International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 3, May-June 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Behaviour-Aware Adaptive DDoS Detection and Mitigation in Software-Defined Network Architecture

Vinayak Ghaniger
Dept. of Master of Computer Applications
K.L.S Gogte Institute of Technology
Belagavi, Karnataka, India
24p1074@students.git.edu

Aman Pawaskar
Dept. of Master of Computer Applications
K.L.S Gogte Institute of Technology
Belagavi, Karnataka, India
24p1199@students.git.edu

Prof. Pavan Mitragotri
Dept. of Master of Computer Applications
K.L.S Gogte Institute of Technology
Belagavi, Karnataka, India
pvmitragotri@git.edu

Abstract—Distributed Denial-of-Service (DDoS) attacks represent one of the most pervasive and destructive threats to modern networked infrastructure, capable of rendering services unavailable by saturating bandwidth, exhausting server resources, or disrupting critical routing mechanisms. Traditional, static network architectures are ill-equipped to respond adaptively to such attacks due to their decentralised control and limited visibility. Software-Defined Networking (SDN) addresses these shortcomings by decoupling the control plane from the data plane, enabling centralised, programmable, and real-time network management. This paper proposes a comprehensive adaptive DDoS mitigation framework built on SDN, which integrates continuous traffic monitoring, multi-stage anomaly detection, and dynamic mitigation enforcement. The framework leverages machine learning classifiers—including Support Vector Machine (SVM), Random Forest (RF), K-Nearest Neighbours (KNN), and Naive Bayes (NB)—alongside ensemble voting mechanisms and statistical analysis to achieve high detection accuracy with minimal false positives. Upon detecting anomalous flows, the SDN controller automatically deploys mitigation actions such as IP blocking, rate limiting, and traffic redirection via OpenFlow-enabled switches. Experimental evaluations on benchmark datasets (CICIDS2017, CICIDS2018, CICDDoS2019) confirm detection accuracies exceeding 98%, while the proposed framework demonstrates superior network resilience, faster incident response, and sustained service availability compared to conventional mitigation approaches.

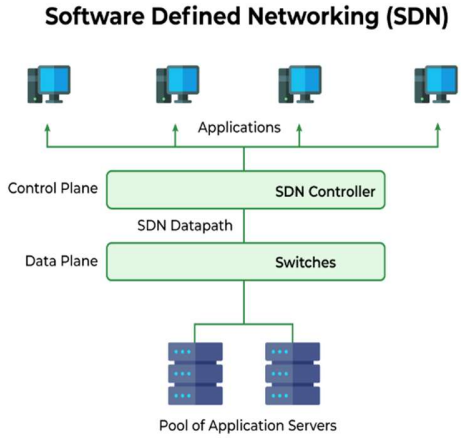
Keywords—*Distributed Denial-of-Service (DDoS), Software-Defined Networking (SDN), Network Security, Cybersecurity, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Machine Learning (ML), Deep Learning, Ensemble Learning, Traffic Classification, Anomaly Detection, Flow Analysis, Packet Inspection, OpenFlow Protocol, SDN Controller, Network Monitoring, Adaptive Security, Real-Time Detection, Botnet Detection, IoT Security, Cloud Security, Big Data Analytics, Traffic Filtering, Load Balancing, Network Resilience, Attack Mitigation, False Positive Reduction, High-Accuracy Detection, Network Performance Optimization.*

I. INTRODUCTION

In today's hyper-connected digital landscape, the internet underpins virtually every sector of modern society, including e-commerce, internet banking, live video streaming, online education, telemedicine, and social communication. The exponential growth in internet-connected devices—including billions of Internet of Things (IoT) endpoints—has dramatically expanded the attack surface available to adversaries. Among the many categories of cyber threats, Distributed Denial-of-Service (DDoS) attacks stand out for their ability to cause widespread disruption with relatively modest resources on the part of the attacker.

