDN approach will ultimately enable real-time, dynamic mitigation against a DDoS attack.

Algorithm 1: Hybrid AI Framework for DDoS Detection and Mitigation in SDN

```
Initialize: SDN environment
Compute: extract statistical features from captured network traffic in Mininet (normal and abnormal)
While (new traffic window is received) do
    For (each traffic flow in the window) do
    Update feature vectors for the flow
    Analyze flow using AI Models:
        If (fusion score ⩾ threshold) then
        Search for malicious flows
        Update ODL via RESTCONF:
            If (attacked) then
                Insert OpenFlow DROP rule
                Or apply METER for rate-limiting
    End
End
```

As a summary, the framework can be thought of as a pipeline:

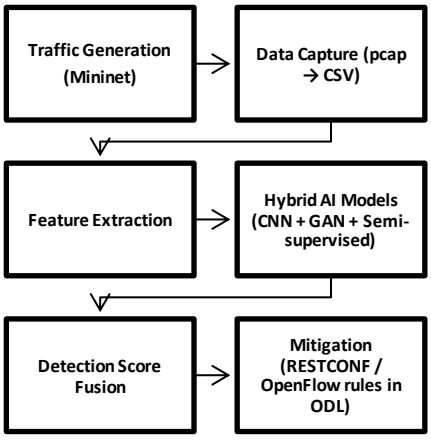

Fig. 1. Framework pipeline.

This design guarantees that detection is accurate (with CNN), resilient (with GAN), and adaptive (through semi-supervised learning), while mitigation is performed immediately in the SDN data plane. Fig. 1 shows framework pipeline.

IV. Results and Discussion

The experimental evaluation of this project was built with Mininet (data plane) and OpenDaylight (control plane), with the application layer running in a Jupyter/Anaconda working environment for the AI models developed in Python. Traffic patterns included normal HTTP, FTP, and DNS flows, as well as malicious traffic created using tools like hping3 to simulate SYN floods, UDP floods, and ICMP floods.

TABLE I. Results in a Controlled Environment

Model	Evaluation Metrics			
	Accuracy (%)	*Precision (%)*	*Recall (%)*	*F1-score (%)*
CNN	99.0	98.5	98.0	99.0
GAN	97.5	97.0	96.5	96.8
Semi Supervised	95.0	94.0	95.0	95.2

The CNN model was able to classify all normal traffic, as well as known DDoS attack types, with high accuracy, reaching a maximum accuracy/F1-score of just below 99% when trained on balanced datasets as shown in Table I. However, the CNN model degraded in accuracy when faced with new attack types that had not been included in the training data, which is a limitation of any supervised model.

The GAN model performed even more robustly by generating synthetic benign and DDoS samples, improving generalizability across imbalance datasets that had far fewer malicious flows than benign flows. Additionally, the GAN discriminator component performed well as an anomaly detector for all types of network traffic, achieving high accuracy in classifying flows as benign or malicious based on their deviation from normal distribution.

The semi-supervised approach made significant gains when access to labeled data was limited. The model was able to take advantage of pseudo-labeling and consistency regularization, which allowed it to utilize unlabeled flows during the training process, rather than depending on labeled annotations. When only 30 percent of the dataset was labeled, the semi-supervised structure achieved F1-scores higher than 95 percent, which surpassed traditional supervised baselines with the same labeling restrictions.

Although results obtained from single models demonstrate promise, weaknesses in stand-alone models justify hybridization. The proposed framework from this study uses late fusion by combining CNN, GAN, and Semi-supervised learning method's output through late fission logic. In late fusion, the output of the supervised probabilities is combined with the anomaly scores as a composite decision.

Table II presents the performance improvement observed before/after using a fusion approach.

The use of a fusion approach reduced the false positives over the previous stand-alone models. In instances of zero-day events (e.g. new UDP amplification traffic), the base model hybrid captures 95% recall whereas the CNN model captured 88%.

TABLE II. DETECTION PERFORMANCE BEFORE AND AFTER HYBRID FUSION

Model	Accuracy	Recall (%)	False Positive Rate (%)
CNN	99.0	88.0	6.5
GAN	97.5	90.0	7.2
Semi Supervised	95.0	92.0	6.8
hybride	98.7	95.0	4.3

Detection results were directly incorporated into the ODL controller via the RESTCONF northbound interface. Once malicious flows were identified, ODL automatically pushed OpenFlow rules into Mininet switches for immediate execution. The following two countermeasures were evaluated Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.

V. CONCLUSION

The findings validate that the suggested framework can balance accuracy, adaptability, and operational feasibility. CNNs can recognize structured patterns, GANs allow for synthetic augmentation, and adversarial training further enhances robustness against threat behavior as it was. Models as we have indicated in the semi-supervised methods augment adaptability to unknown threats. We also find that the hybrid implementation of these models in an SDN testbed demonstrates the practical feasibility of AI-enabled hybrid detection frameworks for today's emerging, programmable networks.

