Systematic Review of Machine Learning-Based DDoS Detection in SDN Networks: A PRISMA Approach

Ananda[1,a)], Yayan Suarghana[2,b)]

[1]*Magister Terapan Teknik Komputer, Politeknik Caltex Riau, Pekanbaru, Indonesia*
[2]*Teknik Informatika, Politeknik Caltex Riau, Pekanbaru, Indonesia*

Corresponding authors: [a)] ananda@pcr.ac.id
[b)] yayan23mttk@mahasiswa.pcr.ac.id

Abstract. This systematic literature review aims to detect the detection of Distributed Denial of Service (DDoS) attacks in Software-Defined Networking (SDN) environments using machine learning techniques. The PRISMA approach was used to ensure a comprehensive and transparent review process. The underlying architecture of SDN is highly vulnerable to DDoS attacks and thus requires efficient detection mechanisms. This review covers the application of various machine learning algorithms, such as Random Forest, Support Vector Machine (SVM), and Neural Networks, and their effectiveness in identifying anomalous traffic. Data from Scopus-indexed journals between 2016 and 2024 is used to provide a comprehensive picture of recent advances in this field. The research found that machine learning algorithms were able to increase the level of accuracy in DDoS detection, but also identified significant challenges such as the limitations of high-quality datasets that reflect real network traffic and the need for real-time detection at large network scales. In addition, the computational complexity of deep learning models and resource efficiency in practical applications are also challenges that need to be resolved. The results of these observations lead to recommendations for developing more efficient algorithms, optimizing the use of computing resources, and improving dataset quality to support more accurate and faster DDoS detection in SDN environments.

Keywords: DDoS Attack Detection, Software Defined Networking, Machine Learning

INTRODUCTION

In recent years, the advent of Software-Defined Networking (SDN) has redefined how networks are managed and operated. SDN introduces a paradigm shift by decoupling the control plane from the data plane, allowing network administrators to program and dynamically manage network configurations through a centralized controller. This shift has ushered in unparalleled flexibility, scalability, and efficiency in modern networks, enabling innovations in fields ranging from data center management to Internet of Things (IoT) deployments. However, while SDN provides numerous advantages, it also introduces a new set of security challenges, making it a prime target for cyberattacks, especially Distributed Denial of Service (DDoS) attacks.

A DDoS attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. In an SDN environment, the centralization of network control presents an attractive point of vulnerability. If a DDoS attack manages to incapacitate the SDN controller, it could lead to network-wide disruption, making the detection and mitigation of such attacks a critical area of research. Traditional network security mechanisms, while effective in conventional networks, often fall short in an SDN context due to its architectural differences, thus necessitating the development of novel and more adaptive defense mechanisms.

Machine learning (ML) has emerged as a promising approach for the detection of DDoS attacks in SDN networks. Unlike traditional rule-based systems, machine learning models can identify and adapt to new and evolving attack patterns by learning from data. These models can be trained to recognize subtle anomalies in network traffic that may indicate the onset of a DDoS attack, allowing for early detection and response. Various machine learning techniques, including supervised learning, unsupervised learning, and deep learning, have been explored in recent studies for their potential to enhance the detection accuracy and reduce false-positive rates in DDoS detection systems.

While machine learning offers a powerful tool for DDoS detection, several challenges remain in its application to SDN environments. One of the primary challenges is the scalability of detection systems. As SDN networks grow in size and complexity, the volume of traffic data that needs to be monitored and analyzed increases exponentially. Machine learning models must be designed to handle this scale without compromising detection speed or accuracy. Additionally, real-time detection is critical in mitigating DDoS attacks, as even a short delay in response can lead to significant network disruption. This necessitates the development of lightweight and efficient models that can operate in real time without imposing a heavy computational burden on the network infrastructure.

Another challenge lies in the evolving nature of DDoS attacks. Attackers continuously modify their strategies to evade detection, making it difficult for static detection models to remain effective over time. Machine learning models must therefore be continually retrained with new data to adapt to these changes. This introduces the issue of data availability, as obtaining large, labeled datasets for training can be time-consuming and resource-intensive. Furthermore, there is the risk of overfitting, where models become too specialized to the training data and fail to generalize to unseen traffic patterns. Addressing these challenges requires a careful balance between model complexity, performance, and adaptability.