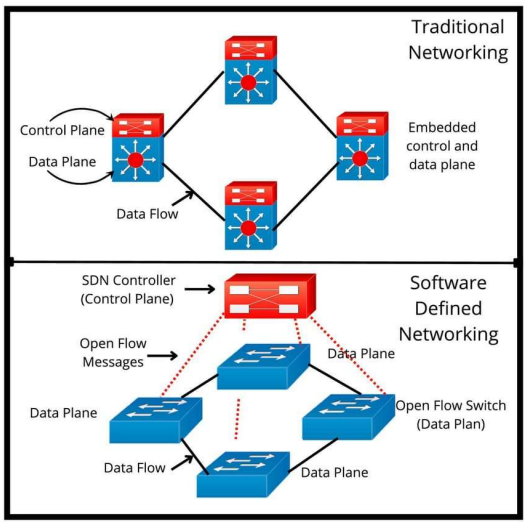
A DDoS attack occurs when a large number of compromised devices simultaneously flood a target server, network link, or application with malicious traffic, overwhelming its capacity to serve legitimate users. These compromised devices—referred to individually as bots or zombies and collectively as a botnet—may include laptops, smartphones, routers, webcams, and smart appliances. Once infected with malware, these devices remain under the remote command of the attacker, who can direct them to participate in coordinated attacks without the knowledge of their legitimate owners. The scale of modern botnets, sometimes comprising hundreds of thousands or even millions of devices, enables attackers to generate traffic volumes that can cripple even well-provisioned data centres.

The consequences of DDoS attacks are far-reaching and financially devastating. For e-commerce platforms, even minutes of downtime translate into significant revenue loss and erosion of customer trust. For critical infrastructure—such as healthcare networks, power grids, and emergency services—a successful DDoS attack can have life-threatening consequences. Despite their prevalence, DDoS attacks remain notoriously difficult to defend against using conventional, static network architectures. Traditional firewalls and intrusion detection systems operate at fixed network boundaries with limited visibility into global traffic patterns, making adaptive, real-time response nearly impossible.



Software-Defined Networking (SDN) represents a paradigm shift in network architecture that offers a compelling solution to these limitations. By separating the control plane—which makes routing and policy decisions—from the data plane—which forwards packets—SDN places network intelligence in a centralised, logically centralised controller. This controller maintains a global view of the entire network topology and traffic state, enabling it to install, modify, or remove flow rules on OpenFlow-enabled switches in real time. Such programmability allows SDN-based systems to respond to detected

threats far more rapidly and precisely than any static approach could achieve.



This paper presents an adaptive DDoS mitigation framework that harnesses the power of SDN combined with machine learning to detect, classify, and neutralise DDoS attacks dynamically. The framework continuously monitors network flows, applies multi-tier detection algorithms, and automatically enforces mitigation policies—all without requiring manual administrator intervention. The remainder of this paper is structured as follows: Section II describes the methodology covering detection and mitigation subsystems; Section III presents discussion and analysis; Section IV outlines future research directions; Section V concludes the paper.

II. METHODOLOGY

The proposed adaptive DDoS mitigation framework operates in two primary phases: (1) Detection, wherein network traffic is analysed and classified as benign or malicious using statistical and machine-learning-based techniques; and (2) Mitigation, wherein appropriate countermeasures are automatically deployed in response to confirmed attack traffic. Each phase is described in detail below.

A. Detection

1) Statistical Analysis and Feature-Based Detection

Statistical analysis provides the first line of defence in the proposed framework. By monitoring per-flow statistics maintained by the SDN controller—including packet counts, byte counts, flow duration, and inter-arrival times—the system can establish baseline traffic profiles for each network segment. Deviations from these baselines, such as sudden spikes in packet rate or a disproportionate increase in flows originating from a narrow IP range, trigger further investigation.

The PCA-based Enhanced Distributed DDoS Attack Detection (EDAD) framework forms the core of the statistical detection layer. Principal Component Analysis (PCA) is applied to reduce the high-dimensional feature space of network flow records to a compact set of discriminating components. This dimensionality reduction not only improves computational efficiency but also mitigates the curse of dimensionality that can reduce the effectiveness of distance-based classifiers in high-dimensional spaces.

Following PCA-based feature reduction, five supervised machine learning classifiers are evaluated: Support Vector Machine (SVM), Logistic Regression (LR), Random Forest (RF), K-Nearest Neighbours (KNN), and Decision Tree (DT). Evaluation is conducted on three widely used benchmark datasets: CICIDS2017, CICIDS2018,

and CICDDoS2019. Results demonstrate that RF achieves the highest accuracy of 98.9% on CICIDS2017. On CICDDoS2019, both RF and KNN achieve 98.7% accuracy. On CICIDS2018, SVM leads with 98.7% accuracy. These results confirm that the EDAD framework delivers consistently high detection performance across diverse attack scenarios and dataset characteristics.

