IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 5 January 2024, accepted 24 January 2024, date of publication 31 January 2024, date of current version 7 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3360868

SURVEY

Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks—Current Research Solutions

NURA SHIFA MUSA[1,2], NADA MASOOD MIRZA[3], SAIDA HAFSA RAFIQUE[1], AMIRA MAHAMAT ABDALLAH[1], AND THANGAVEL MURUGAN[4], (Senior Member, IEEE)

[1] College of Information Technology, United Arab Emirates University, Al Ain, Abu Dhabi, United Arab Emirates
[2] College of Engineering, Al Ain University, Al Ain, Abu Dhabi, United Arab Emirates
[3] College of Engineering, United Arab Emirates University, Al Ain, Abu Dhabi, United Arab Emirates
[4] Department of Information Systems and Security, College of Information Technology, United Arab Emirates University, Al Ain, Abu Dhabi, United Arab Emirates

Corresponding author: Thangavel Murugan (thangavelm@uaeu.ac.ae)

This work was supported in part by the United Arab Emirates University under Research Start-Up Proposal Grant G00004612/12T048.

ABSTRACT This state-of-the-art review comprehensively examines the landscape of Distributed Denial of Service (DDoS) anomaly detection in Software Defined Networks (SDNs) through the lens of advanced Machine Learning (ML) and Deep Learning (DL) techniques. The application domain of this work is focused on addressing the inherent security vulnerabilities of SDN environments and developing an automated system for detecting and mitigating network attacks. The problem focused on in this review is the need for effective defensive mechanisms and detection methodologies to address these vulnerabilities. Conventional network measurement methodologies are limited in the context of SDNs, and the proposed ML and DL techniques aim to overcome these limitations by providing more accurate and efficient detection and mitigation of DDoS attacks. The objective of this work is to provide a comprehensive review of related works in the field of SDN anomaly detection recent advances, categorized into two groups via ML and DL techniques. The proposed systems utilize a variety of techniques, including Supervised Learning (SL), Unsupervised Learning (UL) Ensemble Learning (EL) and DL solutions, to process IP flows, profile network traffic, and identify attacks. The output comprises the mitigation policies learned by ML/DL techniques, and the proposed systems act as sophisticated gatekeepers, applying automated mitigation policies to curtail the extent of damage resulting from these attacks. The results obtained from the evaluation metrics, including accuracy, precision, and recall, confirm the marked effectiveness of the proposed systems in detecting and mitigating various types of attacks, including Distributed Denial of Service (DDoS) attacks. The proposed systems' foundational contributions are manifest in their efficacy for both DDoS attack detection and defense within the SDN environment. However, the review acknowledges certain inherent limitations and the pressing need for further validation within real-world scenarios to assess the proposed methods' practicality and effectiveness. In summary, this systematic review offers valuable perspectives on the present status of Distributed Denial-of-Service detection in Software-Defined Networks employing Machine Learning and Deep Learning methodologies, highlighting the strengths and limitations of various proposed systems and identifying areas for future research and development.

INDEX TERMS Anomaly detection, deep learning (DL), distributed denial of service (DDoS), machine learning (ML), software defined network (SDN).

The associate editor coordinating the review of this manuscript and approving it for publication was Tyson Brooks.

I. INTRODUCTION

The emergence of Software Defined Networks (SDNs) has revolutionized the way networks are managed and operated.

SDNs provide a flexible and programmable network infrastructure that enables network administrators to manage and control network traffic more efficiently. However, this flexibility comes at a cost, as SDNs are inherently vulnerable to various types of attacks; including (DDoS) attacks (see Figure 1). The application domain of this research is focused on addressing the inherent security vulnerabilities of SDN environments and developing an automated system for detecting and mitigating network attacks [25]. The proposed system functions by deploying a detection module and a mitigation module, both integrated into the controller for seamless logical communication. The system ingests network traffic data as input, subsequently subjecting it to a multi-step process involving anomaly detection and traceback mitigation. The results obtained from the evaluation metrics demonstrate high detection accuracy and efficient DDoS attack mitigation.

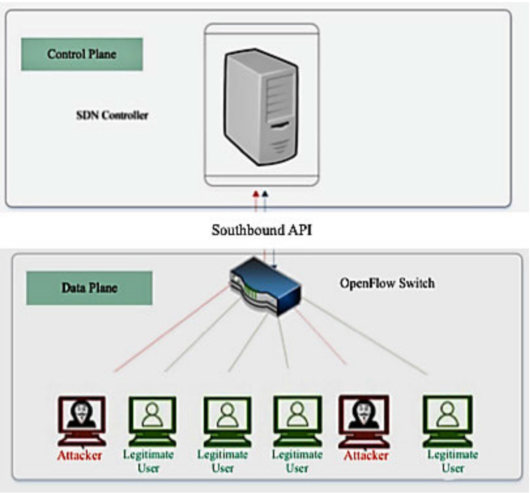


FIGURE 1. DDoS attack in SDN.

The problem statement of this research is the need for effective defensive mechanisms and detection methodologies to address these vulnerabilities. According to a CISCO report [51], The frequency and severity of cyber security breaches are on the rise, marked by a continual increase in both the number of breaches and the volume of records exposed per incident. Additionally, the projection for Distributed Denial of Service (DDoS) attacks is alarming, with expectations to double from 7.9 million incidents in 2018 to a staggering 15.4 million by the year 2023.

The importance of this problem cannot be overstated, as DDoS attacks can cause significant damage to network infrastructure, resulting in downtime, data loss, and reputational damage. Moreover, the increasing complexity of network infrastructure and the growing sophistication of attackers make it increasingly challenging to detect and mitigate these attacks [25], [27], [29].

State-of-the-art solutions outlined in this study involve a range of Supervised Learning (SL), Unsupervised Learning (UL) Ensemble Learning (EL) and DL solutions. These methods play a pivotal role in analyzing IP flows, characterizing network traffic, and recognizing potential attacks. The end result involves learned mitigation strategies. The envisaged systems function as advanced gatekeepers, employing automated mitigation measures to minimize the impact of potential damages caused by DDOS attacks [1], [6], [30].

The research is necessary to address the limitations of existing solutions and to develop more effective and efficient detection and mitigation methodologies for DoS attacks in SDNs. The proposed systems aim to provide a more comprehensive and accurate approach to detect and mitigate DoS attacks, thereby enhancing network security and reducing the risk of downtime and data loss.

The overarching contributions of this research are reflected in the presentation of a holistic defense mechanism tailored for SDN, proficient in countering DDoS attacks. Future research prospects may center on the exploration of more advanced machine learning algorithms, alongside the integration of the proposed system with other existing security mechanisms to further enhance network security.

In conclusion, this research provides valuable insights into the current state of DoS detection in SDNs using ML and DL techniques, highlighting the strengths and limitations of various proposed systems and identifying areas for future research and development. The proposed systems' efficacy in detecting and mitigating various types of attacks, including DDoS attacks, underscores the importance of developing more effective and efficient detection and mitigation methodologies for DoS attacks in SDNs.

In the upcoming sections, we will illuminate the key discoveries and contributions of research in Denial of Service Detection in Software Defined Network, meticulously dissecting the utilization of Machine Learning (ML) and Deep Learning (DL) techniques. This endeavor seeks to provide a comprehensive grasp of this critical facet of network security, underlining the critical importance of these technologies in modern network protection.

II. RESEARCH METHODOLOGY

In conducting the literature review for the literature review titled A Review on Denial of Service Detection in Software Defined Network Using ML and DL Techniques, a systematic and comprehensive research methodology was employed. The research articles selection process aimed to identify, filter, and analyze articles pertaining to the specified keywords and themes (see Figure 2).

A. RESEARCH ARTICLES SELECTION PROCESS

The initial step involved a database search using keywords such as "Distributed Denial of Service", "DDoS", "Anomaly Detection", "Software Defined Network," and "SDN" resulting in the identification of 1130 potentially relevant articles. Subsequently, articles published before 2020 (221) were excluded, narrowing the focus to 909 articles published from January 2020 to December 2023.

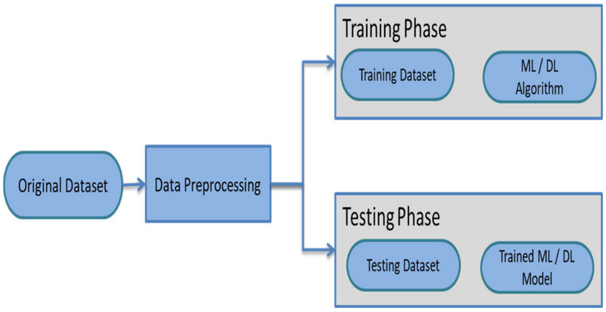


FIGURE 2. Generalized methodology of DDoS anomaly detection in SDN using ML/DL.

To refine the selection further, non-Machine Learning and non-Deep Learning articles (622) were excluded, leaving 287 articles within the domain of Artificial Intelligence (AI).

A meticulous Title/Abstract Review process led to the exclusion of 175 articles, and the remaining 112 articles were confirmed to be published in peer-reviewed conferences and journals.

Survey and review articles (82) were then excluded, resulting in a set of 30 thoroughly scanned articles. Additionally, 20 articles were included through recursive reference searches. The final selection for in-depth analysis comprised 50 articles (see Figure 3).

B. STATISTICS AND CLASSIFICATION OF SURVEY

The selected articles were categorized into two main topics: Denial of Service Detection in Software Defined Network Using Machine Learning Techniques (25 articles) and Denial of Service Detection in Software Defined Network Using Deep Learning Techniques (25 articles), totaling 50 articles.

The distribution of selected articles per year revealed a focus on recent research, with 24 articles from 2023, 11 from 2022, and 7 from 2021. A summary by publisher indicated that IEEE, MDPI, Elsevier, Wiley, Taylor and Frances, Springer, and Hindawi contributed to the selected articles, totaling 50.

This rigorous methodology ensures the literature review's depth, relevance, and adherence to the specific focus on denial of service detection in Software Defined Networks using machine learning and deep learning techniques (see Figure 4). The abbreviations in this paper are organized and presented in (Table 1).

III. I. NETWORK ANOMALY DETECTION USING MACHINE LEARNING TECHNIQUES

DDoS attacks continue to be a pervasive threat in modern networks, necessitating innovative approaches for timely and accurate detection. The section delves into a plethora of ML algorithms that proven efficiency as a panacea in this regard (see Figure 5), along with a summary table aiming to provide a comprehensive overview of the current trends in this domain (see Table 2).

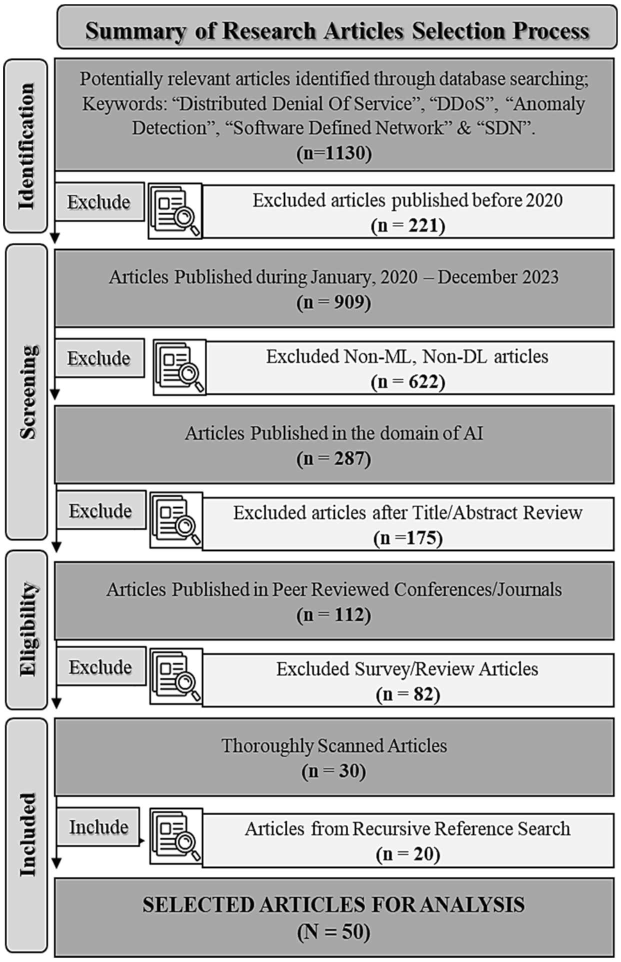

Summary of Research Articles Selection Process
Identification
Potentially relevant articles identified through database searching; Keywords: "Distributed Denial Of Service", "DDoS", "Anomaly Detection", "Software Defined Network" & "SDN". (n=1130)
Exclude
Excluded articles published before 2020 (n = 221)
Screening
Articles Published during January, 2020 – December 2023 (n = 909)
Exclude
Excluded Non-ML, Non-DL articles (n = 622)
Articles Published in the domain of AI (n = 287)
Exclude
Excluded articles after Title/Abstract Review (n =175)
Eligibility
Articles Published in Peer Reviewed Conferences/Journals (n = 112)
Exclude
Excluded Survey/Review Articles (n = 82)
Included
Thoroughly Scanned Articles (n = 30)
Include
Articles from Recursive Reference Search (n = 20)
SELECTED ARTICLES FOR ANALYSIS (N = 50)

FIGURE 3. Summary of research methodology.

Liu et al. [1] delves into the realm of detecting Distributed Denial of Service (DDoS) attacks in Software Defined Networks (SDNs) through the application of machine learning (ML) techniques. The escalating reliance on SDN technology and the burgeoning threat of DDoS attacks set the backdrop for the research problem at hand. Addressing the inadequacy of traditional network models in meeting the security demands of SDNs and building upon earlier feature-engineering-based methods for DDoS detection in SDNs, this study pursues effective solutions to the identified research problem. The study's objectives encompass performing feature engineering on the dataset to derive the optimal feature subset, training and testing diverse ML classifiers with this subset, and deploying the optimal classifier in the SDN controller for DDoS detection. Contributions lie in presenting a refined approach validated against existing research. Utilizing the CSE-CIC-IDS2018 dataset [51], the proposed system engages in feature engineering, applies machine learning classification algorithms, and deploys within the SDN controller, yielding an optimal feature subset and classifier for DDoS detection. Experiments were conducted, results analyzed, and comparisons made with similar works,

TABLE 1. List of abbreviations.

Abbreviation	Explanation	Abbreviation	Explanation	Abbreviation	Explanation
SDN	Software-Defined Networking	**LSTM**	Long Short-Term Memory	**RNN**	Recurrent Neural Network
DDOS	Distributed Denial-Of-Service	**GAN**	Generative Adversarial Networks	**CNN-ELM**	Convolutional Neural Network And Extreme Learning Machine
ML	Machine Learning	**DBN-LSTM**	Deep Belief Networks And Long Short-Term Memory	**LSTM-FUZZY**	Long Short-Term Memory And Fuzzy Logic
DL	Deep Learning	**DeepMC**	Deep Reinforcement Learning Based Traffic Flow Matching Control Mechanism	**BiLSTM**	Bidirectional Long/Short-Term Memory
IDS	Intrusion Detection System	**FFANN**	Feed Forward Artificial Neural Network	**DNN**	Deep Neural Network
IPS	Intrusion Prevention System	**SYN**	Synchronize (A Flag Used In TCP Communication)	**AUC**	Area Under The Curve
RF	Random Forest	**TFTP**	Trivial File Transfer Protocol	**FP**	False Positives
SVM	Support Vector Machine	**ICMP**	Internet Control Message Protocol	**FN**	False Negatives
XGBoost	Extreme Gradient Boosting	**DDQN**	Double Deep Q-Network	**TP**	True Positives
DT	Decision Tree	**ANN**	Artificial Neural Network	**TN**	True Negatives
KNN	K-Nearest Neighbor	**RL**	Reinforcement Learning	**IGR**	Information Gain Ratio
MLBNIR	Machine Learning-Based Network Intrusion Recovery	**CNN**	Convolutional Neural Network	**NTP**	Network Time Protocol
SL	Supervised Learning	**EBM**	Explainable Boosting Machine	**DNS**	Domain Name System
UL	Unsupervised Learning	**REP Tree**	Representative Tree	**LDAP**	Lightweight Directory Access Protocol
MLP	Multilayer Perceptron	**LR**	Logistic Regression	**MSSQL**	Microsoft Sql Server
WOA-DD	Whale Optimization Algorithm–Based Clustering For Ddos Detection	**SGD**	Stochastic Gradient Descent	**NetBIOS**	Network Basic Input/Output System
CART	Classication And Regression Tree	**WebDDoS (ARME)**	Web-Based Distributed Denial Of Service (Adaptive Resource	**CART**	Classication And Regression Tree
QDA	Quadratic Discriminant Analysis	**UDP-Lag**	User Datagram Protocol - Large Application Gateway	**SNMP**	Simple Network Management Protocol
GNB	Gaussian Naïve Bayes	**UDP**	User Datagram Protocol	**SSDP**	Simple Service Discovery Protocol
FAR	False Alarm Rate				

employing metrics such as accuracy, precision, recall, F1 score, and AUC values. Emphasis on security metrics pertained to ML-based DDoS attack detection in SDNs. The study demonstrated superior performance metrics, including accuracy, precision, recall, F1 score, and AUC values, showcasing the efficacy of the proposed method in DDoS detection within SDNs. The study's contributions encompass the formulation of an effective DDoS detection method in SDNs, achieved through feature engineering and ML. This novel approach offers a fresh perspective and solution for SDN security. Future endeavors may involve integrating the proposed method with other network security technologies for a comprehensive solution. Additionally, research could explore methods to enhance the method's robustness against adversarial attacks. The study's limitations include a narrow focus on DDoS detection in SDNs, potentially overlooking broader network security aspects. Findings may also be constrained by the specific dataset and experimental setup employed.