Given the growing interest in machine learning-based DDoS detection in SDN networks, a comprehensive review of the current state of research is necessary to provide clarity on the effectiveness of various approaches and identify areas that require further investigation. While individual studies have explored different machine learning techniques for DDoS detection, there has been limited effort to systematically synthesize the findings from these studies and assess their overall impact on SDN security.

This paper aims to fill this gap by conducting a systematic review of machine learning-based DDoS detection in SDN networks using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology. The PRISMA framework ensures a structured and transparent approach to literature review, allowing us to provide a clear overview of the existing research landscape, highlight key contributions, and identify potential research gaps. By analyzing studies published between 2016 and 2024, we aim to offer insights into the evolution of machine learning techniques in this domain and their applicability in real-world SDN environments.

METHODS

Systematic review is a very procedure rigorous in identifying, assessing, and synthesizing all relevant research results related to the question research, a particular topic, or a becoming phenomenon attention by using strategies in limiting bias (Briner et al., 2009; Garg et al., 2008; Kitchenham, 2004), as well as being the "gold standard" in assimilating and digest research (Oxman et al., 1994; Remme, 2004). Humphrey (2011) and Kitchenham (2004) also emphasize it the importance of developing literature through systematics review in looking for configurations for further investigation and placing activities new research precisely. Cooper (2016) in his book entitled “Research Synthesis and Meta Analysis a Step-by-Step Approach” states that systematic review is a research method that can be used in social Sciences. Social science has many branches of knowledge once, such as: economics, anthropology, demography, psychology, sociology, etc., which generally studies various aspects related to humans and the environment social aspects in terms of implications and consequences. [1].

Petticrew & Roberts (2012) also stated that it is very important for researchers to know the differences between real and assumed knowledge. Systematic review can help us find out what evidence there is exists, by first knowing what is already known, what support they have, and what they don't have explained (Cooper, 2016), and relies heavily on when the measurements were carried out and what the stages were (Rupp et al., 2014). Review of various studies spread across various digital libraries are very important in order to be able to know various kinds of theoretical developments, issues, and research model on a particular topic. [1]

Previous research on DDoS attack detection systems in software defined networks using machine learning algorithms. This is addressed to understand the effectiveness of implementing machine learning algorithms in detecting DDoS attacks in software defined networking. This research data was taken starting from 2014 from the Scopus database. Researchers use Scopus as the main source of information because it is considered Its coverage is wider than other indexes. In this study, researchers Analyzing documents related to DDOS attack detection systems in software defined networks using machine learning algorithms with using the watase.web.id page, then processed using the PRISMA method.

Researchers collected data by searching for journal articles with keywords "machine learning" OR "Ddos Attack" OR "Software Defined Network" OR "SDN".