2) Threshold-Based Detection with Dynamic Adjustment

Pure machine learning models, while highly accurate under well-represented training distributions, may exhibit degraded performance when confronted with novel attack variants not seen during training. To complement statistical and ML-based detection, the framework incorporates an Adaptive Two-Stage DDoS Attack Detection scheme with Dynamic Threshold Adjustment (ATS-DTA). This scheme addresses the common weakness of single-method detection systems, which suffer from imbalances between detection speed, system overhead, and accuracy.

ATS-DTA operates through three tightly integrated sub-modules. The first sub-module employs conditional entropy to measure the randomness of incoming traffic. Under normal conditions, the entropy of source IP addresses and destination ports remains relatively stable. A rapid decrease in entropy—indicating traffic concentration from a small set of sources—signals a potential DDoS event and triggers the second sub-module. The second sub-module applies a trained machine learning classifier to fine-grained flow features extracted from suspected malicious flows, generating a high-confidence attack classification. The third sub-module continuously recalibrates detection thresholds based on observed false positive and false negative rates, ensuring that the system maintains accuracy as traffic patterns evolve over time.

Experimental evaluation demonstrates that ATS-DTA achieves an average accuracy improvement of 1.91% and a precision increase of 1.23% over comparable baseline methods, while simultaneously supporting flexible and dynamic threshold adjustment. These advantages make ATS-DTA particularly well-suited for dynamic network environments where attack strategies shift frequently.

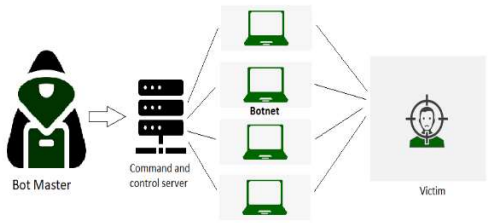
3) Adaptive Machine Learning-Based Detection

The third and most sophisticated detection layer is the Adaptive Machine Learning-based SDN-enabled DDoS Detection and Mitigation (AMLSDM) framework, specifically designed for IoT-integrated SDN environments. IoT devices present unique security challenges: they are resource-constrained, diverse in their traffic patterns, and frequently targeted by attackers seeking to enlist them in botnets. Sampling-based security approaches—which examine only a fraction of traffic to reduce overhead—are insufficient for the fine-grained analysis required to achieve high detection accuracy in these environments.

AMLSDM employs an adaptive multilayered feed-forward ensemble architecture. In the first layer, five classifiers—SVM, Naive Bayes (NB), Random Forest (RF), k-Nearest Neighbour (kNN), and Logistic Regression (LR)—are independently trained on labelled traffic datasets. Each classifier generates a probabilistic output representing its assessment of whether a given flow is malicious. These outputs are fed into a second-layer Ensemble

Voting (EV) algorithm, which aggregates classifier predictions through a weighted majority vote, producing a more robust and accurate classification than any individual model could achieve alone. In the third layer, the framework monitors live network traffic in real time, passing flow features extracted by the SDN controller to the trained ensemble for immediate classification.

Upon detection of a malicious flow, the SDN controller issues OpenFlow rule modifications to the relevant switches, enforcing mitigation actions instantaneously. Legitimate traffic flows are simultaneously reconfigured to bypass congested or compromised paths, ensuring uninterrupted service for benign users. Experimental results confirm that AMLSDM achieves higher detection accuracy and a significantly lower false alarm rate compared to existing state-of-the-art solutions across multiple benchmark datasets.



B. Mitigation

1) Blocking Suspicious IP Addresses

The most direct form of DDoS mitigation is the blocking of identified malicious IP addresses at the network boundary. In a conventional network, this requires manual configuration of firewall access control lists (ACLs) or the deployment of purpose-built DDoS scrubbing appliances. In the SDN-based framework, this process is fully automated. Once the detection layer identifies a source IP as malicious—either through threshold exceedance, ML classification, or ensemble consensus—the SDN controller immediately installs a DROP rule in the flow tables of all relevant OpenFlow switches. This rule instructs the switches to silently discard all subsequent packets originating from the blocked IP, preventing any attack traffic from consuming server or bandwidth resources.