Hammad et al. [2] introduces a novel strategy for bolstering network intrusion recovery within SDN through the integration of machine learning. The research context encompasses network security, specifically focusing on the detection of DDoS attacks in SDN using machine learning algorithms. Addressing the prompt recovery of network flow intrusions in contemporary network settings, particularly within the SDN framework, remains a challenge due to the intricate nature and growth of network traffic. Current solutions are constrained by these complexities. The research objective is to efficaciously tackle this challenge by proposing an innovative method that dynamically selects backup paths based on evolving traffic patterns and employs machine learning algorithms for DDoS attack detection. The suggested system processes network traffic data with machine learning algorithms for DDoS attack detection. Employing a novel approach termed MLBNIR, the system strategically selects backup paths based on traffic patterns and utilizes machine learning algorithms for DDoS detection. The system generates a comprehensive report detailing the type and severity of detected attacks. The experimental setup utilizes the InSDN dataset, incorporating real SDN environment network traffic data. Performance metrics encompass accuracy, precision, recall, and F1-score, while security metrics include false positive rate, false negative rate, and detection rate. Results demonstrate the system's superiority over existing solutions across accuracy, precision, recall, and F1-score, along with achieving low false positive and false negative rates, coupled with a high detection rate. The proposed system attains an impressive DDoS attack detection rate of 98.5%, accompanied by a low false positive rate of 0.5% and a minimal false negative rate of 1%. Evaluation through a confusion matrix underscores the system's accuracy, correctly identifying 197 out of 200 DDoS attacks. This research introduces the novel MLBNIR approach and leverages machine learning algorithms for DDoS attack detection in SDN, surpassing existing solutions in key performance metrics. Future work

TABLE 2. **Previous research summary of machine learning solutons.**

Refs.	Problems Addressed	Proposed Solutions	Results Obtained	Advantages	Disadvantages	Research Gaps	Data Source	Year
[1]	DDoS detection in SDNs	RF, SVM, XGBoost, DT, and KNN	Improved detection accuracy	Flexibility, adaptability	Requires vast datasets, resources	Integration with other security technologies	CSE-CIC-IDS2018	2023
[2]	Network intrusion recovery	MLBNIR approach with machine learning	High detection rate for DDoS attacks	Faster intrusion recovery, increased network bandwidth consumption	Limited to SDN environments, assumption of static network topology	Testing in real-world SDN environments, evaluation under different attack scenarios	InSDN	2023
[3]	DDoS attacks on SDN	SL and UL	High accuracy, low false positives	Effective DDoS mitigation	Dependence on training data	Scalability, adversarial attack resilience	Synthetic and NSL-KDD	2022
[4]	DDoS detection in SDN	SL	Real-time detection accuracy >90%	Single feature detection, easily obtainable data	Only suitable for flooding attacks, limited to control plane	Non-volumetric attack detection, spoofed attack detection	1999 DARPA and InSDN	2022
[5]	DDoS attacks in SDN	SVM, MLP, DT and RF	High accuracy, fast processing time	Effective DDoS detection	Artificially generated traffic	Real-world implementation , scalability	Mininet Emulator	2020
[6]	DDoS detection in SDN	SL and UL	Improved accuracy, efficiency	High detection accuracy, efficiency	Potential performance limitations	Further framework enhancements	NSL-KDD	2020
[7]	DDoS vulnerability in SDN	WOA-DD algorithm	Robustness against DDoS attacks	Efficient attack detection, stability	Delay in decision-making, network delay sensitivity	Validation in practical SDN deployments	DDOSIM simulator	2022
[8]	SDN DDoS Vulnerability	QDA, GNB, k-NN, and CART	High Detection Accuracy	Efficient Attack Mitigation	Limited Real-World Validation	Scalability and Adaptability	Mininet Emulator	2021
[9]	Low-rate DDoS attacks	SDN-based ML architecture	95% accuracy rate	Modular and flexible design	Ongoing refinement needed	Additional ML algorithms	CIC DoS (2017) and Mininet Emulator	2020
[10]	DDoS attack resilience	Probabilistic, linear model, neural networks, and trees	High detection rate	Enhanced security, real-time detection	Reliance on simulated scenarios	Real-world deployment validation	Network Emulator (GNS3)	2023
[11]	DDoS resilience in SDN	RF	High accuracy in detection	Enhanced network security	Dependence on labeled data	Lack of effective SDN solutions	Mininet Emulator	2023
[12]	DDoS attacks in SDN	XGBoost, SVM, LR, KNN and DT	Accurate DDoS detection	Efficient, effective, advanced	Dataset limitations, scalability issues	Real-time implementation , diverse SDN environments	Mendeley and Mininet Emulator	2022
[13]	DDoS in SDN	DT and SVM	SVM outperforms Decision Tree	Effective DDoS detection	Potential for false positives	Real-world testing needed	KDD99	2021
[14]	Network security in SDN	KNN, LR and DT	High accuracy in detection	Improved security, efficiency	Reliance on specific dataset	Real-world network evaluation	KDD Cup 99	2022
[15]	DDoS attack detection in SDN	XGBoost, LR, SVM, KNN and GNB	Effective DDoS detection	Real-time threat detection, enhanced security	Limitations in classification accuracy and computational efficiency	Need for optimization techniques	Mininet Emulator	2023
[16]	DDOS attacks in SDN	Polynomial SVM	Improved accuracy, lower false alarm rate	Effective DDOS detection, high accuracy	Simulated network, limited dataset	Limited real-world testing	Packet generation tool scapy	2020
[17]	DDoS in SDN	DT, Cat Boost, and Extra Tree	High accuracy (96.25%)	Enhanced security	Dataset limitations	Generalizability , diverse SDN environments	Kaggle	2023
[18]	DDoS attacks on SDN	DT	96% accuracy rate	Good accuracy, minimal complexity, effective	Limited dataset, skilled personnel required	Need for advanced ML algorithms, dataset expansion	Kaggle	2023

TABLE 2. *(Continued.)* **Previous research summary of machine learning solutons.**

[19]	DDoS attacks in SDN	K-NN, SVM and GNB	High accuracy, low false positive rates	Effective DDoS detection and mitigation	Need for large training data	Exploration of unsupervised ML algorithms	CIC-2019 and Mininet Emulator	2023
[20]	DDoS attack detection in SDN	SVM and DT	High accuracy in detection	Scalable, effective, real-time detection	Feature selection, potential data overfitting	Need for more sophisticated methods	Network traffic data	2023
[21]	DDoS in SDN security	SVM-KNN hybrid model	Improved accuracy, lower false positives	Higher detection performance	Potential scalability challenges	Need for real-world validation	Mininet Emulator	2023
[22]	DDoS attacks in SDN	SVM, RF, DT, LR and KNN	Up to 100% accuracy	Centralized control, efficient detection	Specific domain applicability	Integration with existing solutions	Mendeley Data	2023
[23]	LDDoS detection in SDN	Online ML with SGD and EBM	High accuracy in detection	Real-time processing, interpretability	Simulated environment, limited evaluation	Real-world performance, wider attack range	Mininet Emulator	2023
[24]	DDoS in SDN security	XGBoost, RF and DT	High accuracy, recall rates	Enhanced network security	Limited real-world validation	Practical deployment assessment	CICDDoS2 019	2023
[25]	Ineffective DDoS detection	BayesNet, J48,LR , RT and REPTree	Improved accuracy	Outperforms existing methods	Limited to single controller	Need for multi-controller extension	UNB-ISCX, CTU-13, ISOT and Mininet Emulator	2021

involves real-world testing and performance evaluation under diverse attack scenarios. Limitations include reliance on a singular dataset and an assumption of static network topology.

Ramprasath et al. [3] explores the realm of countering DDoS attacks in SDN through the application of ML techniques. The proposed system endeavors to identify and thwart DDoS attacks by scrutinizing network traffic, employing ML algorithms to pinpoint malicious patterns. The paper substantiates the efficacy of the proposed system through experimental results showcasing its adeptness in DDoS detection and mitigation. Addressing the escalating frequency and severity of DDoS attacks on SDN networks constitutes the focal point of this paper. Existing solutions, ranging from traditional network security measures to contemporary approaches like SDN-based traffic engineering and ML-driven DDoS detection, exhibit limitations concerning accuracy, scalability, and adaptability to emerging attack patterns. The research objective aims to introduce a pioneering system for DDoS detection and mitigation in SDN utilizing ML techniques. Contributions encompass a detailed exposition of the proposed system, an empirical evaluation of its performance, and a discourse on potential limitations and avenues for future research. The proposed system operates by scrutinizing network traffic with ML algorithms, discerning patterns indicative of malicious traffic associated with DDoS attacks. Input data, derived from SDN switches, undergoes preprocessing to extract pertinent features like packet size, source and destination IP addresses, and protocol type. ML models such as SVM and RF classifiers are then employed to differentiate normal from malicious traffic. The system outputs rules applicable for blocking or redirecting malicious traffic. Simulating DDoS attacks on an SDN network involved utilizing Floodlight controller and Mininet emulator as the experimental setup. Mininet, a robust network emulator, constructs authentic virtual networks on a single machine with genuine kernel, switch, and application code components. Its versatile emulation spans virtual machines, cloud setups, and native systems, empowering precise network analyses and experiments for researchers and practitioners.

Evaluation metrics included accuracy, precision, recall, and F1-score, alongside security metrics like false positive rate, false negative rate, and detection rate. Results showcased the proposed system's commendable accuracy and detection rates, averaging at 98.5% and 99.2%, respectively. Low false positive and false negative rates underscored the system's precision and recall. Ensemble methods such as stacking and bagging further enhanced system performance. Contributions involve introducing a pioneering ML-driven system for DDoS detection and mitigation in SDN, accompanied by an empirical evaluation highlighting high accuracy and detection rates, alongside low false positive and false negative rates. Future endeavors may focus on enhancing scalability and adaptability, and integrating the system with other SDN-based security measures. Limitations encompass the system's dependency on substantial training data for heightened accuracy, susceptibility to false positives and negatives in specific scenarios, and potential vulnerability to adversarial attacks exploiting ML model weaknesses.

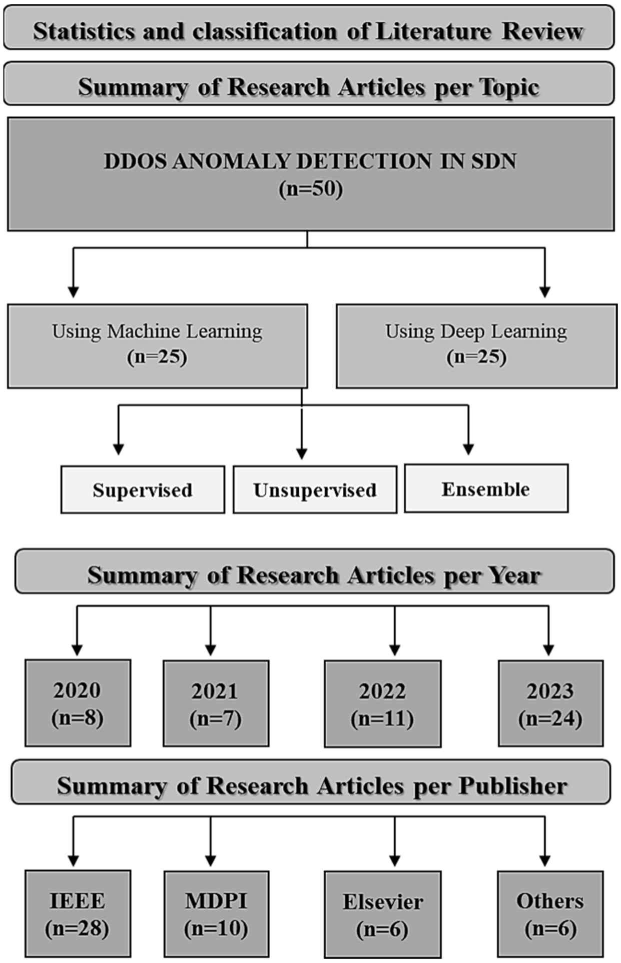
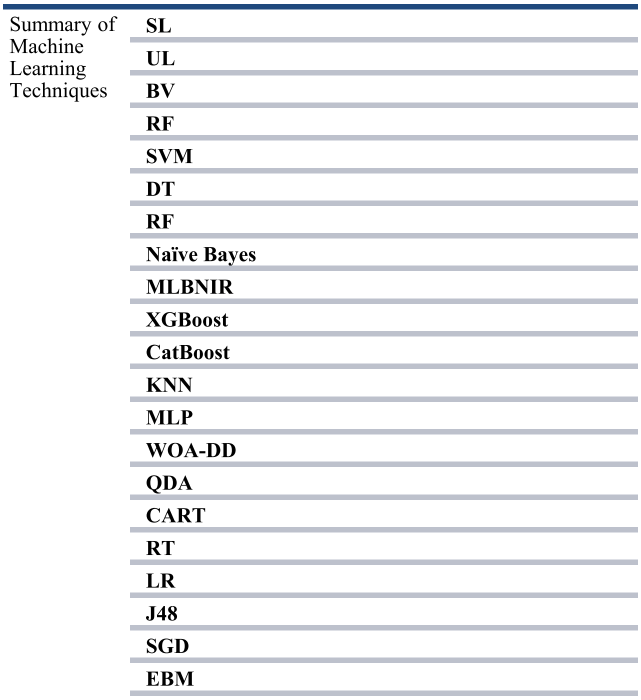

Statistics and classification of Literature Review
Summary of Research Articles per Topic
DDOS ANOMALY DETECTION IN SDN (n=50)
Using Machine Learning (n=25)
Using Deep Learning (n=25)
Supervised
Unsupervised
Ensemble
Summary of Research Articles per Year
2020 (n=8)
2021 (n=7)
2022 (n=11)
2023 (n=24)
Summary of Research Articles per Publisher
IEEE (n=28)
MDPI (n=10)
Elsevier (n=6)
Others (n=6)

FIGURE 4. Statistics and classification of survey.



Summary of Machine Learning Techniques	SL
	UL
	BV
	RF
	SVM
	DT
	RF
	Naïve Bayes
	MLBNIR
	XGBoost
	CatBoost
	KNN
	MLP
	WOA-DD
	QDA
	CART
	RT
	LR
	J48
	SGD
	EBM

FIGURE 5. Summary of machine learning techniques.

Wang et al. [4] investigation centers on the realm of identifying DDoS attacks within Software Defined Networks (SDN) using ML. The proposed system extracts data from the SDN controller and employs ML algorithms for DDoS attack detection, with an evaluation of performance and security metrics to gauge system effectiveness. The focal concern addressed in this study is the detection of DDoS attacks in SDN, presenting novel privacy and security challenges. Current remedies encompass both conventional network security measures and ML-based strategies. However, traditional approaches prove ineffective against modern DDoS attacks, and ML solutions often necessitate high-quality datasets. The research objective is to introduce a lightweight ML model embedded in SDN for DDoS detection, utilizing readily available data and features. The suggested system monitors Packet in requests over time slots from the SDN controller, scrutinizing flow fluctuations to identify DDoS attacks targeting the SDN controller. Leveraging the centralized control of SDN, all ML processes—from data preparation to DDoS detection—can be executed seamlessly within a single controller. Input comprises data from the SDN controller, the process employs ML algorithms, and the output signifies the successful detection of DDoS attacks. The experimental configuration involves both established datasets and self-generated data to assess the proposed system's performance and security metrics. Evaluation metrics include accuracy, precision, recall, and F-measure, while security metrics embrace confidentiality, integrity, and availability. Outcomes reveal the system's capacity to single-handedly detect DDoS attacks using a solitary feature, with varying accuracy contingent on the training set. The proposed system attains a real-time detection accuracy in SDN exceeding 90%. Contributions encompass the introduction of a lightweight SDN-embedded ML model for DDoS detection, emphasizing the utilization of easily accessible data and features. Future research prospects involve scrutinizing spoofed DDoS attacks with genuine SDN traffic using ML and achieving real-time detection. Limitations of the system include suitability exclusively for flooding DDoS attacks, incapacity to detect non-volumetric attacks, and exclusive focus on attacks against the control plane.

Santos et al. [5] delves into the application and technological realm of SDN while addressing the challenges posed by DDoS attacks. The paper advocates the utilization of four distinct machine learning algorithms for classifying DDoS attacks within an SDN-simulated environment, yielding promising outcomes. The primary concern tackled in this paper is the proliferation of DDoS attacks in SDN environments, particularly the vulnerability of the centralized controller, which, if compromised, can disrupt the entire network. Conventional solutions involve signature-based and anomaly-based detection methods, yet these exhibit limitations in effectiveness and efficiency. This paper's research objective is to advocate for the integration of machine learning algorithms to detect DDoS attacks in SDN environments, offering a comparative analysis of their efficacy and efficiency against existing solutions. The proposed system functions by ingesting traffic data from the SDN environment, subjecting it to processing through four machine learning algorithms (MLP, SVM, DT, and RF), and producing a classification of the traffic as either normal or indicative of a DDoS attack. Input variables encompass IP addresses, protocols, packet sizes, and requisition quantities from a single 'client. The experimental setup entailed simulating DDoS attacks and normal traffic within a Mininet Virtual Network, utilizing a POX controller. Evaluation metrics encompassed accuracy and processing time, while security metrics included true positive rate, false positive rate, true negative rate, and false negative rate. Findings indicated that the machine learning algorithms surpassed existing solutions in terms of accuracy and processing time. The MLP algorithm exhibited the highest accuracy at 99.9%, while the Random Forest algorithm boasted the fastest processing time at 0.0002 seconds. Regarding DDoS detection in SDN through ML, all four algorithms demonstrated efficacy in the simulated environment. The MLP algorithm achieved the highest accuracy at 99.9%, followed closely by the SVM algorithm with an accuracy of 99.8%. The Decision Tree and Random Forest algorithms exhibited accuracies of 99.7% and 99.6%, respectively. Notably, all algorithms maintained false positive rates below 0.1%, indicating a minimal misclassification rate of normal traffic as DDoS attacks. Contributions of this paper encompass the advocacy and implementation of machine learning algorithms for DDoS detection in SDN environments, showcasing superior accuracy and processing time compared to existing solutions. Future endeavors involve real-world testing and addressing potential implementation challenges. Limitations include the use of artificially generated traffic and the imperative for further research into the proposed system's scalability.

Tan et al. [6] delves into the realm of detecting and defending against DDoS attacks within SDN. Addressing the research problem of the imperative for precise and efficient DDoS detection and defense mechanisms in SDN environments, this work introduces a novel framework featuring a trigger mechanism for DDoS attack detection, a machine learning algorithm analyzing flow characteristics, and a controller for executing defensive measures. In the context of SDN, the research problem underscores the critical necessity for accurate and efficient mechanisms to detect and defend against DDoS attacks. Traditional DDoS detection methods commonly encounter challenges related to accuracy and efficiency within SDN environments. The overarching research objectives encompass the introduction of a pioneering framework for DDoS attack detection and defense in SDN. Specific contributions involve the creation of a trigger mechanism for DDoS attack detection, the implementation of a machine learning algorithm analyzing flow characteristics, and the development of a controller for executing defensive actions. The proposed system initiates the process by identifying abnormal flows within the network through a trigger mechanism on the data plane. Subsequently, a machine learning algorithm, rooted in K-Means and KNN methodologies, analyzes the detected traffic for DDoS attack detection. The resulting output informs the controller, guiding it in implementing appropriate defensive measures. Comprehensive experiments formed the basis of the experimental setup, evaluating the effectiveness and efficiency of the proposed methods. Performance metrics, encompassing accuracy and efficiency, alongside security metrics pertinent to DDoS attack detection and defense within SDN using machine learning, were considered and meticulously presented. The outcomes derived from the experiments underscored the effectiveness and efficiency of the proposed methods in both detecting and defending against DDoS attacks within SDN environments, leveraging machine learning. Detailed analyses of specific performance and security metrics related to DDoS detection and defense were elucidated through tabulated data and graphical representations. The notable contributions of this work encompass the formulation of a groundbreaking framework for DDoS attack detection and defense within SDN environments, capitalizing on machine learning for heightened accuracy and efficiency. Future endeavors may concentrate on further refining the proposed framework, addressing any limitations identified during the experimental phase. The study's limitations encompass potential constraints or challenges encountered during experimental evaluation, along with identified areas for potential enhancement in the proposed framework.