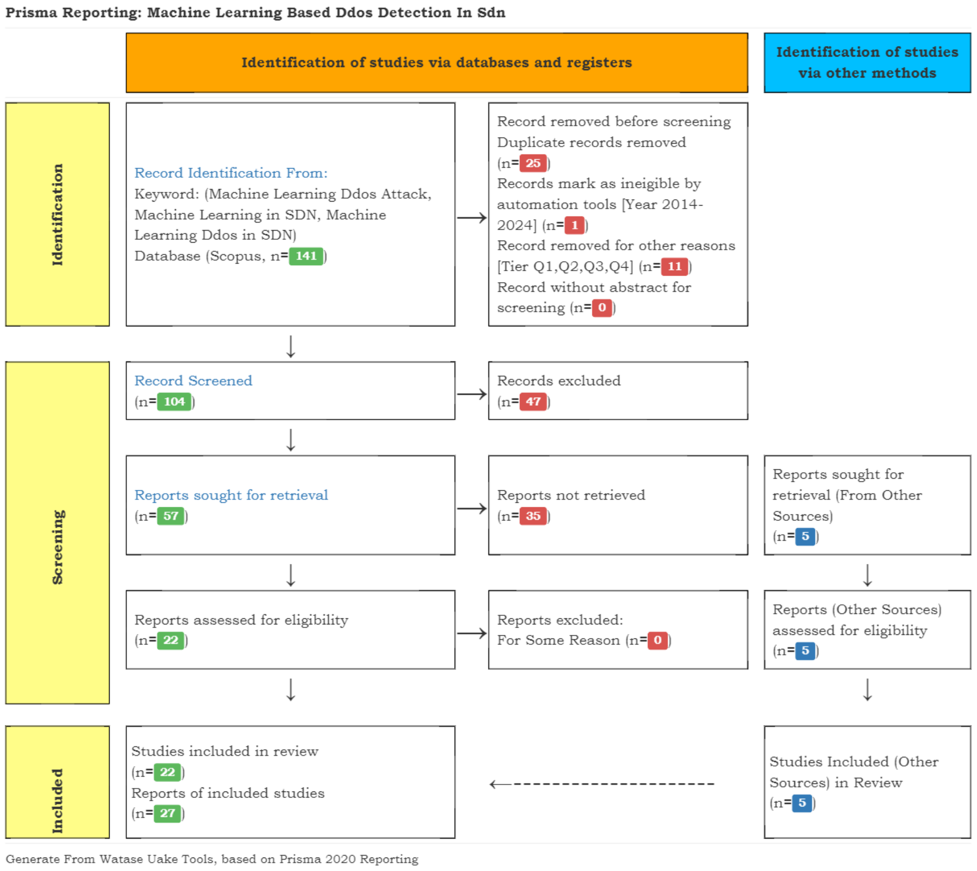
Prisma Reporting: Machine Learning Based Ddos Detection In Sdn
Identification of studies via databases and registers
Identification of studies via other methods
Identification
Record Identification From:
Keyword: (Machine Learning Ddos Attack, Machine Learning in SDN, Machine Learning Ddos in SDN)
Database (Scopus, n=141)
Record removed before screening
Duplicate records removed (n=25)
Records mark as ineigible by automation tools [Year 2014-2024] (n=1)
Record removed for other reasons [Tier Q1,Q2,Q3,Q4] (n=11)
Record without abstract for screening (n=0)
Screening
Record Screened (n=104)
Records excluded (n=47)
Reports sought for retrieval (n=57)
Reports not retrieved (n=35)
Reports sought for retrieval (From Other Sources) (n=5)
Reports assessed for eligibility (n=22)
Reports excluded: For Some Reason (n=0)
Reports (Other Sources) assessed for eligibility (n=5)
Included
Studies included in review (n=22)
Reports of included studies (n=27)
Studies Included (Other Sources) in Review (n=5)
Generate From Watase Uake Tools, based on Prisma 2020 Reporting

FIGURE 1. PRISMA flow diagram of this research

In conducting the systematic review for a study on Machine Learning-based DDoS detection in SDN networks, adhered to the PRISMA methodology to ensure a comprehensive and structured analysis. Our search strategy targeted keywords such as "DDoS in SDN," "Machine Learning DDoS Attack," "Machine Learning in SDN," and "Machine Learning DDoS in SDN." The search was conducted in the Scopus database, yielding 141 records initially.

Before screening, 25 duplicate records were removed, along with one record that was deemed ineligible by automation tools due to not meeting the year criteria (2014–2024). An additional 11 records were removed based on tier classification (Q1, Q2, Q3, Q4), leaving 104 records for the initial screening phase.

During the screening process, 47 records were excluded, narrowing the pool to 57 reports sought for retrieval. Of these, 35 reports were not retrievable, and 5 additional reports were identified from other sources. Following retrieval, 27 reports were assessed for eligibility, and five studies from other sources were also included in the review.

Ultimately, 27 studies were deemed eligible and included in the review, with a total of 27 reports analyzed for this systematic review. These findings reflect a rigorous selection process to ensure that only relevant and high-quality studies were considered in our analysis.