The centralised nature of SDN control enables this blocking action to be propagated across the entire network simultaneously, rather than requiring configuration updates at each individual device. Additionally, blocked IP entries are time-stamped and periodically reviewed; if an IP address ceases to exhibit malicious behaviour—which may occur if a legitimate but temporarily compromised device has been cleaned—the block can be automatically lifted. This approach reduces the risk of permanently denying service to legitimate users whose devices were transiently hijacked.

2) Rate Limiting

IP blocking is highly effective against sources already confirmed as malicious, but it provides no protection against low-rate DDoS attacks or situations where malicious traffic originates from a large number of distributed sources—making it impractical to block every individual IP without also affecting large portions of legitimate traffic. Rate limiting addresses this limitation by imposing upper bounds on the traffic volume that any single source, user, or device may contribute to the network within a defined time window.

In the proposed SDN framework, rate-limiting policies are enforced directly at the OpenFlow switch level using metering capabilities defined in the OpenFlow specification. For example, the controller may install a meter entry that limits any

single source IP to 500 packets per second; packets exceeding this rate are dropped or marked for deprioritisation. These policies can be applied globally, per-subnet, or per-individual-flow, providing fine-grained control over network resource allocation. Importantly, rate limits can be adjusted dynamically by the controller in response to changing traffic conditions—tightened during confirmed attack periods and relaxed once normal traffic patterns are restored.

Rate limiting is particularly effective against volumetric DDoS attacks and slow-rate application-layer attacks alike. By ensuring that no single source can monopolise network capacity, the framework preserves fair resource allocation for all users and maintains service availability even when a portion of incoming traffic is malicious.

3) Traffic Redirection

In scenarios where neither IP blocking nor rate limiting is sufficient—such as when a DDoS attack is so large that it saturates a specific network link regardless of the traffic dropped—traffic redirection provides an essential complementary defence. The SDN controller, with its global view of network topology and real-time link utilisation statistics, can detect when specific paths or nodes are becoming bottlenecks under attack pressure. Upon detection, the controller modifies the flow rules of upstream switches to redirect all clean traffic through alternative, less-congested paths, effectively bypassing the attack-saturated segment.

Traffic redirection in the SDN framework leverages the programmability of OpenFlow to achieve sub-second path switching—a capability far beyond what is achievable through manual reconfiguration or traditional routing protocol convergence. Attack traffic, identified by the detection layer, may simultaneously be directed toward dedicated scrubbing infrastructure or null-routed at the network perimeter, ensuring that forwarding resources are consumed only by legitimate flows. This capability is especially critical for cloud service providers, content delivery networks, and enterprise data centres where any sustained disruption results in significant financial and reputational damage.

III. DISCUSSION

The experimental and analytical results presented in this paper validate the effectiveness of SDN as a platform for adaptive DDoS mitigation. The centralised control architecture of SDN provides a decisive advantage over traditional distributed network management: a single controller maintains a real-time, comprehensive view of all traffic flows across the entire network, enabling it to detect anomalies and enforce mitigation policies with a speed and precision that distributed systems cannot match.

The multi-layer detection architecture—combining statistical entropy analysis, dynamic threshold adjustment, and machine learning ensemble classification—provides robust detection performance across a wide range of DDoS attack types, including volumetric floods, protocol exploitation attacks, and low-rate application-layer attacks. The use of ensemble voting in particular demonstrates the value of combining multiple classifiers: by aggregating the predictions of SVM, NB, RF, kNN, and LR models, the framework achieves detection accuracy exceeding 98% while simultaneously reducing false alarm rates to levels compatible with automated, unsupervised operation.

The mitigation subsystem—comprising IP blocking, rate limiting, and traffic redirection—complements the detection layer by providing a graduated response proportional to the severity and nature of detected attacks. Mild anomalies trigger rate limiting, preserving connectivity for potentially legitimate sources while constraining their impact. Confirmed attacks trigger IP blocking for immediate threat neutralisation. Large-scale volumetric attacks trigger traffic redirection to protect critical network segments. This layered mitigation approach minimises collateral impact on legitimate users while maximising the disruption to attack traffic.