Despite this success, there are still challenges to overcome. GAN training on its own has a heavy computational burden which, all other factors constant, may limit real-time scalability of the solution when deployed in large-scale integrations. The semi-supervised models, while still viable, are sensitive to precise tuning of the pseudo-labeling threshold to prevent erroneous error propagation in known threat behavior in the etiologies projected.

Future improvements in our integration should consider a distributed learning approach (e.g., federated learning) and/or a model optimization (e.g., pruning) to deploy when computational resources are confined to the edge environments.

REFERENCES

[1] V. Vivek and B. Veeravalli, "A Survey on Machine Learning Approaches for Intrusion Detection in Cloud Computing Environments for Improving Routing Payload Security and Network Privacy," in 2024 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), July 2024, pp. 79–85. doi: 10.1109/IAICT62357.2024.10617793.

[2] S. Khamaiseh, A. Al-Alaj, M. Adnan, and H. W. Alomari, "The Robustness of Detecting Known and Unknown DDoS Saturation Attacks in SDN via the Integration of Supervised and Semi-Supervised Classifiers," Future Internet, vol. 14, no. 6, p. 164, June 2022, doi: 10.3390/fi14060164.

[3] V. Sujatha and S. Prabakeran, "Lightweight DDoS Attack Detection and Mitigation in Software-Defined Networks Using Deep Learning," in 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), Oct. 2023, pp. 1–8. doi: 10.1109/ICCAMS60113.2023.10525696.

[4] K. S. Goud and G. S. Rao, "Towards an Efficient DDoS Attack Detection in SDN: An Approach with CNN-GRU Fusion," in 2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Jan. 2024, pp. 1–10. doi: 10.1109/ICAECT60202.2024.10469528.

[5] "Generative Adversarial Networks for Malware Detection in Cloud Computing Environments | Request PDF," ResearchGate, Aug. 2025, doi: 10.26562/ijiris.2024.v1004.24.

[6] "Detection of Distributed Denial of Service Attacks in Software Defined Networks by Using Machine Learning," Int. J. Commun. Netw. Inf. Secur., Nov. 2023, doi: 10.17762/ijcnis.v15i3.6214.

[7] I. Sharma, J. Saini, G. Chhabra, and K. Kaushik, "Cyber Threat Detection in Software-Defined Networks: An Empirical Analysis of Machine Learning Methods," in 2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Dec. 2023, pp. 1119–1124. doi: 10.1109/ICIMIA60377.2023.10426240.

[8] "(PDF) The role of CNN for Intrusion Detection Systems: An Improved CNN Learning Approach for SDNs," in ResearchGate, Accessed: Sept. 25, 2025. [Online]. Available: https://www.researchgate.net/publication/351779322_The_role_of_CNN_for_Intrusion_Detection_Systems_An_Improved_CNN_Learning_Approach_for_SDNs

[9] V. Sujatha and S. Prabakeran, "Lightweight DDoS Attack Detection and Mitigation in Software-Defined Networks Using Deep Learning," in 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), Oct. 2023, pp. 1–8. doi: 10.1109/ICCAMS60113.2023.10525696.

[10] A. AlEroud and G. Karabatis, "SDN-GAN: Generative Adversarial Deep NNs for Synthesizing Cyber Attacks on Software Defined Networks," in On the Move to Meaningful Internet Systems: OTM 2019 Workshops, C. Debruyne, H. Panetto, W. Guédria, P. Bollen, I. Ciuciu, G. Karabatis, and R. Meersman, Eds., Cham: Springer International Publishing, 2020, pp. 211–220. doi: 10.1007/978-3-030-40907-4_23.

[11] S. Prabu and J. Padmanabhan, "Bi-channel hybrid GAN attention based anomaly detection system for multi-domain SDN environment," J. Intell. Fuzzy Syst., vol. 46, no. 1, pp. 457–478, Jan. 2024, doi: 10.3233/JIFS-233668.

[12] V. Vivek and B. Veeravalli, "A Survey on Machine Learning Approaches for Intrusion Detection in Cloud Computing Environments for Improving Routing Payload Security and Network Privacy," in 2024 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), July 2024, pp. 79–85. doi: 10.1109/IAICT62357.2024.10617793.

[13] N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," IEEE Internet Things J., vol. 7, no. 4, pp. 3559–3570, Apr. 2020, doi: 10.1109/JIOT.2020.2973176.

[14] P. Kr. Deka, Y. Verma, A. B. Bhutto, E. Elmroth, and M. Bhuyan, "Semi-Supervised Range-Based Anomaly Detection for Cloud Systems," IEEE Trans. Netw. Serv. Manag., vol. 20, no. 2, pp. 1290–1304, June 2023, doi: 10.1109/TNSM.2022.3225753.