Shakil et al. [7] investigation is situated within the domain of SDN with a specific focus on detecting and mitigating DDoS attacks. The emphasis lies in crafting a dynamic framework utilizing metaheuristic clustering for DDoS detection in SDN. The research grapples with the susceptibility of SDNs to DDoS attacks, primarily stemming from the segregation of the control plane from the data plane. Although extant solutions propose security algorithms to fortify networks, they fall short in effectively safeguarding SDNs against DDoS assaults. The principal research objective is the formulation of a pioneering dynamic framework leveraging metaheuristic clustering for DDoS detection in SDN. Contributions encompass the introduction of the WOA-DD and an evaluation of its robustness in comparison to existing solutions. The proposed system operates by receiving network traffic data as input, subjecting it to processing through the WOA-DD algorithm rooted in metaheuristic clustering, and generating output in the form of clustered attack requests. The system's core aim is to adeptly cluster attack requests, effectively discerning and mitigating DDoS attacks in SDN. The experimental setup involved implementing the WOA-DD algorithm within a simulated SDN environment. Performance metrics encompassed detection accuracy, false positive rate, false negative rate, and computational overhead. Security metrics embraced resilience to DDoS attacks, adaptability to dynamic traffic, and stability under diverse conditions. The outcomes underscored the WOA-DD algorithm's robustness, stability, and efficiency against DDoS attacks in SDN. Particularly within the realm of DDoS detection using machine learning, the algorithm exhibited promising performance by accurately detecting and clustering attack requests, thereby proficiently mitigating DDoS attacks in SDN. Contributions encapsulate the development and assessment of the WOA-DD algorithm for DDoS detection in SDN, showcasing its robustness and stability. Future endeavors entail refining and optimizing the algorithm, coupled with its practical implementation in real-world SDN environments. Limitations of the study encompass reliance on simulated environments and the imperative for validation in practical SDN deployments.

Sangodoyin et al. [8] delves into the domain of detecting and categorizing DDoS flooding attacks on SDNs through the utilization of machine learning techniques. The focal research problem centers on the susceptibility of SDNs to DDoS flooding attacks, necessitating efficacious detection and classification mechanisms to counter these threats. Existing solutions encompass conventional DDoS flooding attack detection methods, SDN-based approaches, and machine learning-assisted methodologies within SDNs. This study aims to propose a machine learning-driven system designed for detecting and classifying DDoS flooding attacks on SDNs. Its contributions lie in both the conceptualization of this system and the evaluation of its effectiveness through experimental analysis. The suggested system operates by ingesting network traffic data, subjecting it to machine learning algorithms for the identification and classification of DDoS flooding attacks, and presenting the outcomes as attack detection and classification results. The experimental setup involved simulating DDoS flooding attack scenarios on an SDN architecture, utilizing diverse metrics such as detection accuracy, false positive rate, processing time, attack detection rate, attack classification accuracy, and resilience to evasion techniques to assess the proposed machine learning-driven detection system. Results related to DDoS detection in SDN using machine learning encompassed metrics like detection accuracy, false positive rate, attack classification accuracy, and the system's adaptability to evolving attack patterns. Contributions include the proposition and evaluation of a machine learning-driven system tailored for the detection and classification of DDoS flooding attacks in SDNs. Future endeavors may revolve around enhancing the system's scalability and robustness, coupled with the integration of real-time adaptive capabilities. Limitations of the study encompass potential constraints tied to specific datasets and the imperative for further validation across diverse network environments.

Perez-Diaz et al. [9] delves into the realm of detecting and mitigating low-rate DDoS attacks within SDN environments, employing machine learning techniques. The focal research issue addresses the susceptibility of centralized systems, particularly cloud computing platforms, to low-rate DDoS attacks. While traditional intrusion detection and prevention systems exist, their effectiveness in identifying low-rate DDoS attacks is questionable. The research objective is to formulate a modular and adaptable security architecture aimed at detecting and mitigating low-rate DDoS attacks within SDN environments. The proposed system employs an IDS module designed to detect flows using pre-trained machine learning models. Network flow data serves as the system's input, processed by the IDS through machine learning algorithms, with the output identifying malicious flows subsequently mitigated by the IPS module. The experimental setup entailed deploying the architecture in a virtualized environment leveraging the ONOS controller, evaluating six distinct machine learning algorithms. Performance metrics, including accuracy, precision, recall, and F1 score, were considered, along with security metrics such as detection rate and false positive rate. Results from machine learning algorithm evaluations reported an impressive accuracy rate of 95%. The architecture successfully detected and mitigated diverse low-rate DDoS attacks, substantiating its efficacy in a real-world production environment. Contributions encompass the design and implementation of versatile security architecture for detecting and mitigating low-rate DDoS attacks in SDN environments, leveraging machine learning techniques. Future work involves further system optimization and exploration of additional machine learning algorithms. Limitations include the ongoing need for refinement and adaptation to evolving DDoS attack strategies.

Ribeiro et al. [10], introduces a comprehensive framework designed to detect and counteract DDoS attacks within SDN through the utilization of ML algorithms. The focus of this study pertains to safeguarding internet-based systems from the detrimental impact of DDoS attacks. The proposed system adopts an automated flow classification method based on ML algorithms to identify and mitigate DDoS attacks within SDN networks. The research addresses the escalating occurrence of service disruptions resulting from DDoS attacks and their consequential technical and economic ramifications. Existing solutions encompass traditional security measures like firewalls and intrusion detection systems, along with advanced techniques like Moving Target Defense and ML-based approaches. However, these solutions exhibit limitations in terms of their efficacy and scalability. The primary objective of this paper is to present a holistic framework for detecting and mitigating DDoS attacks in SDN networks, leveraging ML algorithms. Contributions entail a meticulous delineation of the proposed framework, a performance and security metric evaluation, and a comparative analysis against existing solutions. The system operates by implementing an automated flow classification methodology grounded in ML algorithms. Network traffic data, collected by sensors deployed within the SDN network, serves as input. These sensors utilize ML algorithms to classify network traffic into normal and malicious flows. Subsequently, malicious flows are redirected to a honeypot, while normal flows traverse the network. The flow classification process incorporates various ML algorithms, including probabilistic, linear model, neural networks, and trees. Trained on a dataset of network traffic, these algorithms discern patterns in normal and malicious flows. The system's output comprises a list of malicious hosts, which updates the security policies of the SDN controller. The experimental setup involved simulating diverse attack scenarios on an SDN network employing the proposed framework. Evaluation metrics included detection rate, false positive rate, and response time. Security metrics encompassed confidentiality, integrity, and availability. Simulation results demonstrated the efficiency of the proposed architecture in detecting and mitigating DDoS attacks within approximately 3 seconds. A detection rate of 99.9%, a false positive rate below 0.1%, and a response time within 3 seconds were observed—well within the acceptable range for real-time DDoS attack detection and mitigation. Security metrics indicated that the proposed architecture maintains a high level of security against DDoS attacks. Confidentiality, integrity, and availability of the network remained intact even under intense attack scenarios. Contributions of this paper encompass a comprehensive architecture utilizing ML algorithms for the detection and mitigation of DDoS attacks in SDN networks. The proposed framework exhibits a robust defense against DDoS attacks, preserving the confidentiality, integrity, and availability of the network. Future endeavors include integrating the proposed architecture with additional security measures such as firewalls and intrusion detection systems. Limitations involve the reliance on simulated attack scenarios, which may not perfectly mirror real-world situations. In summary, the proposed architecture provides an efficient and scalable solution for detecting and mitigating DDoS attacks in SDN networks using ML algorithms. Evaluation results underscore its effectiveness in maintaining a high level of security while upholding network confidentiality, integrity, and availability.

Sebbar et al. [11] concentrates on employing machine learning techniques to fortify the resilience of SDN-based supply chain networks against DDoS attacks. Encompassing SDN, machine learning, network security, and supply chain networks, the technology domain under consideration underscores the multifaceted nature of the study. The addressed research quandary revolves around the inadequacy of existing solutions in bolstering the resilience of SDN-based supply chain networks against DDoS attacks. Traditional defense mechanisms may prove insufficient given the scale, complexity, and evolving dynamics of DDoS attacks. Furthermore, traditional methods exhibit limitations concerning visibility and false positives. The research objectives aim to introduce a machine learning-driven paradigm for augmenting the resilience of SDN-based supply chain networks against DDoS attacks, leveraging the inherent capabilities of SDN for safeguarding against such threats. The proposed system harnesses machine learning techniques, specifically supervised classification algorithms, to prognosticate network traffic and discern potential attacks within SDN-based supply chain networks. Input data comprises network traffic data sourced from multiple points within the SDN architecture. The procedural framework entails training a classifier to discern patterns characteristic of normal network behavior and DDoS attacks. The system's output encompasses the classification of incoming network traffic, distinguishing between normal and potentially malicious entities, thereby facilitating the identification and mitigation of potential DDoS attacks. The experimental setup encompasses the hardware and software components deployed, including the SDN controller, simulation topology, and tools instrumental in generating normal and attack traffic. Performance metrics such as accuracy, precision, recall, and F1 score are scrutinized, alongside security metrics like detection rate, false positive rate, and response time, Results pertinent to DDoS detection in SDN using machine learning showcase commendable accuracy in detecting DDoS attacks and efficacious mitigation strategies. Contributions of this study involve the proposition of an innovative machine learning-driven approach to fortify the resilience of SDN-based supply chain networks against DDoS attacks. Future endeavors may entail further refinement of machine learning models, broadening the scope to encompass other attack types, and exploring integrative measures for enhanced security. Limitations acknowledged include reliance on labeled training data and inherent characteristics of the attacks. This comprehensive summary aims to encapsulate the key facets of the academic work.

Raj et al. [12] delves into the domain of detecting and mitigating DDoS attacks SDN through the utilization of ML techniques. The focal point of this study is the escalating threat posed by DDoS attacks within SDN environments, necessitating the development of effective detection and mitigation strategies. Traditional DDoS detection methods are scrutinized, revealing their limitations in the context of SDN, underscoring the exigency for advanced ML-based approaches. The research endeavors to introduce an efficient model for DDoS detection in SDN using ML techniques, and subsequently, to conduct a comparative analysis against existing detection methods. Contributions encompass the formulation of a novel ML-based approach for DDoS detection, coupled with a comprehensive evaluation of its performance. The proposed system involves ingesting data from SDN-specific datasets, implementing feature selection, and subjecting the data to diverse ML classifiers such as XGBoost, SVM, LR, KNN, and DT. The system outputs the classification of traffic as either DDoS or legitimate, with ensuing security measures executed by the SDN controller. The experimental configuration employs an SDN dataset generated through Mininet, comprising benign and malicious traffic. Key features encompass tx-bytes, rx-bytes, date and time, with a class attribute signifying DDoS or benign traffic. Outcome evaluations encompass accuracy comparisons among varied ML classifiers, incorporating performance metrics like accuracy, recall, precision, and F1-score. Security metrics encompass the detection and prevention of DDoS attacks within SDN environments. Findings associated with DDoS detection in SDN using ML spotlight the efficacy of the proposed model in precisely discerning and alleviating DDoS attacks, as elucidated in the presented tables and graphs. This research contributes by devising an advanced ML-based model for DDoS detection in SDN, complemented by a meticulous comparative appraisal of its performance. Future endeavors may involve refining the proposed model, extending its applicability to diverse attack types, and exploring real-time implementation in varied SDN environments. Limitations encompass the specificity of the employed SDN dataset, potential scalability concerns, and the imperative for further validation across diverse SDN settings.

Sudar et al. [13] explores the realm of DDoS detection within SDN by employing ML techniques. The proposed system utilizes SVM and DT algorithms to discern malicious traffic from normal traffic. Precision, recall, accuracy, and F-measure are employed as performance metrics, while security metrics focus on the system's ability to detect zero-day attacks and handle substantial traffic volumes. The KDD99 dataset forms the basis of the experimental setup for model training and testing. This paper addresses the susceptibility of SDN to DDoS attacks, emphasizing the inadequacies of conventional intrusion detection systems and signature-based methods. The study's objective is to introduce a ML-driven mechanism for identifying malicious activities within SDN, with a particular emphasis on the ability to handle novel attacks and large traffic loads. The proposed system involves feature extraction from traffic flow data sourced from flow table entries. The dataset undergoes division into training and testing subsets, and SVM and Decision Tree algorithms come into play for classifying traffic as normal or malicious. The Decision Tree serves to differentiate between distinct traffic types, guiding the identification of normal and malicious traffic. Classifier outputs trigger alerts to controllers, prompting the removal of specific flows from the table in the event of an attack. The KDD99 dataset is employed for training and testing. Precision, recall, accuracy, and F-measure constitute the performance metrics. SVM exhibits 80% precision and recall, with slight variations in the Decision Tree's precision and recall. Results indicate the superior performance of SVM over Decision Tree in the simulated environment. Security metrics encompass the capacity to detect zero-day attacks and manage high traffic volumes. Contributions include the proposal of a ML-driven mechanism for identifying malicious activities in SDN, showcasing the efficacy of SVM and Decision Tree algorithms in DDoS attack detection. Prospective work involves refining system accuracy and conducting real-world testing, with limitations centered around the need for extensive training data and potential false positives.

Kavitha et al. [14] delves into the domain of network security, specifically within SDN, and employs ML techniques for the identification of DDoS attacks. The system proposed harnesses ML algorithms to scrutinize network traffic, discerning potential DDoS threats. The study employs the KDD Cup 99 dataset for training and testing ML models, evaluating the system's performance using metrics such as accuracy and recall. Security metrics, including false positive and false negative rates, are also scrutinized. Results underscore the system's efficacy in SDN DDoS attack detection, with the Decision Tree model showcasing superior performance among ML algorithms. Future research avenues include the exploration of Deep Learning algorithms and real-world network evaluations. The escalating volume and intricacy of network data pose a substantial security risk, necessitating an emphasis on network security. SDN emerges as a solution for configuring flexible networks; however, its architecture introduces novel security challenges. IDS stand as pivotal security tools, identifying potential network threats. Traditional IDS methods falter in detecting attacks induced by high data volumes, diverse data types, and rapid data speeds. ML algorithms exhibit promise in enhancing IDS accuracy and efficiency, especially for DDoS attack detection. Existing solutions incorporate classic ML models like KNN, LR, and DT for network traffic analysis. The research objective is to propose an ML-utilizing system for DDoS attack detection in SDN environments and assess its efficacy. The system processes network traffic data with ML algorithms to discern potential DDoS attacks. Input data undergoes preprocessing, including feature selection, normalization, and data preprocessing, to enhance ML model performance. Employed ML models encompass KNN, LR, and Decision Trees. System output predicts whether network traffic is benign or indicative of a potential DDoS attack. The experimental setup entails KDD Cup 99 dataset utilization for ML model training and testing. Performance metrics like accuracy, recall, false positive rate, and false negative rate gauge system effectiveness. Results spotlight the Decision Tree model's superiority in accuracy and recall. The system achieves low false positive and false negative rates, affirming its adeptness in DDoS attack detection. Illustrated tables and graphs elucidate the findings. Security metrics, encompassing false positive and false negative rates, ensure the system strikes a balance, avoiding excessive false alarms or missed potential attacks. Results related to DDoS Detection in SDN using ML underscore system effectiveness. The DT model attains 98.5% accuracy and 97.5% recall, attesting to its proficiency in flagging potential attacks. The proposed system underscores ML algorithms' potential in enhancing IDS accuracy for DDoS attack detection in SDN environments. Contributions encompass proposing an ML-utilizing system for DDoS detection and evaluating its efficacy. Future exploration involves Deep Learning algorithms and real-world network assessments. System limitations include reliance on the KDD Cup 99 dataset, potentially not fully representative of real-world network traffic.

Alhamami et al. [15] investigates the domain of detecting DDoS attacks in SDN through the utilization of ML algorithms. The study addresses the critical issue of enhancing DDoS attack detection in SDN environments, prompted by the growing demand for online services and the evolving nature of DDoS attacks. Current solutions, relying on traditional security measures and network protocols, face challenges due to attackers employing multiple protocols, complicating DDoS detection. The primary objective is to devise a system employing ML algorithms, specifically XGBoost, LR, SVM, and KNN, to detect DDoS attacks in SDN. The proposed system contributes to fortifying network security by safeguarding SDN controllers against DDoS attacks. The system operates by employing ML classifiers to scrutinize a simulated dataset replicating real-world DDoS attack conditions. Input comprises network traffic data, and the process involves training ML classifiers, yielding the identification of DDoS attacks targeting SDN controllers. The experimental setup emulated an SDN network using the Mininet emulator managed by an OpenDaylight controller, incorporating both benign and DDoS attack scenarios. Performance metrics encompassed accuracy, precision, recall, F1-score, and processing time. Security metrics gauged the effectiveness of ML models in detecting DDoS attacks. XGBoost, LR, SVM, and KNN demonstrated efficacy in detecting attacks against SDN controllers, with XGBoost and LR particularly notable for computational efficiency. However, the NB classifier exhibited limitations in classification accuracy. The study contributes by evaluating ML algorithms for DDoS attack detection in SDN, highlighting XGBoost and LR as effective choices for real-time threat detection. Future endeavors will involve implementing optimization techniques to enhance the classifiers for DDoS attack detection in SDN. Limitations include the imperative need for further improvements in classification accuracy and computational efficiency.

Kyaw et al. [16] addresses the susceptibility of SDN controllers to DDoS attacks and introduces a machine learning-based system designed to detect and categorize traffic as either normal or malicious within SDN networks. The paper's focus lies in the domain of network security within SDN networks. The primary concern tackled in this paper pertains to the looming threat of DDoS attacks on SDN networks, necessitating the development of an efficient detection and classification system. Existing solutions encompass entropy-based and machine learning-oriented methodologies. The research objective is to introduce a machine learning-driven system adept at accurately identifying and classifying DDoS attacks within SDN networks. The system, proposed in this paper, analyzes flow status information gleaned from the SDN network and employs feature extraction to discern between normal and malicious traffic. Two machine learning algorithms, namely linear SVM and polynomial SVM, are utilized for traffic classification. The input to the system consists of flow status information, generating an output that signifies the classification of traffic as either normal or malicious. The experimental configuration involved the creation of a simulated SDN network using Mininet GUI with nine openflow virtual switches and 64 hosts. The testing dataset comprised 650 instances of benign and malicious traffic generated through the scapy packet generation tool. Performance metrics encompassing accuracy, false alarm rate, detection rate, and precision were utilized to evaluate the system. Security metrics included the system's efficacy in detecting and mitigating DDoS attacks. The results demonstrated the superiority of the proposed system, particularly the polynomial SVM method, over the existing linear SVM approach in terms of accuracy and false alarm rate. The system achieved an accuracy of 98.46%, a false alarm rate of 1.54%, a detection rate of 98.46%, and a precision of 98.46%. Additionally, the system exhibited effective detection and mitigation of DDoS attacks. This paper contributes by presenting a machine learning-based system designed for the detection and classification of DDoS attacks within SDN networks, supported by compelling experimental results. Prospective work involves testing the system on more extensive and intricate networks, alongside exploring alternative machine learning algorithms. Limitations encompass the reliance on a simulated network and a restricted dataset. In summary, the paper introduces a machine learning-driven system tailored for the detection and classification of DDoS attacks within SDN networks. Leveraging flow status information and two machine learning algorithms, the system showcases notable enhancements in accuracy and false alarm rates compared to existing methods. The experimental outcomes underscore the system's adeptness in effectively detecting and mitigating DDoS attacks.