RESULTS AND DISCUSSION

In this research, I have classified several studies related to Distributed Denial of Service (DDoS) attacks based on problem addressing or the main focus of the problem raised. The following table summarizes these classifications to provide a clearer picture of the various approaches used to detect, prevent, and address DDoS attacks in various network environments, including Software-Defined Networking (SDN) and other specialized systems

TABLE 1. Classification of DDoS attacks based on Problem Addressing

General DDoS Detection (Not Related to Specific Environments)	Detect Distributed Denial of Service (DDoS) attacks in network traffic using machine learning algorithms. [2] [3] [5] [6]
	Real-time detection and mitigation of Distributed Denial of Service (DDoS) attacks in network traffic. [4]
	Detect DDoS attacks by identifying the best machine learning models and applying them to real-world datasets. [4]
DDoS Detection in an SDN Environment	DDoS attack detection in Software-Defined Networking (SDN) using Machine Learning (ML) and Deep Learning (DL). [7] [8] [9]
	Detect and mitigate DDoS attacks in SDN environments using a hybrid approach between entropy and machine learning. [10] [11]
	Detect Distributed Denial of Service (DDoS) attacks at the transport and application layers in SDN-based environments. [12]
	Detect and mitigate Distributed Denial of Service (DDoS) attacks in Software Defined Networking (SDN) environments. [13] [3] [14] [15]
	Detection of DDoS attacks in Software-Defined Networks (SDN). [16] [17] [18]
	Detect DRDoS attacks in SDN with amplification using machine learning to improve network security and traffic management. [19]
	Real-time detection of DDoS attacks in Software-Defined Networking (SDN). [20] [21]
	DDoS attacks that disrupt network availability, especially in SDN networks [5] [22]

Low or Special Type DDoS Attacks	Identify and mitigate low-rate DDoS attacks in SDN environments. [23]
	Mitigate DDoS attacks (TCP-SYN and ICMP flooding) in ISP networks using SDN and machine learning.
	Detect DoS and DDoS based ICMPv6 attacks using machine learning techniques and explore the application of blockchain to improve security [24]
Cybersecurity in Dedicated SDN Networks	Cyberattacks on healthcare SDN systems, compromising data security and network performance. [25]
	Security threats in SDN networks, specifically focus on Network Intrusion Detection Systems (NIDS). [26]
	Botnet attacks in SDN-enabled IoT networks [27]
Traffic Optimization and Security in SDN	Optimizing traffic classification and security in Software-Defined Networks (SDN) using Machine Learning (ML). [28] [18]

TABLE 2. Classification od DDoS Attack based Dataset

No	Dataset	Total
1	KDD99, KDD Cup 99, NSL-KDD	3
2	CICIDS2017, CIC-IDS2017, CIC-DoS	4
3	CIC-DDoS2019, CICDDoS2019	4
4	CSE-CIC-IDS2018	2
5	InSDN	4
6	UNSW-NB15	2
7	Canadian Institute for Cybersecurity (CIC) IoT Dataset 2022	1
8	Custom Dataset, Customized Datasets	4
9	Real-time Network Traffic Datasets	2
10	Generated Dataset (e.g., from Mininet, Ryu, Bonesi)	3