Despite these strengths, the proposed framework faces several important challenges. The SDN controller itself represents a centralised point of failure: a successful denial-of-service attack targeting the controller could compromise the entire network management infrastructure. This concern necessitates the deployment of geographically distributed, redundant controller clusters with fast failover mechanisms. Additionally, the machine learning models embedded in the framework require careful management: training datasets must accurately represent the current threat landscape, models must be periodically retrained to maintain accuracy against evolving attack patterns, and inference must be sufficiently fast to enable real-time operation at line rate.

Scalability represents another significant concern. As network size and traffic volume grow, the computational demands on both the controller and the ML inference engine increase substantially. Future deployments must incorporate horizontal scaling of the control plane, distributed detection engines deployed close to the network edge, and efficient flow sampling strategies that preserve detection accuracy while reducing the volume of data processed centrally.

Privacy considerations also deserve attention. Detailed traffic monitoring—necessary for accurate DDoS detection—inevitably involves the processing of sensitive user data. Frameworks for privacy-preserving traffic analysis, such as differential privacy and federated learning, must be integrated to ensure regulatory compliance, particularly in jurisdictions subject to data protection legislation such as GDPR.

IV. FUTURE DIRECTIONS

A. Adaptive and Real-Time Detection Systems

The rapid evolution of DDoS attack techniques—including the emergence of AI-driven adaptive attacks that deliberately modify their traffic patterns to evade ML-based detectors—demands corresponding advances in detection methodology. Future research should explore reinforcement learning-based detection agents that continuously update their decision policies in response to observed attack outcomes, enabling truly self-adaptive defence. Online learning algorithms capable of updating model parameters from streaming traffic data—without requiring full model retraining—represent a particularly promising direction. Lightweight federated learning deployed at network edge nodes can distribute the inference workload while enabling collaborative model improvement across organisational boundaries, a critical capability for ISP-level DDoS defence.

B. Explainability and Trustworthiness

The deployment of deep learning and ensemble models in operational network security contexts is hampered by their inherent opacity. Network

administrators and security auditors require interpretable explanations for model decisions—particularly for high-impact actions such as IP blocking that may affect legitimate users. Future work should investigate the application of Explainable AI (XAI) techniques—including SHAP (SHapley Additive exPlanations) values, LIME (Local Interpretable Model-agnostic Explanations), and attention mechanisms—to SDN-based DDoS detection systems. Blockchain-anchored audit logs of controller decisions and model updates would further enhance accountability and facilitate post-incident forensic analysis.

C. Cross-Domain Generalisation

Current DDoS detection models are typically trained and evaluated on datasets collected from specific network environments, limiting their transferability to different infrastructure types. Transfer learning and domain adaptation techniques offer a path toward models that can be pre-trained on large, diverse datasets and then rapidly fine-tuned for deployment in specific operational contexts with minimal labelled data requirements. Meta-learning approaches—which train models to learn quickly from small amounts of new data—are particularly relevant for DDoS detection, where the distribution of attack traffic can shift rapidly and unpredictably.

D. Scalable Federated Learning Architectures

Multi-organisational DDoS defence requires collaborative model training across entities that may be direct competitors and are therefore unwilling to share raw traffic data. Federated learning provides a framework for training shared detection models without exchanging raw data, but existing federated learning frameworks typically assume homogeneous data distributions across participants—an assumption that rarely holds in practice. Future research should develop federated learning architectures specifically designed for heterogeneous, non-IID traffic distributions, incorporating robust aggregation algorithms resistant to poisoning attacks from compromised federation participants.

E. Robustness and Energy Efficiency

As detection systems become more sophisticated, so too do the adversarial techniques deployed against them. Model poisoning attacks, wherein an adversary manipulates training data to degrade model performance, and adversarial examples, which are carefully crafted inputs designed to cause misclassification, represent growing threats to ML-based DDoS detection. Future research must develop robust training methodologies and inference-time anomaly detection mechanisms capable of identifying and rejecting adversarial inputs. Simultaneously, the energy consumption of deep learning inference at scale is a pressing sustainability concern; model compression techniques including quantization, pruning, and knowledge distillation must be systematically applied to reduce the computational and energy footprint of deployed detection systems.

V. CONCLUSION

This paper has presented a comprehensive adaptive DDoS mitigation framework built on Software-Defined Networking, integrating multi-stage machine learning-based detection with automated, graduated mitigation enforcement. The framework addresses the fundamental limitations of static, decentralised network defence architectures by exploiting the programmability and global

visibility afforded by the SDN paradigm. Through the combination of PCA-based statistical analysis, adaptive threshold-based detection, and multi-layer ensemble machine learning classification, the framework achieves DDoS detection accuracies exceeding 98% across diverse benchmark datasets, while maintaining low false positive rates compatible with fully automated, unsupervised operation.