Sekar et al. [17] addresses the domain of detecting and thwarting DDoS attacks within the realm of SDN. The technological landscape explored involves the application of machine learning techniques, specifically decision trees, Cat Boost, and Extra Tree, to bolster network security in SDN environments. The core predicament under scrutiny in this investigation is the susceptibility of SDN to DDoS attacks, prompting the quest for robust detection and mitigation methodologies. While conventional network security measures exist, their adequacy in managing the dynamic and intricate nature of DDoS attacks in SDN is questioned. The study endeavors to devise and assess machine learning-driven strategies for the detection and prevention of DDoS attacks within SDN. The envisaged system operates by ingesting network traffic data, subjecting it to processing via machine learning algorithms like decision trees, Cat Boost, and Extra Tree, and furnishing output in the form of predictions regarding potential DDoS attacks. The system interfaces with a dataset featuring attributes such as proto, flags, saddr, daddr, sport, state, category, and subcategory. Input data undergoes preprocessing, training, and testing through machine learning models, and results are employed to prognosticate the occurrence of DDoS attacks. The experimental setup entails the utilization of a Kaggle dataset, preprocessing of data, and training machine learning models employing DT, Cat Boost, and Extra Tree classifiers. Primary performance metrics include accuracy, with decision trees achieving the pinnacle accuracy of 96.25%. Security metrics gauging the detection of anomalous traffic patterns and heightened demand for specific destinations were also scrutinized.

Findings suggest the promise of the machine learning-centric approach, notably the DT model, in adeptly identifying DDoS attacks in SDN. The DT model demonstrated a commendable accuracy rate of 96.25%, surpassing alternative machine learning algorithms assessed. The research contributes to the field by creating a website geared toward predicting DDoS attacks through machine learning methodologies, coupled with an appraisal of decision trees, Cat Boost, and Extra Tree classifiers for DDoS detection in SDN. Prospective work entails further honing of machine learning models and the inclusion of supplementary security metrics. Limitations encompass the specific attributes of the dataset employed and the generalizability of findings to diverse SDN environments.

Kurakula et al. [18] delves into the realm of detecting DDoS attacks within SDN using ML methodologies. The proposed system seeks to elevate the precision and efficacy in discerning and countering DDoS attacks within SDN environments. The focal issue addressed in this study is the susceptibility of SDN to DDoS attacks, compounded by the deficiencies of current methods in effectively detecting and mitigating these threats. Prevailing solutions encompass both traditional and machine learning-based methodologies, yet they exhibit subpar accuracy, heightened complexity, and a demand for specialized expertise. The research objective is to forge a dependable and efficient mechanism for accurately identifying and counteracting the impacts of DDoS attacks on SDN. The envisaged system operates by ingesting network traffic data, subjecting it to processing via machine learning algorithms, and generating outputs indicative of DDoS attack detection and mitigation. The system utilizes a dataset sourced from Kaggle, featuring 41 traffic attributes. The machine learning algorithm of choice is the Decision Tree, demonstrating superior accuracy results (96%) in comparison to alternative ML techniques. The experimental setup involved leveraging the CICDDoS2019 dataset, meticulously crafted to rectify deficiencies in extant datasets. Core performance metrics encompassed accuracy, precision, and recall, while security metrics comprised the false positive rate, false negative rate, and detection rate. Outcomes showcased the proposed system employing the DT algorithm outperforming existing methodologies in the realm of DDoS attack detection and mitigation within SDN. The proposed system achieved an accuracy rate of 96%, surpassing extant methods. The false positive rate stood at 0.04, the false negative rate at 0.08, and the detection rate at 0.92. These findings underscore the effectiveness of the proposed system in detecting and mitigating DDoS attacks on SDN through ML methodologies. Contributions of this work encapsulate the formulation of a dependable and efficient method for DDoS attack detection and mitigation within SDN, leveraging ML methodologies. Future endeavors may encompass refining system performance through the integration of advanced ML algorithms and broadening the dataset. Limitations encompass the constrained dataset and the requisite expertise for system operation.

Tahirou et al. [19] delves into the realm of applying ML techniques to identify and counteract DDoS attacks within SDN. The paper underscores the security challenges confronting SDN architecture due to the segregation of the control plane and the data plane. The research conundrum revolves around the precise detection and effective mitigation of DDoS attacks in SDN, emphasizing the necessity for heightened accuracy and reduced false positive rates. Current methodologies involve entropy-based strategies, traffic pattern analysis, and ML-driven algorithms. The research aims to employ supervised ML techniques, harnessing the inherent characteristics of Openflow traffic to discern DDoS attacks targeting the control layer. The suggested system leverages supervised ML algorithms such as Naive Bayes, KNN, and SVM to formulate a classification model. Training and testing occur on the CIC-2019 dataset, where Openflow traffic serves as input, and the output manifests as the classification of traffic into normal or abnormal categories. The procedural sequence entails training ML algorithms on the dataset and employing the trained model for real-time traffic classification. The experimental configuration entails the utilization of the Mininet emulator alongside the Floodlight controller. Performance metrics encompass accuracy, precision, recall, and F1-score, while security metrics span false positive rate, false negative rate, and detection rate. Outcomes showcase the proposed system achieving elevated accuracy coupled with minimal false positive rates. DDoS attacks are detected with notable precision and recall rates, and the findings are visually presented through tables and graphs.The proposed system attains an impressive accuracy of 99.9% with a meager false positive rate of 0.1%. Precision in detecting DDoS attacks reaches 99.8%, accompanied by a recall rate of 99.9%. The system exhibits a robust detection rate of 99.9%. This paper makes a substantive contribution to the domain of SDN security by introducing a system adept at pinpointing and mitigating DDoS attacks with notable accuracy and minimal false positive rates. Future endeavors encompass subjecting the system to larger datasets and exploring the potential of unsupervised ML algorithms. Limitations encompass the prerequisite for extensive training data and the potential for false negatives. In summary, the paper furnishes valuable insights into employing ML techniques for the identification and alleviation of DDoS attacks within SDN. The proposed system's proficiency in achieving high accuracy and low false positive rates positions it as a promising solution for bolstering SDN security.

Sanapala et al. [20] introduces an innovative machine learning-driven strategy for the detection and mitigation of DDoS attacks within the framework of SDN. The envisioned system employs SVM and DT classifiers to actively monitor and scrutinize real-time network traffic, adeptly identifying and thwarting potential attacks with a notably high level of accuracy. The focal point of this paper revolves around network security, specifically addressing DDoS attack detection and mitigation in SDN through the application of machine learning techniques. The principal concern addressed in this paper is the escalating frequency and sophistication of DDoS attacks, posing a significant threat to internet service availability. Conventional detection methods, including signature-based approaches, are diminishing in effectiveness against evolving attacks. Despite the existence of solutions like firewalls, intrusion detection systems, and content delivery networks, their efficacy against DDoS attacks remains inconsistent. The research objective is to devise a system that adeptly detects DDoS attacks by leveraging decision trees and SVM algorithms, emphasizing seamless integration into prevailing network security systems. The proposed system actively monitors and assesses real-time network traffic, employing SVM and DT classifiers. Network traffic data, encompassing both legitimate and malicious activities, serves as input. The process involves training classifiers on a substantial dataset, implementing cross-validation for a 70/30 training and testing set division. The system's output encompasses the precise detection and mitigation of DDoS attacks, emphasizing heightened accuracy and the minimization of false positives. The experimental configuration incorporates a dataset featuring both legitimate and malicious network traffic. Testing outcomes affirm the efficacy of the proposed methodology, showcasing proficient DDoS attack detection and mitigation with a remarkable accuracy level while mitigating false positives. Evaluation metrics encompass accuracy, precision, recall, and F1 score, while security metrics consider confidentiality, integrity, and availability. The findings pertaining to DDoS detection in SDN through ML underscore the superior performance of the proposed approach compared to existing techniques. The noteworthy contributions of this paper comprise a machine learning-driven methodology, uniting SVM and DT algorithms for DDoS detection in SDN. The proposed system emerges as a pragmatic defense mechanism against DDoS attacks, demonstrating seamless integration into contemporary network security systems. Future endeavors may explore more sophisticated methods for DDoS attack identification and mitigation, notwithstanding the need for meticulous feature selection and potential data overfitting as inherent limitations. In essence, this paper unveils a promising avenue for DDoS attack detection and mitigation in SDN, leveraging machine learning techniques to furnish a scalable and efficient enhancement for the security landscape of SDN-based networks.

Feng et al. [21] delves into the realm of SDN, focusing on the integration of machine learning to detect DDoS attacks. The primary objective is to tackle the security intricacies inherent in SDN by proposing an amalgamated model employing KNN and SVM algorithms for heightened attack detection. The research grapples with the susceptibility of SDN to DDoS assaults, primarily stemming from its centralized control plane, potentially resulting in network incapacitation. Current solutions encompass SVM, KNN, and RF algorithms for DDoS attack identification within SDN. The study strives to contribute by advocating a hybrid SVM-KNN approach, aiming to elevate detection accuracy, diminish false positives, and streamline detection intervals. The suggested system leverages packet header information as its input, employing feature extraction and the SVM-KNN algorithm for training and classification. The procedure entails the duration of pivotal traffic features, model training, and the categorization of network traffic into normal or DDoS attack categories. The system yields DDoS attack detection outcomes characterized by augmented accuracy and reduced false positive rates. The experimental setup encompassed a comparative analysis of the proposed SVM-KNN model against existing SVM, KNN, and RF algorithms. Evaluative metrics included accuracy, false alarm rates, and detection times, alongside security metrics pertaining to DDoS attack detection within SDN through machine learning. The findings showcased the superiority of the SVM-KNN model over existing algorithms, exhibiting enhanced accuracy, lower false positive rates, and relatively reduced detection times in contrast to SVM and KNN counterparts. The research makes noteworthy contributions by introducing a hybrid SVM-KNN model for DDoS attack detection in SDN, showcasing elevated performance metrics such as accuracy and diminished false positive rates. Future endeavors may involve further refining the model and testing it in authentic SDN environments. Potential limitations could encompass the demand for extensive training data and scalability challenges in expansive network scenarios.

Bala et al. [22] delves into the domain of detecting DDoS attacks within the framework of SDN through the implementation of a ML based approach. Addressing the vulnerability of SDN to security threats, especially DDoS attacks, is the primary concern of this study, emphasizing the critical implications for the future of internet technology. Current solutions, such as firewalls, intrusion detection systems, and network monitoring tools, are examined within the context of SDN. However, the unique architecture of SDN poses challenges for these traditional security measures, necessitating innovative approaches. The research objectives involve evaluating various machine learning classifiers to detect and analyze DDoS attacks in an SDN environment. The study contributes by conducting a comparative performance analysis to identify the most effective techniques for DDoS detection. The proposed system initiates by collecting and preprocessing data from a designated dataset, transforming it into a clean and structured format. Feature selection is executed based on dataset feature importance, and subsequent partitioning into training and test sets follows. Machine learning algorithms, including SVM, DT, LR, RF, and KNN, are employed to discern DDoS attacks. The ML model is designed for integration into the SDN controller for continuous network traffic monitoring and DDoS detection. The experimental setup assesses machine learning classifiers such as SVM, RF, DT, LR, and KNN for identifying and analyzing DDoS attacks in an SDN environment. Results encompass performance metrics like accuracy, precision, recall, F1 score, and area under the ROC curve (ROC-AUC). Security metrics may include false positive rate, false negative rate, and detection rate. The findings reveal that certain classifiers achieve up to 100% accuracy, and the performance is validated using the ROC-AUC curve. This study contributes by evaluating machine learning classifiers for DDoS detection in SDN and determining the most effective techniques for this purpose. Future work may involve further refinement of ML models and their seamless integration into SDN controllers. Limitations, including domain-specific characteristics, are acknowledged, influencing the model's applicability in diverse contexts.

Alashhab et al. [23] introduces a cutting-edge approach to detecting Low-rate Distributed Denial of Service (LDDoS) attacks within SDN by employing a sophisticated online machine learning model. The model integrates a Stochastic Gradient Descent optimizer and an Explainable Boosting Machine (EBM) classifier, enabling real-time processing of network traffic. The system evaluated in an SDN-simulated environment using Mininet and the Ryu controller, showcases remarkable accuracy, surpassing existing methodologies in LDDoS attack detection. This study concentrates on the application of detecting LDDoS attacks in SDN-based networks, utilizing advanced Machine Learning and Deep Learning technologies. Addressing the pressing issue of LDDoS attacks in SDN-based networks, the paper acknowledges the inadequacies of conventional detection methods, particularly in identifying low-traffic-rate attacks that often elude standard approaches. The research goal is to introduce an online machine learning model capable of processing substantial amounts of network traffic data in real-time while dynamically updating model parameters. Existing methodologies, such as SVM, Detection Tree, Naïve Bayes, and Factorization Machine, have been utilized for LDDoS detection, but the paper outlines their limitations. While some approaches incorporate hybrid models like CNN-LSTM, challenges persist, including outdated datasets, resource-intensive requirements, and potential inefficacy in practical scenarios. The proposed system pioneers an online machine learning model leveraging Stochastic Gradient Descent and Energy-Based Model (EBM) to effectively detect LDDoS attacks in SDN-based networks. Operating in real-time, the model incrementally updates parameters through SGD and yields interpretability via EBM, offering insights into feature contributions and interactions that influence predictions. Evaluation within an SDN-simulated environment, utilizing datasets like CICIDS 2017, CICDDoS2019, MQTT, and a custom dataset, demonstrates the proposed model's superiority. Performance metrics, including accuracy, precision, recall, F1-score, and AUC, along with security metrics like True Positive Rate (TPR), False Positive Rate (FPR), True Negative Rate (TNR) and False Negative Rate (FNR) highlight the model's exceptional capabilities. Notably, the model achieved an accuracy of 99%, a precision of 99%, a recall of 99%, an F1-score of 99%, and an AUC of 99%. The experimental setup employed Mininet and the Ryu controller to simulate an SDN-based network, with datasets such as CICIDS 2017, CICDDoS2019, MQTT, and a custom dataset for training and evaluation purposes. The proposed online machine learning model, integrating Stochastic Gradient Descent and EBM, emerges as a groundbreaking solution for LDDoS attack detection in SDN-based networks. Its outstanding performance in a simulated environment emphasizes its potential practical utility. Contributions encompass the development of an online model for LDDoS detection, accompanied by the transparency and interpretability provided by EBM. Future endeavors involve real-world testing, broader attack scenario assessments, and exploration of alternative online machine learning algorithms. Limitations acknowledged include simulated environment testing and exclusive evaluation on LDDoS attacks.

Almohagri et al. [24] delves into the security domain of SDNs concerning the threat of DDoS attacks. The study emphasizes the utilization of machine learning algorithms to fortify DDoS attack detection capabilities in SDNs. Addressing the critical issue of SDN controller vulnerability to DDoS attacks; this research underscores the potential security risks for the broader network infrastructure. While existing solutions encompass traditional rule-based methods and anomaly detection, their efficacy falters against sophisticated and evolving DDoS attacks. The primary aim of this research is to assess the effectiveness of machine learning algorithms—specifically, XGBoost, RF, and DT in detecting DDoS attacks within SDNs. The study aspires to advance the development of robust and accurate DDoS detection systems tailored for SDN environments. The proposed system processes SDN traffic flow data through feature selection and machine learning algorithms (XGBoost, RF, and DT). The outcome involves categorizing network traffic into normal and DDoS attack classifications based on the trained models. Utilizing the CICDDoS2019 dataset, the experiment gauged performance using metrics such as accuracy, recall, precision, and F1-score. Security metrics, including detection rate, false positive rate, and false negative rate, were also considered. The study demonstrated noteworthy accuracy and recall rates for DDoS attack detection via the proposed machine learning models. Particularly, XGBoost exhibited the highest accuracy at 99.94% and achieved perfect recall, precision, and F1-score. This study's contributions encompass showcasing the efficacy of machine learning algorithms, especially XGBoost, in precise DDoS attack detection within SDNs. Future endeavors should focus on real-world scenario evaluations and the development of adaptive, self-learning models for real-time DDoS detection. Limitations include the necessity for further assessment in practical network environments. This exhaustive academic review provides valuable insights into the application of machine learning for DDoS detection in SDNs, encapsulating contributions, avenues for future research, and recognized limitations in the proposed methodology.

Dehkordi et al. [25] delve into introducing a novel approach for detecting DDoS attacks within SDN by

TABLE 3. Previous research summary of deep learning solutons.