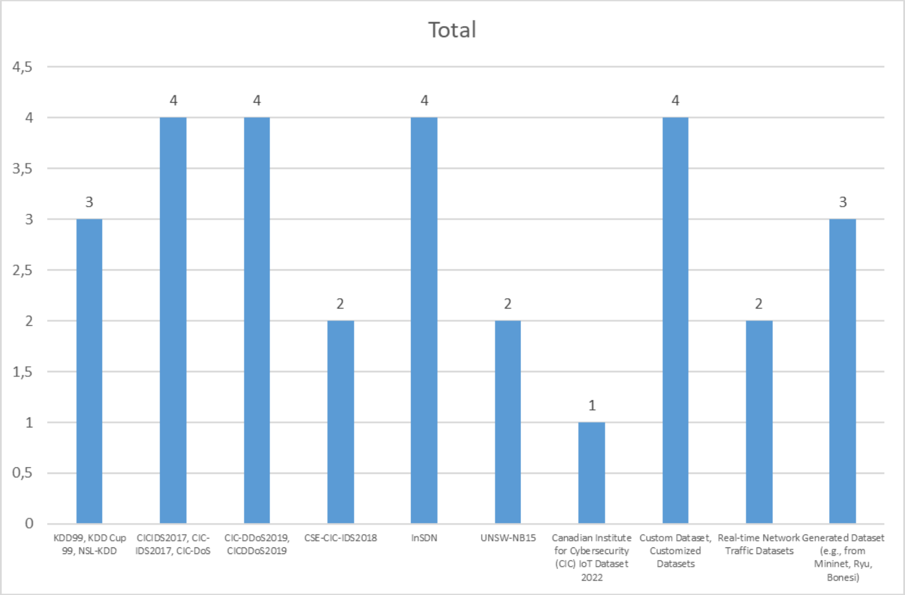

FIGURE 2 . Graphics Based on Dataset Clasification

a. Machine Learning mechanisms to predict Specific DDoS Attacks

Machine Learning approaches provide significant advantages over traditional methods due to their ability to analyze complex patterns in network traffic and adapt to new forms of attacks. Specifically, Machine Learning models can be trained on features extracted from network data, allowing them to distinguish between normal and malicious traffic with greater accuracy. This ability to predict and identify abnormal traffic is seen as crucial for mitigating DDoS attacks before they cause significant damage. Machine Learning techniques, such as supervised, unsupervised, and ensemble learning methods, have shown promise in improving detection accuracy and reducing false positives compared to conventional methods like statistical analysis and rule-based approaches. Machine Learning models can be further enhanced through the use of SDN-specific datasets and feature selection methods, which would allow models to better capture the unique characteristics of DDoS attacks in SDN environments [7].

Jesús Arturo Pérez-Díaz, Ismael Amezcua Valdovinos, Kim-Kwang Raymond Choo, and Dakai Zhu , 2020 explain that machine learning (ML) mechanisms as effective tools for predicting and identifying specific DDoS attacks, particularly in software-defined networking (SDN) environments. They highlight that ML models like J48, Random Forest, and Support Vector Machines (SVM) can achieve high detection rates for various types of low-rate DDoS (LR-DDoS) attacks. The authors appreciate the flexibility of ML techniques, allowing them to adapt to different attack patterns and improve detection accuracy when applied to the specific characteristics of network traffic [23].

Noe Marcelo Yungaicela-Naula, Cesar Vargas-Rosales, and Jesus Arturo Perez-Diaz. It was published in 2021 [12] describe that Machine Learning (ML) and Deep Learning (DL) mechanisms significantly enhances the detection of Distributed Denial of Service (DDoS) attacks. They emphasize the need for up-to-date datasets, like the CICDoS2017 and CICDDoS2019 datasets, to train these models effectively. According to the authors, previous detection methods were not as robust due to outdated datasets and the lack of evaluation in real-world or simulated environments. Their proposed architecture addresses these limitations by testing multiple ML/DL methods in a simulated environment using an SDN (Software-Defined Networking) controller. The authors found that ML/DL models demonstrated high accuracy, with rates above 99% for classifying attack types and conditions, highlighting the superiority of certain models like GRU and LSTM.

Nguyen Ngoc Tuan et al. 2020 [5] Machine Learning (ML) mechanisms can play a significant role in predicting specific DDoS attacks like TCP-SYN and ICMP flood attacks. The authors use K-Nearest Neighbor (KNN) and XGBoost algorithms to efficiently mitigate these types of attacks. The algorithms were deployed in an SDN environment, which allowed for flexible and centralized management of traffic. The authors found that the ML models could accurately differentiate between attack traffic and benign traffic, with over 98% efficiency in mitigating attacks, while ensuring that legitimate traffic was not affected. This demonstrates the strong predictive capabilities of ML for specific DDoS attack patterns

b. Accuracy of DDoS detection using various Machine Learning Algorithms

A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," authored by Muhammad Ismail Mohmand et al. and published in 2022 [6], reports the accuracy of DDoS detection using various machine learning algorithms. Random Forest Algorithm: Precision (PR) and Recall (RE) were both approximately 89%, with an average accuracy (AC) of around 89%. XGBoost Algorithm: Precision (PR) and Recall (RE) were approximately 90%, with an average accuracy (AC) of around 90%.