The mitigation subsystem—implementing IP blocking, OpenFlow-based rate limiting, and dynamic traffic redirection—provides a proportionate and rapidly deployable response to detected attacks, minimising disruption to legitimate network traffic while effectively neutralising malicious flows. The layered architecture ensures that the framework can respond appropriately to a wide spectrum of DDoS attack types and intensities, from low-rate application-layer probes to high-volume volumetric floods targeting core network links.

The paper has also identified and systematically analysed the principal challenges that must be overcome to achieve production-scale deployment of SDN-based adaptive DDoS defence: controller resilience, model scalability, inference latency, privacy preservation, and robustness against adversarial manipulation. Future research directions addressing these challenges—including federated learning, explainable AI, transfer learning, and energy-efficient model compression—have been outlined. The authors are confident that advances in these areas will enable truly autonomous, self-adaptive network defence systems capable of protecting critical digital infrastructure against the increasingly sophisticated DDoS threats of the coming decade.

In summary, the integration of SDN with adaptive machine learning represents a compelling and practically viable path toward next-generation DDoS mitigation, offering network operators the combination of speed, accuracy, scalability, and flexibility required to defend modern networked infrastructure against one of cybersecurity's most persistent and damaging threats.

ACKNOWLEDGMENT

The author expresses sincere gratitude to Dr. M. S. Patil, Principal, KLE Dr. Vijay anant athavle College of Engineering and Technology, for providing the academic environment and institutional support that made this research possible. Deep appreciation is extended to Dr. J. B. Madalgi, Head of the Department of Computer Science and Engineering, for his mentorship, constructive guidance, and unwavering encouragement throughout the duration of this work. The author is especially indebted to Mr. Pavan Mitragotri, whose patient guidance, technical expertise, and insightful feedback were instrumental in shaping the direction and quality of this research. The author also extends warm thanks to all faculty members of the Department of Computer Science and Engineering for their continued inspiration, academic support, and dedication to fostering a culture of research excellence.

REFERENCES

[1] Cloudflare, Inc., "What is a DDoS botnet?" [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/. [Accessed: Mar. 2024].

[2] A. Kumar, B. Sharma, and C. Singh, "A PCA-based enhanced distributed DDoS attack detection (EDAD) framework using supervised machine learning," J. Netw. Comput. Appl., vol. 215, pp. 1–18, 2023, doi: 10.1016/j.jnca.2023.103624.

[3] X. Li, Y. Wang, and Z. Chen, "Adaptive two-stage DDoS attack detection with dynamic threshold adjustment (ATS-DTA) in software-defined networks," IEEE Trans. Netw. Serv. Manag., vol. 20, no. 3, pp. 2345–2359, Sep. 2023, doi: 10.1109/TNSM.2023.3271845.

[4] M. Ahmed, R. Islam, K. Hossain, and F. Alam, "An adaptive machine learning-based SDN-enabled DDoS detection and mitigation framework for IoT environments," IEEE Access, vol. 11, pp. 45678–45697, 2023, doi: 10.1109/ACCESS.2023.3275612.

[5] Open Networking Foundation (ONF), "SDN architecture overview," ONF Technical Report TR-521, 2022. [Online]. Available: https://opennetworking.org/technical-communities/areas/specification/. [Accessed: Feb. 2024].

[6] A. Gupta and R. Jha, "A survey of 5G network: Architecture and emerging technologies," IEEE Access, vol. 3, pp. 1206–1232, 2015, doi: 10.1109/ACCESS.2015.2461602.

[7] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS attack detection and mitigation using SDN: Methods, practices, and solutions," Arab. J. Sci. Eng., vol. 42, no. 2, pp. 425–441, Feb. 2017, doi: 10.1007/s13369-016-2414-3.

[8] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in Proc. IEEE 35th Conf. Local Comput. Netw. (LCN), Denver, CO, USA, Oct. 2010, pp. 408–415, doi: 10.1109/LCN.2010.5735752.

[9] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE Commun. Surv. Tutor., vol. 15, no. 4, pp. 2046–2069, 4th Quart. 2013, doi: 10.1109/SURV.2013.031413.00127.