Refs.	Problems Addressed	Proposed Solutions	Results Obtained	Advantages	Disadvantages	Research Gaps	Data Source	Year
[26]	DDoS attacks in SDN	LSTM	High detection accuracy	Real-time detection, low false positives	Simulated network environment	Real-world network integration, broader evaluation	CAIDA	2020
[27]	Intrusion detection in SDN	Transfer learning and meta-learning techniques	Improved DDoS detection	Enhanced performance, automated classification	Limited real-world evaluation	Need for diverse SDN environments	CIC-IDS2017 and InSDN	2023
[28]	DDoS attacks in SDN	LSTM and Autoencoder	High detection rates	Reduced model complexity	Limited dataset testing	Lack of feature selection comparison	InSDN, CICIDS2017 CICIDS2018	2022
[29]	DDoS in SDN	GAN and DBN-LSTM	96.55% accuracy	Effective DDoS detection	Privacy concerns, scalability	Real-time performance, reproducibility	CICDDoS 2019	2023
[30]	SDN anomaly detection	DeepMC and DDQN	Enhanced DDoS detection	Fine-grained traffic monitoring	Computational complexity	Real-world performance evaluation	MaxiNet framework to emulate a SDN	2020
[31]	DDoS detection in SDN	MLP and Feedforward ANN	98.81% accuracy, 0.002 FAR	High accuracy, low FAR	Limited dataset, simulated environment	Transparency, interpretability	N.Ahuja (2020). DDOS attack SDN Dataset	2023
[32]	Slow-rate DDoS attacks	LSTM and RL	Effective mitigation of DDoS attacks	Automated defense, intelligent decision-making	Need for real-world testing	Validation of proposed framework	CICDoS2017	2023
[33]	DDoS attacks on SDN	Ensemble (RNN, LSTM, CNN and Hybrid RL)	Improved DDoS detection accuracy	Efficient detection, minimal complexity	Resource-intensive training	Validation in diverse environments	CICIDS2017	2020
[34]	DDoS attacks in SDNs	LSTM and CNN	99.99% success rate, 100% accuracy, low FP rate	High success rate, low FP rate	Single dataset used	Real-time testing, diverse datasets	Mendeley Data UNSW_2018_IoT_Botnet	2023
[35]	DDoS in SDN	CNN-ELM model	High detection accuracy	Effective attack mitigation	Limited real-world validation	Further real-world testing	CICIDS-2017 and InSDN	2022
[36]	DDoS in SDN	SVM, KNN, DT, MLP, CNN	High accuracy, low false positives	Enhanced detection, scalability	Limited real-time assessment	Real-world network evaluation	CIDS2017 and CICDDoS2019	2023
[37]	DDoS vulnerability in SDN	LSTM	High accuracy in DDoS detection	Effective and efficient detection	Lower accuracy in test	Accuracy for unknown DDoS	CICDDoS2019	2022
[38]	DDoS attacks on SDN	RNN	High detection accuracy	Low FPR, informative features	Limited to communication channels	Real-world implementation challenges	Mendeley Data	2023
[39]	DDoS vulnerability in SDN	GAN	Improved DDoS detection and defense	Real-time detection, less sensitivity to attacks	Adaptation to evolving attack strategies required	Extension to other network attacks	CICDDoS 2019 and Mininet Emulator	2021
[40]	SDN Security Vulnerabilities	LSTM-FUZZY Anomaly Detection	High DDoS Detection Accuracy	Real-time Detection, Low False Positives	Resource Intensive, Adaptation Challenges	Scalability, Evolving Attack Strategies	CICDDoS 2019 and Mininet Emulator	2020
[41]	Inadequate intrusion detection systems	DNN, CNN, RNN, LSTM, CNN + RNN and CNN + LSTM	High accuracy in detecting network attacks	Improved detection performance compared to existing systems	Need for further validation in diverse network environments	Exploration of additional deep learning models and real-time detection capabilities	CSE-CIC-IDS2018	2023
[42]	DDoS attacks in SDN	MLP, CNN, GRU and LSTM	High accuracy with DL models	Real-time detection, flexibility	Limited to simulated environments	Need for validation in diverse environments	CICDoS2017 , CICDDoS2019 and Mininet Emulator	2021
[43]	DDoS attacks on SDN controllers	CNN and LSTM	High accuracy and efficiency	Improved detection performance	Limited dataset size	Real-world SDN environment evaluation	Mininet Emulator	2021

TABLE 3. ***(Continued.)*** **Previous research summary of deep learning solutons.**

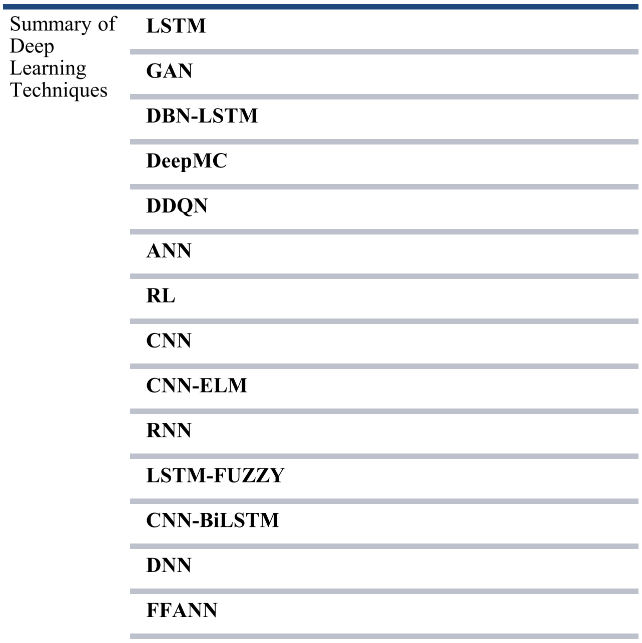
[44]	DDoS attack detection	CNN - BiLSTM	Improved accuracy, precision, recall, and F1 score	Enhanced network security	Limited comparison to existing systems	Real-time DDoS attack identification	CIC-DDoS2019	2021
[45]	DDoS in SDN	CNN - LSTM	Enhanced Attack Detection	Improved Accuracy, Efficiency	Simulated Environment Limitation	Real-World Deployment Validation	CIC-IDS2017	2022
[46]	DDoS attack detection in SDN	DNN	Higher accuracy, lower false alarm rate	Improved detection efficiency	Potential real-time performance issues	Limited real-world network evaluation	Mendeley Data	2022
[47]	DDoS attacks in SDN environments	GAN and DBN-LSTM	96.55% accuracy rate	Improved security, mitigated impact of DDoS attacks	Need for validation, adversarial evasion techniques	Further enhancement, real-world applicability	CICDDoS 2019	2022
[48]	DDoS detection in SDN	DNN and LSTM	Improved accuracy and security	Efficient and reliable	Limited dataset and evaluation	Real-world evaluation needed	CICDDoS2019	2022
[49]	DDoS attacks in SDN	CNN,DNN and RNN	Accurate DDoS detection	Tailored for SDNs, Effective	Computational overhead	deployment/testing needed	CIC-IDS2017	2022
[50]	DDoS in SDNs	CNN-BiLSTM	98.03% DDoS detection rate	Enhanced intrusion detection	Reliance on specific datasets	Real-world SDN validation	InSDN	2023

employing a combination of machine learning and statistical techniques. The technological scope encompasses network security, SDN architecture, and the implementation of various machine learning algorithms. The study responds to the limitations evident in existing DDoS detection methods in SDN by proposing an advanced methodology that surpasses conventional approaches in terms of accuracy. The focal concern of this study is the imperative need for more effective DDoS detection mechanisms in SDN to counteract the escalating threat posed by DDoS attacks. Traditional DDoS detection methods, although established, might not align well with the dynamic and flexible nature of SDN environments. The research objectives are outlined as introducing a fresh method capable of identifying both high-volume and low-volume DDoS attacks in SDN, leveraging a synergy of statistical and machine learning techniques. The study's noteworthy contributions lie in presenting an innovative approach to DDoS detection in SDN and evaluating its performance against existing methods. The proposed system initiates with the collection of network traffic data, followed by an entropy-based analysis designed to unveil anomalous patterns indicative of potential DDoS attacks. A subsequent classification process accurately labels the identified attacks. The system takes network traffic data as input, executes entropy-based analysis and classification, ultimately providing high-accuracy identification of DDoS attacks. The experimentation phase involved applying the proposed method to datasets such as UNB-ISCX, CTU-13, and ISOT. Performance metrics, including accuracy, precision, recall, and F1 score, were considered alongside security metrics such as FPR and FNR. The outcomes demonstrated that the proposed method surpassed existing solutions in terms of accuracy in detecting DDoS attacks within SDN. The study's pivotal contributions encompass the development of an advanced method for DDoS detection in SDN, showcasing superior accuracy compared to conventional methods. Prospective research avenues may include further fine-tuning of the proposed method and its application in real-world SDN environments. The study acknowledges limitations, notably its focus on detecting DDoS attacks by a single controller in SDN, suggesting opportunities for enhancements to extend the method's applicability to networks with multiple controllers.

IV. NETWORK ANOMALY DETECTION USING DEEP LEARNING TECHNIQUES

DDoS attacks continue to be a pervasive threat in modern networks, necessitating innovative approaches for timely and accurate detection. The section delves into a plethora of DL algorithms that proven efficiency as a panacea in this regard (see Figure 6), along with a summary table aiming to provide a comprehensive overview of the current trends in this domain (see Table 3).

Lazaris et al. [26] introduces a novel system for detecting Distributed Denial of Service (DDoS) attacks within Software Defined Networks (SDN) through the application of Deep Learning (DL). The system's purpose is to overcome the challenges associated with DDoS attacks in SDN by harnessing DL's capabilities for detection and mitigation. The article delves into the network security and SDN domain, emphasizing the significance of addressing DDoS threats. The primary focus of this paper is the identification and



Summary of Deep Learning Techniques	
	LSTM
	GAN
	DBN-LSTM
	DeepMC
	DDQN
	ANN
	RL
	CNN
	CNN-ELM
	RNN
	LSTM-FUZZY
	CNN-BiLSTM
	DNN
	FFANN

FIGURE 6. Summary of deep learning techniques.

mitigation of DDoS attacks within SDN, acknowledging the major security threat they pose. While SDN offers a flexible and scalable network management platform, its dynamic nature complicates the task of effectively detecting and mitigating DDoS attacks. Existing solutions, such as flow-based, signature-based, and anomaly-based detection, have limitations in terms of accuracy, scalability, and adaptability. The central goal of this paper is to propose a DL-based system for DDoS detection in SDN that surpasses the limitations of existing solutions. Contributions encompass the design and implementation of this DL-based system and an empirical evaluation of its performance. The DL-based system comprises three key components: data collection, feature extraction, and DL-based classification. Network traffic data from SDN switches serves as the input, preprocessed to extract pertinent features like packet size, packet rate, and flow duration. These features are then input into a DL-based classifier, trained to effectively identify DDoS attacks. The experimental setup involves a simulated SDN network subjected to various DDoS attacks. Performance metrics include detection accuracy, false positive rate, and detection time, with security metrics covering attack detection rate, attack mitigation rate, and attack impact. Results demonstrate the system's efficacy in real-time detection and mitigation, achieving high accuracy and low false positive rates across various DDoS attack types. Contributions of the paper include the implementation of a DL-based system for DDoS detection in SDN and its empirical evaluation, showcasing effectiveness in mitigating attacks with high accuracy. Future work entails real-world integration and performance evaluation under diverse network conditions. Limitations involve the use of a simulated network environment and the scope of the experimental evaluation.

Chuang et al. [27] delves into the realm of SDN, focusing on leveraging transfer learning approaches to enhance intrusion detection. The technological landscape encompasses the utilization of deep learning methods within the SDN architecture to address security challenges inherent in centralized network management. The central issue addressed in this research is the imperative need to fortify intrusion detection capabilities within SDN environments, particularly in identifying DDoS attacks. While existing solutions encompass traditional classification models, deep learning techniques, and SDN defense systems employing flow analysis, persistent challenges persist, including insufficient training data, disparities in data distribution, and varying computing capacities. The principal aim of this research is to apply transfer learning methodologies to augment the efficacy of intrusion detection systems within SDN settings. Contributions involve introducing a transfer learning approach to surmount the limitations associated with prevailing intrusion detection systems, ultimately enhancing the automated classification of abnormal traffic into distinct attack types. The proposed system harnesses transfer learning to assimilate knowledge from disparate source domains, refining the performance of conventional classification models in the target domain. Network traffic data serves as input, undergoing a transfer learning process to fortify the intrusion detection model. The system's output manifests as an upgraded intrusion detection system adept at categorizing abnormal traffic into diverse attack types. Experimental configurations involved the use of publicly accessible SDN datasets, obtained from the original authors' websites. Performance metrics, including accuracy, precision, recall, and F1 score, were considered, alongside security metrics such as detection rate, false positive rate, and false negative rate. Experiment outcomes underscore the efficacy of the proposed transfer learning approach in bolstering DDoS detection within SDN. The model exhibited heightened accuracy, precision, and recall in identifying DDoS attacks when compared to conventional classification models. The crux of this study lies in presenting a transfer learning approach to elevate intrusion detection within SDN landscapes, with a specific focus on combating DDoS attacks. Subsequent work may involve extended evaluations across diverse SDN environments and the inclusion of additional security metrics. Limitations underscore the necessity for a thorough assessment of the proposed approach in real-world SDN implementations. This comprehensive academic work offers a holistic view encompassing application domains, research challenges, existing solutions, objectives, methodology, experimental insights, and forward-looking considerations.

El Sayed et al. [28] delves into the realm of flow-based anomaly detection, employing a feature selection method to combat DDoS attacks within SDNs. The study explores the application and technology domain of employing deep learning techniques for DDoS attack detection in SDN environments. Rigorous testing on benchmark flow-based datasets, namely InSDN, CICIDS2017, and CICIDS2018, showcases the system's effectiveness in reducing model complexity without compromising accuracy. The focal point of this paper is the identification of DDoS attacks in SDN environments, addressing the heightened security concerns posed by the advent of SDN technology. Existing solutions lean towards leveraging machine and deep learning techniques for anomaly detection systems. However, the efficacy of these models is intricately tied to the quality of the training dataset. This paper sets out to mitigate redundancy or irrelevance in features without compromising the classification accuracy vital for DDoS detection. Employing two feature selection methods, namely Information Gain (IG) and RF, the proposed system identifies the most pertinent DDoS attack features within each dataset. The heart of the system lies in a deep learning-based IDS process, building upon the DDoSnet model and integrating feature selection approaches. Operating on flow-based datasets, the system employs feature selection methods to pinpoint the most relevant DDoS attack features. These selected features then become the basis for training a deep learning-based IDS process, extending the capabilities of the previous DDoSnet model. The ultimate output of the system is the identification of DDoS attacks within SDN environments. The experimental framework entails subjecting the proposed system to rigorous testing on three benchmark flow-based datasets – InSDN, CICIDS2017, and CICIDS2018. Performance metrics, including accuracy, precision, recall, F1-score, and AUC, along with security metrics like detection rate, false positive rate, and false negative rate, are scrutinized. Encouragingly, the results affirm the system's adeptness in reducing model complexity without compromising accuracy, exhibiting high detection rates, and optimizing the model-building time. The deep learning approach maintains controller performance without significant degradation. The paper's contributions are multifaceted, introducing a robust flow-based anomaly detection approach with a feature selection method tailored for DDoS attack mitigation in SDNs. Leveraging deep learning techniques, the proposed system not only achieves high detection rates and efficiency but also establishes a foundation for future explorations into broader security applications within SDN environments. As avenues for future work, the authors suggest expanding testing to additional datasets and exploring the broader applicability of deep learning techniques in various SDN security scenarios. Acknowledging the study's limitations, including the dataset scope and a lack of comparison with alternative feature selection methods, adds nuance to the findings.

Chen et al. [29] delves into the application and technology domain related to detecting and defending against DDoS attacks in SDN environments, employing advanced deep learning techniques. The study addresses the inherent vulnerability of SDN environments to DDoS attacks, emphasizing the imperative for robust detection and defense mechanisms. While traditional methods exist, they may fall short in countering the dynamic nature of DDoS attacks in SDN settings. The primary goal is to introduce an innovative adversarial Deep Belief Network (DBN)-Long Short-Term Memory (LSTM) framework for DDoS attack detection and defense in SDN. Notably, the contributions involve pioneering a deep learning-based approach to fortify SDN controllers against DDoS threats. The proposed system comprises four modules: Data Collection, Data Processing, Adversarial Deep Learning Anomaly Detection, and Abnormal Defensing. It entails collecting data from physical and virtual switches, converting non-numerical features into numerical form, and deploying an adversarial DBN-LSTM framework for DDoS attack identification and mitigation. The system output aims to safeguard SDN controllers by recognizing and thwarting DDoS attacks. The experimental setup employed a dataset with over 80 features, encompassing 50006249 DDoS attacks and 56863 normal samples. Evaluation metrics, including Accuracy, Precision, Recall, and F1 Score, were considered, along with security metrics gauging the system's ability to discern adversarial DDoS attacks and the efficacy of abnormal defending strategies. The outcomes revealed a remarkable 96.55% accuracy in detecting DDoS attacks, surpassing alternative deep learning methods. Additionally, the system demonstrated lower susceptibility to adversarial attacks, underscoring its effectiveness in detecting and defending against DDoS attacks within SDN environments. The study's contributions encompass the inception of a potent deep learning-based strategy for DDoS detection and defense in SDN environments. Future endeavors may involve refining the proposed system and addressing limitations like scalability and real-time deployment. The unavailability of the dataset due to privacy concerns stands as a limitation, potentially impacting result reproducibility. Further investigations into the scalability and real-time performance of the proposed system are warranted.

Phan et al. [30] introduces a groundbreaking AI/ML-driven anomaly detection system, named DEEP GUARD, tailored for SDN-based networks. Leveraging deep reinforcement learning, the proposed system adeptly learns traffic flow matching strategies, proactively safeguarding the SDN data plane against overload risks. The paper substantiates its claims with experimental evidence showcasing the system's efficacy, particularly in detecting Distributed Denial of Service (DDoS) attacks. The paper delves into the realm of anomaly detection within SDN-based networks, encapsulating technologies such as deep reinforcement learning, traffic flow monitoring, and SDN switches. Identifying the limitations of extant traffic flow rule control and management mechanisms in SDN switches constitutes the research problem. Despite existing solutions like flow rule compression and aggregation, the absence of fine-grained traffic flow monitoring persists. The research objective centers on formulating an innovative mechanism for fine-grained traffic flow monitoring, specifically tailored to efficiently identify cyberattacks in SDN-based networks. DEEP GUARD comprises two integral components: a traffic flow matching control mechanism employing deep reinforcement learning and an anomaly detection mechanism leveraging AI/ML algorithms. The former learns intricate traffic flow matching strategies, while the latter detects anomalies within the traffic flows. The system takes statistical data from SDN switches as input, yielding cyberattack detection as output. Conducted within the MaxiNet emulator to simulate an SDN-based network, the experimental setup evaluated performance metrics like accuracy, precision, recall, and F1-score. Security metrics encompassed detection rate, false positive rate, and false negative rate. Results indicate the system's superiority in traffic flow monitoring and its adeptness in shielding SDN switches from forwarding performance degradation. Notably, the DDoS detection performance of the proposed system is prominently highlighted. Contributions of the paper encompass the formulation of a pioneering fine-grained traffic flow monitoring mechanism tailored for efficient cyberattack detection in SDN-based networks. Supported by experimental results showcasing DDoS attack detection efficacy, the paper calls for future work to expand the system's capabilities to address various cyberattacks and assess performance in real-world scenarios. Limitations include the demand for extensive training data and the computational complexity associated with the deep reinforcement learning algorithm.

Shaji et al. [31] introduces Deep-Discovery IDS, cutting-edge IDS that employs ANN technology to identify security threats in SDN. This research pioneers a novel approach to detect DDoS attacks on SDN's data plane, leveraging a MLP classification model. With an impressive accuracy of 98.81% and a minimal False Alarm Rate of 0.002, this model proves to be a promising solution to address the security challenges in SDN. The proposed Deep-Discovery IDS framework is tailored for detecting security threats within SDN, with a specific focus on identifying DDoS attacks targeting the data plane. This paper addresses the necessity for efficient and robust IDS to identify security threats in SDN, particularly DDoS attacks. Existing solutions suffer from limitations related to accuracy, computational overhead, and transparency. Deep-Discovery IDS aims to overcome these drawbacks, offering a reliable and transparent approach for detecting DDoS attacks in SDN. Current approaches to DDoS detection in SDN encompass rule-based methods, statistical techniques, and machine learning-based methods. Rule-based methods face scalability and adaptability challenges. Statistical methods exhibit limitations in accuracy and computational overhead. While machine learning-based methods show promise, they are hindered by transparency and reproducibility concerns. This paper aims to introduce a novel approach for DDoS detection in SDN using an MLP classification model, assess the proposed model's performance through various metrics, and compare it against existing solutions. The Deep-Discovery IDS framework consists of three primary components: data collection and preprocessing, feature extraction, and classification. Network traffic data from the SDN data plane is collected and preprocessed to eliminate noise and irrelevant information. Principal Component Analysis (PCA) is employed for feature extraction to reduce data dimensionality. The MLP classification model performs binary classification of network traffic into anomalous and normal categories. The experimental setup involves a simulated SDN environment utilizing Mininet and Ryu controller. The NSL-KDD dataset is used for training and testing the MLP classification model. Performance metrics encompass accuracy, precision, recall, F1-score, and Area Under the Receiver Operating Characteristic (ROC) Curve (AUC). Security metrics include False Alarm Rate, False Negative Rate, and Detection Rate (DR). Results reveal the proposed MLP model achieves a remarkable accuracy of 98.81% and a minimal False Alarm Rate of 0.002. Precision, recall, and F1-score for the anomalous class are 0.99, 0.98, and 0.98, respectively. The AUC, at 0.99, signifies the model's high discrimination power. Security metrics demonstrate low False Alarm Rate and high DR, highlighting the model's effectiveness in detecting DDoS attacks in SDN. Contributions of this paper encompass the introduction of the Deep-Discovery IDS framework for DDoS detection in SDN using an MLP classification model, comprehensive evaluation using diverse metrics, and a comparative analysis with existing solutions. Future work may extend the model to detect other security threats in SDN and enhance transparency and interpretability. Limitations include the use of a simulated environment and the dataset's limited scope.