The journal titled "Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset" by Naveen Bindra and Manu Sood (2019) [4] reports the following results regarding the accuracy of DDoS detection using various machine learning algorithms ,Random Forest Classifier: Achieved an accuracy of 96.2%, with an ROC score of 0.99, making it the top-performing model. K-Nearest Neighbor (KNN): Achieved an accuracy of 95.1%. Logistic Regression: Achieved an accuracy of 82.5%. Gaussian Naïve Bayes (GNB): Achieved an accuracy of 81.0%. Linear SVM: Achieved an accuracy of 82.3%. The Random Forest Classifier is identified as the best-performing algorithm for DDoS detection in this study, providing the highest accuracy (96.2%) when tested on the CIC IDS 2017 dataset, which is a real-world, contemporary dataset. This supports the authors' conclusion that Random Forest is a superior choice for detecting DDoS attacks using machine learning.

Rami J. Alzahrani and Ahmed Alzahrani, (2021) [3], The results for DDoS detection using various machine learning algorithms are as follows: Decision Tree (DT): Achieved an accuracy of 99%. Random Forest (RF): Also achieved an accuracy of 99%, but with longer computation time compared to DT (84.2 seconds vs. 4.53 seconds). K-Nearest Neighbors (K-NN): Accuracy of 98%. Super Vector Machine (SVM): Accuracy of 86%. Logistic Regression (LR): Accuracy of 98%. Naïve Bayes (NB): Accuracy of 45%.

The best performance in terms of accuracy and precision was achieved by the Decision Tree (DT) and Random Forest (RF) algorithms, both reaching 99% accuracy

Huseyin Polat, et al. 2020 [16] . The study compares various machine learning algorithms for detecting DDoS attacks in SDN using feature selection methods. The key result is that the K-Nearest Neighbors (KNN) classifier, combined with the wrapper-based feature selection method, achieved the highest accuracy of 98.3% for detecting DDoS attacks.

TABLE 3. Accuracy of DDoS detection using various Machine Learning Algorithms

No	Topic	Author	Year	Country	Algorithm	Accuracy
1	A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks [6]	Muhammad Ismail Mohmand, Hameed Hussain, Ayaz Ali Khan, Ubaid Ullah, Muhammad Zakarya, Aftab Ahmed, Mushtaq Raza, Izaz Ur Rahman, Muhammad Haleem	2022	Pakistan	Random Forest, XGBoost	Random Forest achieved ~89% accuracy, and XGBoost achieved ~90% accuracy
2	Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset [4]	Naveen Bindra, Manu Sood	2019	India	Random Forest, KNN, SVM, Naïve Bayes, Logistic Regression	Random Forest achieved highest accuracy (96.13%) for DDoS detection compared to other models
3	Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Network Traffic [3]	Rami J. Alzahrani, Ahmed Alzahrani	2021	Saudi Arabia	KNN, SVM, Naïve Bayes, Decision Tree (DT), Random Forest (RF), Logistic Regression (LR)	Decision Tree and Random Forest algorithms showed the best performance with 99% accuracy, precision, recall, and F1 score
4	Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models [16]	Huseyin Polat, Onur Polat, Aydin Cetin	2020	Turkey	Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Artificial Neural Network (ANN), Naive Bayes (NB)	KNN achieved the highest accuracy (98.3%) in detecting DDoS attacks with wrapper-based feature selection

CONCLUSIONS

The systematic literature review conducted in this study provides an in-depth analysis of detecting and mitigating Distributed Denial of Service (DDoS) attacks in Software-Defined Networking (SDN) environments using machine learning techniques. DDoS attacks, which overwhelm a target system with malicious traffic to degrade its performance or cause a complete shutdown, pose a significant threat to network security. The study highlights that traditional security measures often fall short in SDN due to its centralized control architecture, making the use of machine learning algorithms such as Random Forest, Support Vector Machine (SVM), and Neural Networks an effective approach for improving detection accuracy.