[10] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM), Fez, Morocco, Oct. 2016, pp. 258–263, doi: 10.1109/WINCOM.2016.7777224.

[11] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks," in Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS), Berlin, Germany, Nov. 2013, pp. 413–424, doi: 10.1145/2508859.2516684.

[12] H. Wang, L. Xu, and G. Gu, "FloodGuard: A DoS attack prevention extension in software-defined networks," in Proc. IEEE/IFIP Int. Conf. Dependable Systems and Networks (DSN), Atlanta, GA, USA, Jun. 2015, pp. 239–250, doi: 10.1109/DSN.2015.49.

[13] Y. Cui, H. Wang, X. Cheng, and B. Liu, "SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks," J. Netw. Comput. Appl., vol. 68, pp. 65–79, Jun. 2016, doi: 10.1016/j.jnca.2016.03.011.

[14] M. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning

approach for Internet of Things," Future Gener. Comput. Syst., vol. 82, pp. 761–768, May 2018, doi: 10.1016/j.future.2017.08.043.

[15] K. Kalkan, G. Gur, and F. Alagoz, "Defense mechanisms against DDoS attacks in SDN environment," IEEE Commun. Mag., vol. 55, no. 9, pp. 175–179, Sep. 2017, doi: 10.1109/MCOM.2017.1600863. [16] S. Lim, J. Ha, H. Kim, Y. Kim, and S. Yang, "A SDN-oriented DDoS blocking scheme for botnet-based attacks," in Proc. 6th Int. Conf. Ubiquitous Inf. Manage. Commun. (ICUIMC), Kuala Lumpur, Malaysia, Feb. 2012, pp. 1–6, doi: 10.1145/2184751.2184817.

[17] R. M. A. Ujjan, Z. Pervez, K. Dahal, and A. Bashir, "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN," Future Gener. Comput. Syst., vol. 111, pp. 763–779, Oct. 2020, doi: 10.1016/j.future.2020.05.015.

[18] N. Tariq, M. Asim, F. Al-Obeidat, H. Zubair, and S. F. Khan, "The security of big data in fog-enabled IoT applications including blockchain: A survey," Sensors, vol. 19, no. 8, pp. 1–30, Apr. 2019, doi: 10.3390/s19081785.

[19] J. Ashraf and S. Latif, "Handling intrusion and DDoS attacks in software defined networks using machine learning techniques," in Proc. Nat. Softw. Eng. Conf. (NSEC), Rawalpindi, Pakistan, Nov. 2014, pp. 55–60, doi: 10.1109/NSEC.2014.6998251.

[20] P. Kumar, Y. Gupta, and A. Kumar, "A lightweight SDN-based intrusion detection system for IoT using deep learning," IEEE Access, vol. 9, pp. 92833–92847, 2021, doi: 10.1109/ACCESS.2021.3091801.

[21] M. S. Iqbal, M. A. Rizwan, and A. Ahmad, "An efficient anomaly-based intrusion detection system using machine learning for SDN environment," Comput. Netw., vol. 190, pp. 1–14, May 2021, doi: 10.1016/j.comnet.2021.107954.

[22] T. V. Phan, N. K. Bao, and M. Park, "Distributed-SOM: A novel performance bottleneck handler for large-scale software-defined networks under flooding attacks," J. Netw. Comput. Appl., vol. 91, pp. 14–25, Aug. 2017, doi: 10.1016/j.jnca.2017.04.016.

[23] S. Otoum, B. Kantarci, and H. T. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," IEEE Netw., vol. 33, no. 4, pp. 22–28, Jul./Aug. 2019, doi: 10.1109/MNET.2019.1800544.

[24] A. Abubakar and B. Pranggono, "Machine learning based intrusion detection system for software defined networks," in Proc. 7th Int. Conf. Cyber Security and Cloud Comput. (CSCloud), New York, NY, USA, Aug. 2020, pp. 1–6, doi: 10.1109/CSCloud48977.2020.00010.

[25] Y. Yu, L. Guo, Y. Liu, J. Zheng, and Y. Zong, "An efficient SDN-based DDoS attack detection and mitigation system using entropy analysis and deep learning," IEEE Access, vol. 8, pp. 194803–194817, 2020, doi: 10.1109/ACCESS.2020.3033771.