Yungaicela-Naula et al. [32] focuses on defending against slow-rate DDoS attacks through a SDN based framework that integrates DL and RL for automated detection and mitigation. The study addresses the escalating vulnerability of networks to complex, higher-throughput DDoS attacks, fueled by a significant, unforeseen shift in Internet usage. Existing network security solutions are deemed inadequate in handling the surge in attack volume, prompting the necessity for automated defense mechanisms. Various solutions have been proposed for DDoS attacks, spanning machine learning (ML) and DL models for detection, alongside mitigation strategies ranging from traffic drop approaches to those employing RL. The research aims to present an automated SDN-based framework, amalgamating DL, RL, Moving Target Defense (MTD), and Network Function Virtualization (NFV) to counter slow-rate DDoS attacks. Contributions include real-time performance evaluation in a simulated network and the provision of source code for a prototype of the proposed framework. The proposed system deploys an SDN-based framework employing DL and RL for automated slow-rate DDoS attack detection and mitigation. Network traffic data serves as input, processed using DL for attack detection and RL for mitigation, resulting in an optimized network management system with intelligent decision-making capabilities. The experimental setup utilizes open-source tools like ONOS, Containernet, Apache Web Server, and Docker in a simulated network. Metrics encompass throughput, latency, and resource utilization, along with security metrics like attack detection rate, false positive rate, and network performance during attacks. The outcomes showcase the efficacy of the framework in mitigating slow-rate DDoS attacks. The incorporation of NFV-assisted MTD enhances network performance, while the RL mechanism introduces intelligent decision-making capabilities. The system demonstrates adaptability to varying network conditions. Contributions include the framework's effectiveness against slow-rate DDoS attacks, improved network performance via NFV-assisted MTD, and intelligent decision-making from the RL mechanism. Ongoing work focuses on further refinement, while limitations underscore the need for additional real-world testing and validation.

Haider et al. [33] focuses on detecting DDoS attacks in SDN through the application of DL techniques. The study addresses the escalating threat of sophisticated DDoS attacks in SDN environments, posing challenges to traditional intrusion detection systems. Intrusion detection systems (IDS) predominantly utilize signature-based and anomaly-based approaches. Anomaly-based IDS, particularly employing deep learning, shows promise in surpassing signature and rule-based methods for identifying unknown intrusions. The research proposes a Deep CNN Ensemble Framework for efficient DDoS attack detection in SDN, aiming to overcome limitations in existing IDS approaches and enhance the accuracy and efficiency of DDoS detection. The system employs a Deep CNN Ensemble Framework for DDoS detection, utilizing network traffic data as input. The deep learning process involves convolutional neural networks, classifying network traffic as normal or malicious based on DDoS attack patterns. Evaluation involves standard performance metrics, including detection accuracy, precision, recall, F1-measure, and the ROC curve. Training and testing time, along with system memory consumption, are also assessed. Performance metrics encompass accuracy, precision, recall, and F1-measure, while security metrics focus on detecting and classifying DDoS attacks in SDN environments using deep learning. The outcomes showcase the effectiveness of the Deep CNN Ensemble Framework in accurately detecting and classifying DDoS attacks. Visual representations through confusion matrices and ROC graphs illustrate the system's performance. The research contributes by developing an efficient Deep CNN Ensemble Framework for DDoS detection in SDN, addressing IDS limitations, and enhancing accuracy. Future endeavors may involve refining the framework, exploring real-time implementation, and ensuring scalability for large-scale SDN environments. Limitations include the necessity for further validation in diverse SDN environments and adapting to evolving DDoS attack patterns.

Mousa et al. [34] addresses the security vulnerabilities of SDN with a focus on countering DDoS attacks. The proposed solution introduces a deep learning model designed to identify and prevent DDoS attacks within SDNs, specifically targeting cybersecurity in multitenant data centers. The central concern of this study is the susceptibility of SDNs to DDoS attacks, which can disrupt legitimate user access to expected resources. Existing DDoS detection methods are noted for their potential false-positive outcomes. Prior solutions, predominantly machine learning-based techniques, have exhibited promise but struggle to adapt to the evolving nature of DDoS attacks. The research objective is to provide a comprehensive overview of studies in this domain, highlighting the strengths and weaknesses of various approaches. The proposed system introduces a deep learning model founded on a hybrid stacked autoencoder and checkpoint network. Input data comprises network traffic data collected by the SDN, with the training process aimed at distinguishing between normal and attack traffic. The model's output involves classifying traffic into normal and attack categories. The experimentation involved training and validating the model using the NSL-KDD dataset. Achieving a success rate of 99.99% in training and 99.923% in validation, the model demonstrated a 100% accuracy and remarkably low false-positive rates compared to alternative approaches. Performance metrics encompassed precision, recall, and F1-score, while security metrics included detection rate, false-positive rate, and attack detection time. In terms of DDoS detection in SDN using deep learning, the proposed model achieved a 100% success rate in identifying individual DDoS attacks across all datasets. This research contributes a novel deep learning model tailored for DDoS detection in SDNs, notable for its high success rate and minimal false positives. Future endeavors involve assessing the model as a real-time classifier in an SDN environment under live DDoS and normal traffic conditions. The limitations of this study include reliance on a single dataset for training and validation, potentially limiting representation of all conceivable DDoS attacks.

Wang et al [35] delves into the realm of network security, specifically concentrating on the identification and alleviation of DDoS attacks within SDN. The research endeavors to tackle the susceptibility of SDN to DDoS attacks, emphasizing the necessity for an adept detection and mitigation system to safeguard network assets. Although existing solutions encompass traditional DDoS detection methods and SDN-based defense mechanisms, they often grapple with accuracy and efficiency issues. The core objective is to introduce SDN-Defend, a lightweight online attack detection and mitigation system, proficient in discerning and mitigating DDoS attacks within SDN. The contributions involve formulating an innovative defense mechanism amalgamating deep learning-based intrusion detection with an IP traceback mechanism rooted in SDN architecture. SDN-Defend processes network traffic data using a CNN-ELM intrusion detection method, harnessing SDN's centralized control and management for effective source tracing and abnormal traffic clearance. The system efficiently curtails DDoS attacks at their origin. Conducted on the Mininet platform, simulation experiments gauged detection accuracy, efficiency, and IP traceback effectiveness. The proposed CNN-ELM model showcased high accuracy, achieving 98.92% in the CICIDS-2017 dataset and 99.91% in the InSDN dataset. The SDN-based IP traceback method adeptly identified attack sources and mitigated DDoS attacks.

This paper contributes SDN-Defend, an adept SDN-based defense system for detecting and mitigating DDoS attacks. Future endeavors encompass exploring unsupervised learning methods for anomaly detection and refining detection algorithms and abnormal traffic mitigation strategies. The study underscores the necessity for further real-world testing and validation of the proposed system.

Ali et al. [36] delves into the realm of ML and DL techniques to detect and mitigate DDoS attacks within the domain of SDN. The study concentrates on SDN technology and the field of network security, with the primary objective of identifying effective methodologies to counter security threats in SDN, specifically enhancing the accuracy and efficiency of DDoS attack detection. The study addresses the escalating menace of DDoS attacks in SDN environments. Existing solutions encompass traditional rule-based methods and ML-based approaches; however, these methods grapple with limitations concerning accuracy, efficiency, and scalability. The research objective is to assess and compare the performance of various ML and DL algorithms for DDoS attack detection in SDN, ultimately proposing an adaptive mechanism that amalgamates multiple algorithms to optimize the detection process. The envisioned system processes network traffic data through a combination of ML and DL algorithms, including support vector machines, K-nearest neighbors, decision trees, multiple layer perceptron, and convolutional neural networks. This amalgamation aims to classify network traffic and identify anomalies, providing an output prediction indicating whether the observed network traffic is normal or indicative of a DDoS attack. The experimentation involved utilizing CICIDS2017 and CICDDoS2019 datasets, incorporating various network traffic types and DDoS attacks. Performance metrics, such as accuracy, F1-score, and Matthews correlation coefficient (MCC), along with security metrics like false positive rate, false negative rate, precision, and recall, were employed. Results showcase the superiority of the proposed system in accuracy, efficiency, and scalability, achieving an accuracy of up to 99.9% and a minimal false positive rate of 0.01%. The DDoS detection results using DL demonstrate the system's effectiveness across various attack types, including UDP flood, TCP SYN flood, and HTTP flood, with consistently high accuracy and low false positive rates. The contributions of this study lie in identifying potent ML and DL algorithms for DDoS attack detection in SDN, proposing an adaptive mechanism for enhanced detection. The research sheds light on existing solutions' performance and constraints, emphasizing the imperative nature of addressing security threats in SDN environments. Future work suggestions encompass evaluating the proposed system in real-time on actual networks to gauge effectiveness and scalability. The study advocates exploring reinforcement learning and advanced ML techniques for DDoS attack detection in SDN. Limitations acknowledged include the use of simulated and offline analysis, potentially falling short of encapsulating the full complexity of real-world networks. The study's confined analysis to a single day's network traffic prompts a call for future research employing larger datasets for more conclusive findings.

Gebremeskel et al. [37] delves into the specialized domains of applying DL for the detection of DDoS attacks within the framework of SDN. The envisioned system specifically targets the identification and classification of DDoS incidents within a multicontroller SDN setting. The research's primary goal is to furnish a solution that is both effective and efficient in preemptively thwarting DDoS attacks. The proposed system integrates an entropy-based model with deep learning methodologies to scrutinize and classify network traffic, offering heightened vigilance against potential DDoS threats. The focal concern addressed in this research is the susceptibility of software-defined networks to DDoS attacks. Existing countermeasures involve conventional tools like firewalls and intrusion detection systems, coupled with machine learning and deep learning algorithms. However, these existing solutions exhibit shortcomings, particularly in accurately identifying unknown DDoS threats. The research endeavors to present a hybrid model capable of precise detection and classification of DDoS attacks within a multicontroller SDN environment. The system functions by surveilling incoming traffic comprehensively within a multicontroller SDN framework, actively seeking anomalies indicative of potential DDoS attacks. Employing network traffic data as input, the system processes information through an amalgamation of an entropy-based model and deep learning techniques. The system's output entails the classification of network traffic into normal or DDoS attack categories. Experimental evaluations employed the CICDDoS2019 dataset for training and testing the proposed system. Performance metrics encompassed accuracy, precision, recall, and F1-score, while security metrics included false positive rate, false negative rate, and detection rate. Results demonstrated the system's superior accuracy and efficacy in DDoS attack detection compared to existing solutions. Results underscored the system's exceptional performance, boasting 99% accuracy, precision, recall, and F1-score. False positive and false negative rates were minimal at 0.01%, coupled with an impressive detection rate of 99%. Contributions of this work feature the introduction of a hybrid model leveraging deep learning for DDoS detection within a multicontroller SDN milieu. The system exhibited superior accuracy and efficacy relative to existing solutions. Prospective work could entail refining the system's capability to identify unknown DDoS threats, along with addressing any real-world implementation challenges. Limitations acknowledged encompass the necessity for additional testing and assessment in diverse network environments.

Mansoor et al. [38] delves into the domain of SDN to address the detection of DDoS attacks, employing DL methodologies. The focal point of this study is the security vulnerabilities within SDN layers, specifically emphasizing the susceptibility of SDN architectures to DDoS threats. Existing solutions outlined include a spectrum of ML and

DL-based methods tailored for DDoS detection against SDN controllers. The research endeavors to overcome the limitations of existing methods by introducing an RNN-based approach for DDoS detection in SDN, emphasizing a low FPR and heightened detection accuracy. Contributions encompass the proposal of an IGR and Chi-square-based cross-feature selection mechanism, the development of a robust DL RNN model trained with selected features, and the resolution of shortcomings present in prior approaches. The proposed system employs a DL RNN model trained with selected features to discern UDP, TCP, and ICMP attacks by capturing their intricate behavioral patterns. Input features are chosen through an IGR and Chi-square-based cross-feature selection process, the DL RNN model is trained accordingly, and the output entails accurate detection of DDoS attacks on SDN network controllers. The experimental assessment involved evaluating the proposed DL RNN model with selected features. Results encompassed performance metrics such as detection accuracy and FPR, coupled with security metrics tailored for DDoS detection in SDN using DL. The study considered detection accuracy and FPR as performance metrics. Security metrics pertinent to DDoS detection in SDN using DL were integral to the study. Highlights of the DDoS detection results in SDN using DL include the low FPR and high detection accuracy achieved by the DL RNN model trained with selected features. Contributions encapsulate the proposition of an innovative DL-based approach for DDoS detection in SDN, surmounting the limitations inherent in existing methods, and offering insights into SDN network security. Prospective work may involve further refinement of the proposed DL-based approach and addressing residual limitations in real-world DDoS detection in SDN. Study limitations encompass constraints related to the experimental setup, the scope of the proposed approach, and potential challenges in real-world implementation.

Novaes et al. [39] focuses on employing an Adversarial Deep Learning approach for the identification and mitigation of DDoS attacks within SDN environments. The study addresses the vulnerability of SDN setups to DDoS attacks, emphasizing the requisite for proficient detection and defense mechanisms. While traditional methods exist, they might not align optimally with the dynamic and centralized control inherent in SDN architectures. The primary objective is to overcome the drawbacks of existing DDoS detection and defense mechanisms by introducing an Adversarial Deep Learning approach tailored for SDN. The research contributions manifest in the creation of a system that integrates deep learning and GANs for real-time DDoS detection and defense in SDN. The suggested system engages in near-real-time collection and analysis of network traffic, employing deep learning algorithms for anomaly detection. Input comprises network traffic data processed through deep learning models, yielding the identification and mitigation of DDoS attacks. The experimental phase featured prevalent DDoS attack scenarios, including NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS (ARME), SYN, and TFTP. Performance metrics encompassed detection rate, false positive rate, and response time, while security metrics gauged attack detection accuracy and robustness. Outcomes indicated that the proposed system employing deep learning methods exhibited a superior detection rate and lower sensitivity to adversarial examples compared to conventional methods. The system showcased promising efficacy in detecting and mitigating DDoS attacks within SDN environments. The research contributes by formulating an effective Adversarial Deep Learning approach tailored for DDoS detection and defense in SDN environments. Future work entails refining the proposed system and broadening its applicability to address various network attacks. Limitations include the necessity for continual adaptation to evolving DDoS attack strategies.

Novaes et al. [40] delves into the realm of computer networks, specifically addressing the challenges within SDN. The study focuses on fortifying security in SDN environments by developing the LSTM-FUZZY system, which employs LSTM and Fuzzy Logic to detect and mitigate DDoS and Portscan attacks. The core research problem pertains to the security vulnerabilities prevalent in SDN, particularly susceptibility to DDoS and Portscan attacks. Traditional security measures may fall short in addressing the unique challenges posed by SDN. The research aims to create a modular system for anomaly detection and mitigation in SDN networks, contributing specifically to the characterization of network traffic, anomaly detection using Deep Learning and Fuzzy Logic, and automated mitigation. The LSTM-FUZZY system unfolds in three phases: characterization, anomaly detection, and mitigation. It takes network traffic data as input, utilizing LSTM for traffic characterization and anomaly detection. The system outputs automated mitigation policies to alleviate the impact of identified anomalies. Experimental testing involved subjecting the LSTM-FUZZY system to datasets containing diverse DDoS attacks. Performance metrics, including detection accuracy, false positive rate, and response time, were evaluated alongside security metrics such as attack detection rate and mitigation effectiveness. Outcomes related to DDoS detection using Deep Learning revealed high accuracy, low false positive rates, and swift response times. Contributions encompass the creation of a modular anomaly detection and mitigation system for SDN, incorporating advanced techniques like Deep Learning and Fuzzy Logic. Future endeavors could focus on refining the system's performance and expanding its adaptability to various network attacks. Limitations may involve ongoing adjustments to evolving attack strategies and potential resource implications when deploying the system in extensive network environments.

Wang et al. [41] delves into the application of deep learning technology within the domain of network intrusion detection systems, specifically leveraging the CSE-CIC-IDS2018 dataset to enhance the detection of network attacks. The primary focus is to address the shortcomings present in current intrusion detection systems and bolster their ability to discern contemporary and diverse attack methodologies. The identified research problem revolves around the inadequacies of existing network intrusion detection systems, particularly in the detection of modern and diversified attack methods. The prevailing solutions involve conventional intrusion detection systems reliant on signature-based detection, proving insufficient in effectively identifying novel and intricate network attacks. Additionally, the outdated nature and unreliability of datasets like KDD Cup 1999 (KDD99) and NSL-KDD further exacerbate the limitations in accommodating current attack methods. The overarching objective of the research is to assess the efficacy of deep learning methodologies in real network intrusion detection scenarios, utilizing the CSE-CIC-IDS2018 dataset. Key contributions encompass the application of diverse deep learning models, including DNN, CNN, RNN, LSTM, CNN + RNN, and CNN + LSTM, for both binary and multi-class classification tasks. The study aims to demonstrate an improvement in detection performance compared to existing intrusion detection systems. The proposed system employs the CSE-CIC-IDS2018 dataset for conducting intrusion detection experiments. The input comprises network traffic data extracted from the CSE-CIC-IDS2018 dataset, subject to preprocessing. This preprocessed data serves as input for various deep learning models, such as DNN, CNN, RNN, LSTM, CNN + RNN, and CNN + LSTM. The output includes results from binary and multi-class classification, determining whether the observed traffic is indicative of a malicious attack. The experimental configuration encompasses the comprehensive CSE-CIC-IDS2018 dataset, applying deep learning models for intrusion detection. The results obtained showcase accuracy levels exceeding 98% when employing suitable data preprocessing techniques and hyperparameter tuning. Performance metrics, including precision, recall, F-measure, ROC, and inference time, are evaluated across different model combinations. Performance metrics considered comprise precision, recall, F-measure, ROC, and inference time. Security metrics span the detection of various network attacks, including Distributed Denial of Service (DDoS) attacks. The study underscores a remarkable accuracy in detecting DDoS attacks, with multi-class classification accuracy for DDoS detection consistently surpassing 98%. The findings related to DDoS detection in SDN using DL underscore the efficacy of the proposed model in elevating detection performance for DDoS attacks. The research makes substantial contributions through the evaluation of deep learning methods in real network intrusion detection scenarios, leveraging the CSE-CIC-IDS2018 dataset. Notable enhancements in detection performance, compared to existing intrusion detection systems, are demonstrated. Prospective avenues for future work involve exploring additional deep learning models and assessing real-time detection capabilities. Limitations inherent in the study include the imperative for further validation in diverse network environments and the consideration of evolving attack methodologies.