This review employed the PRISMA methodology to systematically filter and select relevant studies, resulting in 27 articles published between 2014 until 2024 being included in the analysis. The PRISMA approach helped ensure a transparent and structured review process, identifying the strengths and limitations of existing machine learning-based detection methods. The findings revealed that while machine learning models show promise in enhancing detection capabilities and reducing false positives, challenges such as computational complexity, scalability issues, and the need for high-quality datasets remain prevalent in current research.

Furthermore, the study observes that as DDoS attacks evolve, there is a need for adaptive and efficient models that can operate in real time to detect emerging threats. This necessitates ongoing improvements in algorithm design and the integration of hybrid models to address the dynamic nature of attack patterns. Overall, the systematic review underscores the importance of advancing machine learning techniques and refining datasets to develop more robust and scalable solutions for DDoS detection in SDN environments.

ACKNOWLEDGMENTS

The author would like to express sincere gratitude to all those who contributed to this study. Special thanks to the faculty and staff of the Magister Terapan Teknik Komputer program at Politeknik Caltex Riau for their continuous support and guidance throughout the research process. Appreciation is also extended to the reviewers and conference organizers for providing valuable feedback and recommendations that helped improve the quality of this paper. Finally, heartfelt thanks to family and friends for their encouragement and understanding during the completion of this work.

REFERENCES

[1] S. Hadi, U. S. Tamansiswa, M. Palupi, and U. I. Indonesia, *SYSTEMATIC*, no. April. 2020.

[2] T. A. Tuan, H. V. Long, L. H. Son, R. Kumar, I. Priyadarshini, and N. T. K. Son, "Performance evaluation of Botnet DDoS attack detection using machine learning," *Evol. Intell.*, vol. 13, no. 2, pp. 283–294, 2020, doi: 10.1007/s12065-019-00310-w.

[3] R. J. Alzahrani and A. Alzahrani, "Security analysis of ddos attacks using machine learning algorithms in networks traffic," *Electron.*, vol. 10, no. 23, 2021, doi: 10.3390/electronics10232919.

[4] Naveen Bindra and Manu Sood, "Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset," *Autom. Control Comput. Sci.*, vol. 53, no. 5, pp. 419–428, 2019, doi: 10.3103/S0146411619050043.

[5] N. N. Tuan, P. H. Hung, N. D. Nghia, N. Van Tho, T. Van Phan, and N. H. Thanh, "A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN," *Electron.*, vol. 9, no. 3, pp. 1–19, 2020, doi: 10.3390/electronics9030413.

[6] Ismail *et al.*, "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," *IEEE Access*, vol. 10, no. February, pp. 21443–21454, 2022, doi: 10.1109/ACCESS.2022.3152577.

[7] N. Aslam, S. Srivastava, and M. M. Gore, "A Comprehensive Analysis of Machine Learning- and Deep Learning-Based Solutions for DDoS Attack Detection in SDN," *Arab. J. Sci. Eng.*, vol. 49, no. 3, pp. 3533–3573, 2024, doi: 10.1007/s13369-023-08075-2.

[8] M. A. Almaiah, R. Alrawashdeh, T. Alkhdour, R. Al-Ali, G. Rjoub, and T. Aldahyani, "Detecting DDoS attacks using machine learning algorithms and feature selection methods," *Int. J. Data Netw. Sci.*, vol. 8, no. 4, pp. 2307–2318, 2024, doi: 10.5267/j.ijdns.2024.6.001.

[9] T. E. Ali, Y. W. Chong, and S. Manickam, "Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review," *Appl. Sci.*, vol. 13, no. 5, 2023, doi: 10.3390/app13053183.

[10] A. I. Hassan, E. A. El Reheem, and S. K. Guirguis, "An entropy and machine learning based approach for DDoS attacks detection in software defined networks," *Sci. Rep.*, vol. 14, no. 1, pp. 1–18, 2024, doi: 10.1038/s41598-024-67984-w.