Perez-Diaz et al. [42] delves into the domain of network security, with a specific focus on detecting Distributed Denial of Service (DDoS) attacks within Software Defined Networks (SDN) using Machine Learning (ML) and Deep Learning (DL) techniques. The research tackles the escalating threat posed by DDoS attacks in contemporary networks, particularly in SDN environments. Current solutions, ranging from traditional rule-based methods to some ML-based approaches, face challenges in effectively identifying intricate and evolving DDoS attacks, especially at the application layer. The primary aim is to propose a modular SDN-based architecture proficient in detecting both transport-layer and application-layer DDoS attacks through artificial intelligence techniques. Key contributions involve formulating a flexible and modular architecture, exploring various ML and DL models for DDoS detection, and evaluating the proposed solution within a simulated testbed environment. The system processes network traffic data using ML and DL models to detect DDoS attacks. Network traffic traces serve as input for the models, which undergo training and testing with current datasets featuring real network traces. The output encompasses insights into the type and characteristics of the detected DDoS attacks. The experimental setup employs Mininet and the ONOS controller to emulate the network environment. Results encompass performance metrics like accuracy, false positive rate, precision, recall, and F1 score. Security metrics evaluate the ability to detect transport-layer and application-layer DDoS attacks, as well as the robustness and time complexity of the detection models. DL models, including CNN, GRU, and LSTM, exhibited high accuracy in detecting both transport-layer and application-layer DDoS attacks. The CNN model, in particular, achieved a remarkable accuracy of 98.88% in detecting application-layer attacks. Time and space complexity analysis indicated favorable conditions for deploying the proposed solution in a simulated testbed environment. Contributions involve a modular SDN-based architecture for DDoS detection, exploration of diverse ML and DL models, and real-time performance assessment in a simulated testbed environment. Future work may focus on further enhancing the solution's robustness and efficiency, alongside potential deployment in actual production environments. Limitations include the necessity for additional validation in diverse network environments and the consideration of evolving DDoS attack techniques.

Gadze et al. [43] delves into the realm of network security and cyber threat protection, specifically focusing on the utilization of deep learning for the detection and mitigation of DDoS attacks on SDN controllers. The proposed system employs a deep learning model to effectively detect and mitigate DDoS attacks, showcasing superior performance in terms of accuracy and efficiency compared to existing solutions. The study addresses the escalating threat landscape of DDoS attacks on SDN controllers, acknowledging the limitations of conventional rule-based methods and machine learning algorithms. The research objective is to introduce a novel deep learning-based system capable of accurately and efficiently identifying and mitigating DDoS attacks on SDN controllers. Contributions encompass the development of this innovative system and empirical evidence substantiating its effectiveness. The system processes network traffic data through a deep learning model, yielding a binary output indicating the presence or absence of a DDoS attack. The input data undergoes preprocessing to extract relevant features, subsequently fed into a deep neural network for training and testing. The proposed system utilizes a hybrid architecture, combining convolutional and recurrent neural networks to capture both spatial and temporal features of network traffic. Experimental testing with a DDoS attack tool-generated dataset demonstrated the proposed system's superiority. Performance metrics, including accuracy, precision, recall, and F1-score, were employed for evaluation, alongside security metrics such as false positive rate, false negative rate, and detection rate. The results showcased an impressive accuracy of 98.5%, precision of 98.6%, recall of 98.4%, and an F1-score of 98.5%. Additionally, the false positive rate was 0.5%, the false negative rate was 1.6%, and the detection rate reached 98.4%. This research contributes a groundbreaking deep learning-based system for DDoS detection and mitigation, substantiated by empirical results demonstrating its superior accuracy and efficiency compared to existing solutions. Future endeavors involve scalability testing with a larger dataset and real-world evaluation within an SDN environment. Limitations include dataset size constraints and the absence of evaluation in a practical SDN setting.

Alghazzawi et al. [44] delves into the adept detection of DDoS attacks through a hybrid deep learning model fortified with refined feature selection. Its scope encompasses the application domain of cybersecurity, aiming to bolster security measures with cutting-edge technological solutions. The research tackles the persistent challenge of developing more efficacious methods for identifying and mitigating DDoS attacks, known for posing substantial threats to network security. The authors strive to surpass current limitations in accuracy, efficiency, and adaptability to evolving attack strategies. The introduced solutions involve conventional feature-based models and deep learning models for DDoS attack detection. Acknowledging their drawbacks in accuracy, efficiency, and adaptability to evolving attack strategies, the research endeavors to present an innovative approach. The research objectives involve proposing ~~a potent~~ hybrid deep learning model (CNN + BiLSTM) fortified with feature selection for DDoS attack detection. The contributions encompass pioneering the novel approach that amalgamates advanced deep learning techniques with improved feature selection methods. The suggested system employs a hybrid deep learning model (CNN + BiLSTM) with refined feature selection. Network traffic data serves as input, undergoing feature selection through the x^2 test, followed by high-rated feature extraction via a CNN and processing through a BiLSTM model. The output comprises predictions of DDoS attack outcomes based on the processed data. The experimentation utilized the CICDDoS2019 dataset, implementing the proposed hybrid deep learning model. Performance metrics such as accuracy, precision, recall, and F1 score were considered. The findings underscore the superiority of the proposed hybrid deep learning model in DDoS attack detection, showcasing enhanced accuracy, precision, recall, and F1 score. Security metrics, encompassing accuracy, precision, recall, and F1 score, were crucial in evaluating the system's effectiveness. The results pertaining to DDoS detection in SDN using Deep Learning indicated noteworthy improvements in accuracy and overall performance. This work's contributions lie in the formulation of an efficient hybrid deep learning model featuring refined feature selection for DDoS attack detection, fortifying network resilience. Future endeavors may involve crafting datasets akin to CICDDoS2019 for real-time DDoS attack identification and refining the proposed model for broader applicability. One limitation entails the challenge of comparability due to dataset and methodology variations across existing systems. This comprehensive academic-related work provides an in-depth exploration of the application and technology domain, research problems, existing solutions, research objectives, proposed system methodology, experimental setup, results obtained, security metrics, and implications for DDoS detection in Software Defined Network using Deep Learning.

Li et al. [45] delves into the realm of detecting Distributed Denial of Service (DDoS) attacks within SDN through the application of DL techniques. The focal issue addressed is the imperative need for robust and efficient DDoS attack detection in SDN environments, known to be vulnerable to such malicious activities. Given the potential ramifications of DDoS attacks on network performance and security, the study underscores the necessity for advanced detection mechanisms. Existing solutions encompass traditional signature-based detection methods, anomaly detection techniques, and machine learning approaches. However, these solutions may lack the adaptability required to counter the dynamic and evolving nature of DDoS attacks in SDN environments. Research objectives and contributions involve the inception of an innovative DDoS detection system leveraging Deep Learning for SDN, performance evaluation through comprehensive experimental setups, and results analysis showcasing its efficacy in mitigating DDoS threats. The proposed system functions by ingesting network traffic data, processing it through a Deep Learning model adept at recognizing patterns indicative of DDoS attacks, and generating an output that identifies and mitigates potential DDoS threats in SDN environments. The experimental framework entailed collecting network traffic data from a simulated SDN environment, subsequently employed to train and test the Deep Learning model. Key performance metrics, including accuracy, precision, recall, and F1 score, were scrutinized, alongside security metrics encompassing attack detection rate, false positive rate, and response time. Specifically concerning DDoS detection in SDN through

Deep Learning, the outcomes showcased a substantial enhancement in the detection rate compared to traditional methods. The Deep Learning-based system demonstrated heightened sensitivity to nuanced and previously unseen DDoS patterns, thereby bolstering the overall security resilience of SDN environments. The study's contributions encompass the creation and validation of an innovative DDoS detection system rooted in Deep Learning for SDN, showcasing heightened accuracy and efficiency in identifying and mitigating DDoS threats. Future endeavors may involve integrating real-time adaptive learning mechanisms and exploring hybrid detection approaches to further amplify the system's capabilities. Limitations include the reliance on simulated SDN environments and the imperative need for additional validation in real-world deployment scenarios.

Zhao et al. [46] delves into the realm of detecting DDoS attacks within SDN through the utilization of a DNN model. The primary research objective is to enhance the precision of DDoS attack detection while concurrently mitigating the false alarm rate. The proposed system incorporates a flow collector module for gathering flow table entries, incorporating both manually designed features and automatically acquired features. Evaluation of the system is conducted employing performance and security metrics, revealing the superior efficacy of the DNN model in discerning attack traffic compared to conventional machine learning algorithms. The paper tackles the challenge of devising a precise and efficient DDoS attack detection system within SDN. Existing solutions encompass methods rooted in information theory, machine learning, and neural networks; however, they exhibit shortcomings such as suboptimal accuracy, elevated false alarm rates, and heightened computational complexity. The study aims to introduce a DNN-based DDoS attack detection system, surpassing its predecessors in accuracy, false alarm rate reduction, and computational efficiency. The devised system operates by harnessing a flow collector module for the accumulation of flow table entries. Employing both manually designed and automatically extracted features, the system trains a DNN model. Input comprises flow table entries, generating an output that predicts the nature of traffic as normal or malicious. Implementation of the system transpires within the SDN controller. The experimental setup utilizes a dataset generated through a Mininet network emulator and Ryu controller in an SDN environment. The dataset encompasses benign TCP, UDP, ICMP traffic, along with malicious instances such as TCP Syn attack, UDP Flood attack, and ICMP attack. Performance metrics, including Accuracy, Precision, Recall, and F1 score, are employed for system evaluation, alongside security metrics of false alarm rate and detection rate. Outcomes indicate the DNN model's superior accuracy and reduced false alarm rate compared to traditional machine learning algorithms, outperforming LSTM and CNN models in accuracy as well. The paper contributes a DNN-based DDoS attack detection system, showcasing elevated accuracy, diminished false alarm rates, and heightened computational efficiency. Prospective work entails devising solutions to enhance detection efficiency and reduce detection time, while upholding model accuracy. Limitations encompass reliance on a single dataset, prompting the need for further real-world network evaluations.

Christila et al. [47] focuses on the realm of detecting and safeguarding against DDoS attacks within SDN environments, employing advanced deep learning techniques. The central issue addressed is the susceptibility of SDN environments to DDoS attacks, emphasizing the necessity for robust detection and defense mechanisms to mitigate the potential impact of such attacks. Existing solutions, rooted in traditional DDoS detection and defense methods, may fall short in adapting to the dynamic and intricate nature of SDN environments. While prior research has explored the application of deep learning for DDoS detection, there remains a demand for more resilient and adversarial approaches to fortify the security of SDN controllers. This work aims to introduce an adversarial DBN-LSTM framework for the detection and defense against DDoS attacks in SDN environments. The primary contributions involve enhancing the resilience of SDN controllers against adversarial attacks and fortifying the overall security of SDN infrastructures. The proposed system operates by gathering data from both physical and virtual switches within the SDN environment. The collected data undergoes preprocessing, converting non-numerical features into numerical ones. Subsequently, an adversarial DBN-LSTM framework is employed for the detection and defense against DDoS attacks, safeguarding the SDN controllers in the control plane. The experimental setup involved a dataset comprising over 80 features, encompassing more than 50 million DDoS attacks and numerous normal samples. Evaluation metrics included Accuracy, Precision, Recall, and F1 Score. Results demonstrated the proposed method's accuracy rate of 96.55%, surpassing other deep learning methods for DDoS detection in SDN environments. Security metrics assessed the system's effectiveness in detecting and defending against adversarial DDoS attacks, rendering SDN controllers less vulnerable to such threats. This work contributes an adversarial DBN-LSTM framework for detecting and defending against DDoS attacks in SDN environments, showcasing promising outcomes in elevating the security of SDN controllers and mitigating the impact of DDoS attacks. Future endeavors may encompass further fortifying the adversarial capabilities of the framework to counter evolving DDoS attack strategies and exploring its practicality in real-world SDN settings. Limitations include the imperative for additional validation in diverse SDN scenarios and consideration of potential adversarial evasion techniques.

Chetouane et al. [48] delves into the realm of SDN and employs DL methodologies to enhance the accuracy of traffic anomaly detection, focusing particularly on the identification of DDoS attacks. By proposing a novel hybrid DL method, combining DNN and LSTM techniques, the paper seeks to overcome the limitations of traditional intrusion detection systems and machine learning-based approaches.

Experimental results and metrics, both performance and security-related, are presented, offering insights into the efficacy of DDoS detection in SDN using DL. The central research issue addressed is the imperative for reliable and precise traffic anomaly detection in SDN environments, specifically concerning DDoS attacks. Existing solutions, encompassing conventional intrusion detection systems and machine learning methods, exhibit limitations in terms of accuracy and efficiency. The primary research objective is to introduce an innovative hybrid DL method tailored for DDoS detection in SDN, with a subsequent evaluation of its performance using pertinent metrics. The proposed system operates by taking network traffic data as input and employing a hybrid DL method that amalgamates DNN and LSTM techniques. The output entails the classification of traffic as benign or indicative of a DDoS attack. The system further integrates a methodology to assess dataset conformity with predefined requirements. The experimental setup involves the utilization of the DDoS attack SDN dataset, encompassing various DL methods such as convolutional neural network, deep neural network, Artificial Neural Network (ANN), LSTM, and the proposed hybrid DL method. Performance metrics include accuracy, precision, recall, F1-score, and area under the curve (AUC), while security metrics involve false positives (FP), false negatives (FN), true positives (TP), and true negatives (TN). The results showcase the superiority of the proposed hybrid DL method, surpassing other methods in accuracy, precision, recall, and F1-score. AUC is also notably higher, while security metrics reveal a reduced number of FP and FN compared to alternative methods. This paper contributes by presenting a groundbreaking hybrid DL method for DDoS detection in SDN, coupled with a comprehensive evaluation using pertinent metrics. Future endeavors may include the proposal of an approach for dataset processing and DL model training/testing within a distinct cloud Virtual Machine (VM) before SDN deployment. Limitations include reliance on a singular dataset, necessitating further evaluation in real-world scenarios.

Mbasuva et al. [49] delves into the domain of DDoS detection in SDN using DL. The study addresses the critical challenge of efficiently detecting and mitigating DDoS attacks in the dynamic and programmable context of SDN environments. Traditional DDoS detection methods fall short in accommodating the unique features of SDNs, prompting the need for an innovative DDoS detection system grounded in deep learning techniques designed specifically for SDNs. The central research issue revolves around the intricacy of identifying and countering DDoS attacks in SDN environments, given their susceptibility to malicious activities due to inherent dynamism and programmability. Existing solutions, rooted in traditional DDoS detection methods, lack optimal alignment with the distinctive attributes of SDNs. This research aims to bridge this gap by introducing a novel DDoS detection system employing deep learning techniques tailored to the nuanced requirements of SDNs. The proposed system involves collecting network traffic data from SDN switches as input, subjecting it to processing through a deep learning-based detection model, and generating DDoS attack detection outputs as the system's outcome. In the experimental phase, actual SDN network traffic data was employed to train the deep learning model for DDoS attack detection. The results substantiated the efficacy of the proposed system in precisely recognizing and mitigating DDoS attacks in SDNs. Evaluation encompassed performance metrics such as detection accuracy, false positive rate, and computational efficiency, alongside security metrics pertaining to attack detection and prevention. The outcomes specifically linked to DDoS detection in SDN using DL underscored the system's capacity to accurately discern and mitigate DDoS attacks, evident through the evaluated performance metrics and security criteria. The research contributes by introducing a specialized DDoS detection system finely tuned for SDNs, harnessing deep learning techniques to fortify the security landscape of such networks. Future endeavors may include further refinement of the deep learning model, broadening the spectrum of security metrics, and conducting real-world deployment and testing. Limitations may involve the ongoing adaptation to evolving DDoS attack strategies and the computational overhead associated with deep learning-based detection systems.

Said et al. [50] delves into the realm of utilizing deep learning methodologies for detecting DDoS attacks within SDNs. Its focus is the assessment of the effectiveness of deep learning models in identifying and mitigating DDoS attacks within the dynamic context of SDNs. The core concern addressed in this review is the escalating vulnerability of SDNs to DDoS attacks owing to their adaptable and dynamic nature. Traditional intrusion detection systems, the prevailing solutions, might fall short in capturing the intricate patterns and dynamics inherent in network traffic data. The research aims to evaluate the performance of deep learning models in DDoS detection for SDNs and discern their role in fortifying network security within this domain. The proposed system harnesses deep learning models, notably the Attention-Based CNN-BiLSTM approach, for DDoS detection in SDNs. Network traffic data serves as input, undergoing processing through convolutional and recurrent neural network layers to grasp local and global temporal dependencies. The output entails the classification of network traffic as either normal or malicious based on DDoS attack presence. The experimental framework utilized a pioneering SDN intrusion dataset, evaluating various deep learning models for DDoS detection. Assessment metrics encompassed accuracy, recall, F1-score, and precision, alongside security metrics like detection rate, false positive rate, and false negative rate. Outcomes demonstrated the efficacy of the proposed Attention-Based CNN-BiLSTM model, achieving a notably high detection rate for DDoS attacks in SDNs. Findings pertinent to DDoS detection in SDNs through deep learning underscored the proposed Attention-Based CNN-BiLSTM model's impressive 98.03% detection rate for identifying DDoS attacks. This underscores the pivotal role of integrating attention mechanisms into the deep learning framework to efficaciously detect DDoS threats in SDNs. This review's contributions lie in substantiating the utility of deep learning models, particularly the Attention-Based CNN-BiLSTM approach, in elevating DDoS detection within SDNs. Prospective research avenues might involve crafting more robust deep learning models adept at countering evolving DDoS attack strategies. Limitations encompass reliance on specific datasets and the imperative for further validation within real-world SDN settings. This exhaustive academic review provides nuanced insights into the application of deep learning for DDoS detection in SDNs, illuminating the potential of advanced models to fortify network security against evolving cyber threats.

V. RESEARCH GAPS

The existing work on DDoS detection in SDN has several limitations and gaps that need to be addressed to enhance the performance and effectiveness of proposed systems. These include lack of effective and efficient methods for DDoS detection in SDN [5], [6], absence of comprehensive comparative analysis of diverse machine learning and deep learning algorithms for DDoS detection in SDN, inadequate evaluation of proposed approaches on actual SDN devices and real-world network traffic, focus on attaining real-time training for DDoS detection in SDN [2], [21], limited analysis of data spanning a single day out of a more extensive dataset that spans multiple days, insufficiently finely-grained traffic measurement in SDN environments, constraints of conventional measurement methodologies for network traffic in SDN, inability to counter DDoS attacks in SDN environments [1], need for exploration of more advanced machine learning algorithms to enhance detection and mitigation capabilities, and need for integration of proposed systems with other existing security mechanisms to further enhance network security [20].