[11] İ. Avcı and M. Koca, "Predicting DDoS Attacks Using Machine Learning Algorithms in Building Management Systems," *Electron.*, vol. 12, no. 19, pp. 1–13, 2023, doi: 10.3390/electronics12194142.

[12] 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, doi: 10.1109/ACCESS.2021.3101650.

[13] A. A. Alashhab *et al.*, "Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble

Online Machine Learning Model," *IEEE Access*, vol. 12, no. March, pp. 51630–51649, 2024, doi: 10.1109/ACCESS.2024.3384398.

[14]"SmartDetectionAnOnlineApproachforDoSDDoSAttackDetectionUsingMachineLearningFranciscoSalesdeLimaFilho,1FredericoA.F.Silveira,1AgostinhodeMedeirosBritoJunior,1GenovevaVargas-Solar,2andLuizF.Silveira11ComputerEngine.pdf."

[15] 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, 2023, doi: 10.1080/25765299.2023.2261219.

[16] H. Polat and O. Polat, "Detecting DDoS Attacks in Software-Defined.pdf," *Mdpi*, 2020.

[17] M. H. H. Khairi *et al.*, "Detection and Classification of Conflict Flows in SDN Using Machine Learning Algorithms," *IEEE Access*, vol. 9, pp. 76024–76037, 2021, doi: 10.1109/ACCESS.2021.3081629.

[18] R. Ma, Q. Wang, X. Bu, and X. Chen, "Real Time," *Appl. Sci.*, vol. 13, no. 13, 2023, doi: 10.3390/app13137872.

[19] M. Akbari Kohnehshahri, R. Mohammadi, H. Abdoli, and M. Nassiri, "An Efficient Method for Online Detection of DRDoS Attacks on UDP-Based Services in SDN Using Machine Learning Algorithms," *Mob. Inf. Syst.*, vol. 2022, 2022, doi: 10.1155/2022/1169035.

[20] R. Abubakar *et al.*, "An Effective Mechanism to Mitigate Real-Time DDoS Attack," *IEEE Access*, vol. 8, pp. 126215–126227, 2020, doi: 10.1109/ACCESS.2020.2995820.

[21] M. A. Setitra, M. Fan, B. L. Y. Agbley, and Z. E. A. Bensalem, "Optimized MLP-CNN Model to Enhance Detecting DDoS Attacks in SDN Environment," *Network*, vol. 3, no. 4, pp. 538–562, 2023, doi: 10.3390/network3040024.

[22] S. Dong and M. Sarem, "DDoS Attack Detection Method Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks," *IEEE Access*, vol. 8, pp. 5039–5048, 2020, doi: 10.1109/ACCESS.2019.2963077.

[23] J. A. Perez-Diaz, I. A. Valdovinos, K. 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, doi: 10.1109/ACCESS.2020.3019330.

[24] M. Tayyab, B. Belaton, and M. Anbar, "ICMPV6-based DOS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review," *IEEE Access*, vol. 8, no. October, pp. 170529–170547, 2020, doi: 10.1109/ACCESS.2020.3022963.

[25] L. M. Halman and M. J. F. Alenazi, "MCAD: A Machine Learning Based Cyberattacks Detector in Software-Defined Networking (SDN) for Healthcare Systems," *IEEE Access*, vol. 11, no. April, pp. 37052–37067, 2023, doi: 10.1109/ACCESS.2023.3266826.

[26] "Network Threat Detection Using MachineDeep Learning inSDN-Based Platforms A Comprehensive Analysis ofState-of-the-Art Solutions, Discussion, Challenges, and FutureResearch Direction.pdf."

[27] W. G. Negera, F. Schwenker, T. G. Debelee, H. M. Melaku, and Y. M. Ayano, "Review of Botnet Attack Detection in SDN-Enabled IoT Using Machine Learning," *Sensors*, vol. 22, no. 24, 2022, doi: 10.3390/s22249837.

[28] R. H. Serag *et al.*, "Machine-Learning-Based Traffic Classification in Software-Defined Networks," pp. 1–30, 2024.