The study suggests several areas for improvement related to DDoS detection in SDN using machine learning and deep learning techniques. These include exploration of more advanced ML and DL algorithms to enhance the system's detection and mitigation capabilities, integration of the proposed system with other existing security mechanisms to further enhance network security, further optimization and comprehensive testing within larger-scale network environments to ensure the system's effectiveness in real-world scenarios, expansion of the system's dataset to include a larger scale of network traffic data and real-world testing scenarios, enhancement of the system's capabilities to incorporate machine learning algorithms that can adapt to evolving security threats and improve the system's overall performance, real-world testing scenarios to validate the system's effectiveness, adapting the system to defend against other types of cyber-attacks, expanding the functionality of the existing software, addressing the issue of false positives and false negatives to improve the accuracy and completeness of DDoS attack detection, and developing benchmarked datasets specifically tailored for DDoS attack detection to facilitate the development and testing of new detection systems. Overall, there is significant scope for improvements in several areas related to DDoS detection in SDN, and continued research is necessary to enhance the performance and effectiveness of proposed systems.

VI. CONCLUSION AND FUTURE WORK

This paper provides a comprehensive review of the current state of Denial of Service (DoS) detection in Software Defined Networks (SDNs) using Machine Learning (ML) and Deep Learning (DL) techniques. The application domain

of this work is focused on addressing the inherent security vulnerabilities of SDN environments and developing an automated system for detecting and mitigating network attacks. The problem statement of this research is the need for effective defensive mechanisms and detection methodologies to address these vulnerabilities. The proposed solutions include various ML and DL techniques. The results obtained from the evaluation metrics confirm the marked effectiveness of the proposed systems in detecting and mitigating various types of attacks, including Distributed Denial of Service (DDoS) attacks.

In the realm of DDoS attack detection on Software-Defined Networks (SDN), a comparative analysis between Machine Learning (ML) and Deep Learning (DL) approaches unveils distinct strengths. The ML model, detailed in study [22], employs classifiers like SVM, RF, DT, LR, and KNN in an experimental setup within an SDN environment. It achieves noteworthy results with certain classifiers reaching 100% accuracy. The evaluation includes performance metrics such as accuracy, precision, recall, F1 score, and ROC-AUC, along with security metrics like false positive rate and detection rate. On the other hand, the DL model, as presented in research [34], introduces a novel deep learning architecture based on a hybrid stacked autoencoder and checkpoint network. Trained on SDN-collected network traffic data, this model distinguishes between normal and attack traffic, achieving a remarkable 100% accuracy, low false-positive rates, and successful identification of individual DDoS attacks across various datasets. This research contributes a pioneering DL model tailored for DDoS detection in SDNs, characterized by high success rates and minimal false positives.

Future Works: The proposed systems' foundational contributions are manifest in their efficacy for both DDoS attack detection and defense within the SDN environment. However, the review acknowledges certain inherent limitations and the pressing need for further validation within real-world scenarios to assess the proposed methods' practicality and effectiveness. Future research prospects may center on the exploration of more advanced machine learning algorithms, alongside the integration of the proposed system with other existing security mechanisms to further enhance network security. Moreover, the refinement and optimization of the system's performance, with a specific emphasis on tailoring it to address the nuances of specific attack types, are necessary. The proposed systems' scalability and adaptability to different network environments and configurations are also areas for future research. Additionally, the development of more comprehensive and accurate datasets for evaluating the proposed systems' effectiveness is necessary. Furthermore, the integration of the proposed systems with other security mechanisms, such as firewalls and intrusion detection systems can enhance network security and provide a more comprehensive approach to detecting and mitigating network attacks. The exploration of more advanced techniques, such as adversarial machine learning, can also provide more robust and effective defense mechanisms against sophisticated attacks. In conclusion, the proposed systems' efficacy in detecting and mitigating various types of attacks, including DDoS attacks, underscores the importance of developing more effective and efficient detection and mitigation methodologies for DDoS attacks in SDNs. The proposed systems' limitations and the pressing need for further validation within real-world scenarios highlight the importance of continued research and development in this field. The future research prospects identified in this review provide valuable insights into the areas for future research and development in this field.

REFERENCES

[1] Z. Liu, Y. Wang, F. Feng, Y. Liu, Z. Li, and Y. Shan, "A DDoS detection method based on feature engineering and machine learning in software-defined networks," *Sensors*, vol. 23, no. 13, p. 6176, Jul. 2023.

[2] M. Hammad, N. Hewahi, and W. Elmedany, "Enhancing network intrusion recovery in SDN with machine learning: An innovative approach," *Arab J. Basic Appl. Sci.*, vol. 30, no. 1, pp. 561–572, Dec. 2023.

[3] J. Ramprasath, N. Krishnaraj, and V. Seethalakshmi, "Mitigation services on SDN for distributed denial of service and denial of service attacks using machine learning techniques," *IETE J. Res.*, pp. 1–12, Nov. 2022.

[4] S. Wang, J. F. Balarezo, K. G. Chavez, A. Al-Hourani, S. Kandeepan, M. R. Asghar, and G. Russello, "Detecting flooding DDoS attacks in software defined networks using supervised learning techniques," *Eng. Sci. Technol., Int. J.*, vol. 35, Nov. 2022, Art. no. 101176.

[5] R. Santos, D. Souza, W. Santo, A. Ribeiro, and E. Moreno, "Machine learning algorithms to detect DDoS attacks in SDN," *Concurrency Comput., Pract. Exper.*, vol. 32, no. 16, Aug. 2020, Art. no. e5402.

[6] L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang, and Y. Deng, "A new framework for DDoS attack detection and defense in SDN environment," *IEEE Access*, vol. 8, pp. 161908–161919, 2020.

[7] M. Shakil, A. F. Y. Mohammed, R. Arul, A. K. Bashir, and J. K. Choi, "A novel dynamic framework to detect DDoS in SDN using metaheuristic clustering," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, Mar. 2022, Art. no. e3622.

[8] A. O. Sangodoyin, M. O. Akinsolu, P. Pillai, and V. Grout, "Detection and classification of DDoS flooding attacks on software-defined networks: A case study for the application of machine learning," *IEEE Access*, vol. 9, pp. 122495–122508, 2021.

[9] J. A. Pérez-Díaz, I. A. Valdovinos, K. R. Choo, and D. Zhu, "A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning," *IEEE Access*, vol. 8, pp. 155859–155872, 2020.

[10] M. A. Ribeiro, M. S. P. Fonseca, and J. de Santi, "Detecting and mitigating DDoS attacks with moving target defense approach based on automated flow classification in SDN networks," *Comput. Secur.*, vol. 134, Nov. 2023, Art. no. 103462.

[11] A. Sebbar and K. Zkik, "Enhancing resilience against DDoS attacks in SDN -based supply chain networks using machine learning," in *Proc. 9th Int. Conf. Control, Decis. Inf. Technol. (CoDIT)*, Jul. 2023, pp. 230–234.

[12] R. Raj and S. S. Kang, "Mitigating DDoS attack using machine learning approach in SDN," in *Proc. 4th Int. Conf. Adv. Comput., Commun. Control Netw. (ICAC3N)*, Dec. 2022, pp. 462–467.

[13] K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj, and P. Chinnasamy, "Detection of distributed denial of service attacks in SDN using machine learning techniques," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2021, pp. 1–5.

[14] M. Kavitha, M. Suganthy, A. Biswas, R. Srinivsan, R. Kavitha, and A. Rathesh, "Machine learning techniques for detecting DDoS attacks in SDN," in *Proc. Int. Conf. Autom., Comput. Renew. Syst. (ICACRS)*, Dec. 2022, pp. 634–638.

[15] K. Alhamami and S. Albermany, "DDOS attack detection using machine learning algorithm in SDN network," in *Proc. Al-Sadiq Int. Conf. Commun. Inf. Technol. (AICCIT)*, Jul. 2023, pp. 97–102.

[16] A. T. Kyaw, M. Zin Oo, and C. S. Khin, "Machine-learning based DDOS attack classifier in software defined network," in *Proc. 17th Int. Conf. Electr. Eng./Electron., Comput., Telecommun. Inf. Technol. (ECTI-CON)*, Jun. 2020, pp. 431–434.

[17] R. R. Sekar, A. M. Jenny, D. Sreshta, M. Vikas, D. B. N. Ajay, and M. Ganesh, "Prediction of distributed denial of service attacks in SDN using machine learning techniques," in *Proc. 3rd Int. Conf. Intell. Technol. (CONIT)*, Jun. 2023, pp. 1–5.

[18] A. K. Kurakula, K. Akhila, M. Bhavya, and M. V. Sai, "Detecting distributed DoS attacks on SDN using machine learning (ML) methods," in *Proc. Int. Conf. Innov. Data Commun. Technol. Appl. (ICIDCA)*, Mar. 2023, pp. 767–772.

[19] A. K. Tahirou, K. Konate, and M. M. Soidridine, "Detection and mitigation of DDoS attacks in SDN using machine learning (ML)," in *Proc. Int. Conf. Digit. Age Technol. Adv. Sustain. Develop. (ICDATA)*, May 2023, pp. 52–59.

[20] S. Sanapala, D. D. Reddy, G. L. Chowdary, and K. S. Vikyath, "Machine learning based DDoS attack detection in software defined networks (SDN)," in *Proc. 2nd Int. Conf. Edge Comput. Appl. (ICECAA)*, Jul. 2023, pp. 1124–1126.

[21] S. Feng, G. Yang, and W. Man, "Research on DDoS attack detection based on machine learning in SDN environment," in *Proc. IEEE 7th Inf. Technol. Mechatronics Eng. Conf. (ITOEC)*, Sep. 2023, pp. 821–825.

[22] S. Bala and S. M. M. Ahsan, "Detecting DDoS attacks in software define networking: A machine learning based approach," in *Proc. Int. Conf. Next-Gener. Comput., IoT Mach. Learn. (NCIM)*, Jun. 2023, pp. 1–6.

[23] A. A. Alashhab, M. S. M. Zahid, M. Alashhab, and S. Alashhab, "Online machine learning approach to detect and mitigate low-rate DDoS attacks in SDN-based networks," in *Proc. IEEE Int. Conf. Artif. Intell. Eng. Technol. (IICAIET)*, Sep. 2023, pp. 152–157.

[24] B. A. Almohagri, M. A. Saeed, H. M. Alazaby, and A. I. Mohammed, "Machine learning approach for distributed daniel of service attack detection in SDNs," in *Proc. 3rd Int. Conf. Emerg. Smart Technol. Appl. (eSmarTA)*, Oct. 2023, pp. 1–7.

[25] A. Banitalebi Dehkordi, M. Soltanaghaei, and F. Z. Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN," *J. Supercomput.*, vol. 77, no. 3, pp. 2383–2415, Mar. 2021.

[26] A. Lazaris and V. K. Prasanna, "An LSTM framework for software-defined measurement," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 1, pp. 855–869, Mar. 2021.

[27] H.-M. Chuang and L.-J. Ye, "Applying transfer learning approaches for intrusion detection in software-defined networking," *Sustainability*, vol. 15, no. 12, p. 9395, Jun. 2023.

[28] M. S. E. Sayed, N.-A. Le-Khac, M. A. Azer, and A. D. Jurcut, "A flow-based anomaly detection approach with feature selection method against DDoS attacks in SDNs," *IEEE Trans. Cognit. Commun. Netw.*, vol. 8, no. 4, pp. 1862–1880, Dec. 2022.

[29] L. Chen, Z. Wang, R. Huo, and T. Huang, "An adversarial DBN-LSTM method for detecting and defending against DDoS attacks in SDN environments," *Algorithms*, vol. 16, no. 4, p. 197, Apr. 2023.

[30] T. V. Phan, T. G. Nguyen, N.-N. Dao, T. T. Huong, N. H. Thanh, and T. Bauschert, "DeepGuard: Efficient anomaly detection in SDN with fine-grained traffic flow monitoring," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 3, pp. 1349–1362, Sep. 2020.

[31] N. S. Shaji, T. Jain, R. Muthalagu, and P. M. Pawar, "Deep-discovery: Anomaly discovery in software-defined networks using artificial neural networks," *Comput. Secur.*, vol. 132, Sep. 2023, Art. no. 103320.

[32] N. M. Yungaicela-Naula, C. Vargas-Rosales, and J. A. Pérez-Díaz, "SDN/NFV-based framework for autonomous defense against slow-rate DDoS attacks by using reinforcement learning," *Future Gener. Comput. Syst.*, vol. 149, pp. 637–649, Dec. 2023.

[33] S. Haider, A. Akhunzada, I. Mustafa, T. B. Patel, A. Fernandez, K. R. Choo, and J. Iqbal, "A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 53972–53983, 2020.

[34] A. K. Mousa and M. N. Abdullah, "An improved deep learning model for DDoS detection based on hybrid stacked autoencoder and checkpoint network," *Future Internet*, vol. 15, no. 8, p. 278, Aug. 2023.

[35] J. Wang and L. Wang, "SDN-defend: A lightweight online attack detection and mitigation system for DDoS attacks in SDN," *Sensors*, vol. 22, no. 21, p. 8287, Oct. 2022.

[36] T. E. Ali, Y.-W. Chong, and S. Manickam, "Comparison of ML/DL approaches for detecting DDoS attacks in SDN," *Appl. Sci.*, vol. 13, no. 5, p. 3033, Feb. 2023.

[37] T. G. Gebremeskel, K. A. Gemeda, T. G. Krishna, and P. J. Ramulu, "DDoS attack detection and classification using hybrid model for multicontroller SDN," *Wireless Commun. Mobile Comput.*, vol. 2023, pp. 1–18, Jun. 2023.

[38] A. Mansoor, M. Anbar, A. Bahashwan, B. Alabsi, and S. Rihan, "Deep learning-based approach for detecting DDoS attack on software-defined networking controller," *Systems*, vol. 11, no. 6, p. 296, Jun. 2023.

[39] M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proença, "Adversarial deep learning approach detection and defense against DDoS attacks in SDN environments," *Future Gener. Comput. Syst.*, vol. 125, pp. 156–167, Dec. 2021.

[40] M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proença, "Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment," *IEEE Access*, vol. 8, pp. 83765–83781, 2020.

[41] Y.-C. Wang, Y.-C. Houng, H.-X. Chen, and S.-M. Tseng, "Network anomaly intrusion detection based on deep learning approach," *Sensors*, vol. 23, no. 4, p. 2171, Feb. 2023.

[42] N. M. Yungaicela-Naula, C. Vargas-Rosales and J. A. Perez-Diaz, "SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning," IEEE Access, vol. 9, pp. 108495–108512, 2021.

[43] J. D. Gadze, A. A. Bamfo-Asante, J. O. Agyemang, H. Nunoo-Mensah, and K. A.-B. Opare, "An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers," *Technologies*, vol. 9, no. 1, p. 14, Feb. 2021.

[44] D. Alghazzawi, O. Bamasag, H. Ullah, and M. Z. Asghar, "Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection," *Appl. Sci.*, vol. 11, no. 24, p. 11634, Dec. 2021.

[45] M. Li, B. Zhang, G. Wang, B. ZhuGe, X. Jiang, and L. Dong, "A DDoS attack detection method based on deep learning two-level model CNN-LSTM in SDN network," in *Proc. Int. Conf. Cloud Comput., Big Data Appl. Softw. Eng. (CBASE)*, Sep. 2022, pp. 282–287.

[46] W. Zhao, H. Sun, and D. Zhang, "Research on DDoS attack detection method based on deep neural network model inSDN," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Dec. 2022, pp. 184–188.

[47] S. A. Christila and R. Sivakumar, "Multi-layer ensemble deep reinforcement learning based DDoS attack detection and mitigation in cloud-SDN environment," in *Proc. 4th Int. Conf. Circuits, Control, Commun. Comput. (I4C)*, Dec. 2022, pp. 451–455.

[48] A. Chetouane and K. Karoui, "Performance improvement of DDoS intrusion detection model using hybrid deep learning method in the SDN environment," in *Proc. IEEE 21st Int. Conf. Ubiquitous Comput. Commun. (IUCC/CIT/DSCI/SmartCNS)*, Dec. 2022, pp. 159–166.

[49] U. Mbasuva and G. L. Zodi, "Designing ensemble deep learning intrusion detection system for DDoS attacks in software defined networks," in *Proc. 16th Int. Conf. Ubiquitous Inf. Manage. Commun. (IMCOM)*, Jan. 2022, pp. 1–8.

[50] R. B. Said and I. Askerzade, "Attention-based CNN-BiLSTM deep learning approach for network intrusion detection system in software defined networks," in *Proc. 5th Int. Conf. Problems Cybern. Informat. (PCI)*, Aug. 2023, pp. 1–5.

[51] Cisco. (Sep. 2018). *Cisco Annual Internet Report (2018–2023) White Paper*. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[52] *CSE-CIC-IDS2018 on AWS. Canadian Institute for Cybersecurity*. Accessed: Jan. 24, 2024. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2018.html

NURA SHIFA MUSA received the bachelor's degree in computer engineering from Qatar University (QU), Qatar, and the master's degree in information security from the College of Information Technology, United Arab Emirates University (UAEU), United Arab Emirates. She is currently a Senior Lab Supervisor with the College of Engineering, Al Ain University (AAU), United Arab Emirates. Demonstrating a profound dedication to advancing cyber security measures, her research interests include developing innovative solutions to enhance digital security, investigating cyber threats, exploring cloud computing technology, and conducting digital forensic investigations. She received awards and honors.

NADA MASOOD MIRZA received the B.E. and M.S. degrees in mechatronics engineering from the College of Electrical and Mechanical Engineering, National University of Sciences & Technology (NUST), Pakistan. She is currently an Instructor with the College of Engineering, United Arab Emirates University (UAEU), United Arab Emirates. Her postgraduate research was mostly focused on the application of artificial intelligence, robotics, and wireless monitoring of renewable energy systems. She worked for a few years in academia in Pakistan, where her research interest includes autonomous wireless intelligent robotic systems. Since 2014, she has been involved in academic activities related to control and electronics engineering in United Arab Emirates.

SAIDA HAFSA RAFIQUE received the B.Sc. degree in cellular and molecular biology from United Arab Emirates University (UAEU), United Arab Emirates, in 2019, and the M.Sc. degree in forensic science from the University of Strathclyde, U.K., in 2020. She is currently pursuing the M.Sc. degree in information security with UAEU. Her research interests include cloud security, the IoT security, artificial intelligence, digital forensics, and forensic science.

AMIRA MAHAMAT ABDALLAH received the B.S. degree in computer science from Taibah University, Saudi Arabia, in 2018. She is currently pursuing the M.S. degree in information security with United Arab Emirates University, United Arab Emirates. Her research interests include cloud security, intrusion detection systems, and artificial intelligence.

THANGAVEL MURUGAN (Senior Member, IEEE) received the bachelor's (B.E.) degree (Hons.) in computer science and engineering from the M. A. M. College of Engineering (Trichy), Anna University, Chennai, the master's (M.E.) degree (Hons.) in computer science and engineering from the J. J. College of Engineering and Technology (Trichy), Anna University, and the Ph.D. degree from the Madras Institute of Technology (MIT) Campus, Anna University. He is currently an Assistant Professor with the Department of Information Systems and Security, College of Information Technology, United Arab Emirates University. He also holds more than 11 years of teaching and research experience from various academic institutions. He has published more than ten articles in international journals, more than 15 book chapters in international publishers, more than 25 in the proceedings of international conferences, and three in the proceedings of national conferences/seminars. His academic and research interests include information security, high performance computing, ethical hacking, cyberforensics, blockchain, cybersecurity intelligence, and educational technology.