Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 1, pp. 249–265
DOI : 10.47974/JDMSC-2219

Enhancing SDN security : Mitigating DDoS attacks with robust authentication and shapley analysis

Monika Dandotiya *
Ajay Khunteta [#]
Department of Computer Science & Engineering
Poornima University
Jaipur 303905
Rajasthan
India

Rajni Ranjan Singh Makwana [$]
Centre for Artificial Intelligence
Madhav Institute of Technology & Science
Gwalior 474005
Madhya Pradesh
India

Abstract

SDN (Software-Defined Networking) revolutionized network administration by splitting the control plane from the data plane, allowing for centralized control also improved network flexibility. However, SDN also introduces security vulnerabilities, particularly Distributed Denial of Service (DDoS) attacks, which can significantly disrupt network services. This research introduces a novel two-phase method to improve the security of SDN environments through the use of SHAP (Shapley Additive Explanations). To mitigate the risk of unauthorized access, initial phase entails the establishment of a secure authentication mechanism that prevents unauthorized nodes from accessing network services. The second phase is dedicated to the mitigation & detection of DDoS attacks that are initiated by verified nodes. A SHAP (Shapley Additive Explanations)-based detection system is created, trained on a variety of datasets, including CICDDoS2019, and incorporated into the SDN controller for real-time traffic analysis. The efficiency of the proposed methodology in enhancing detection accuracy, reducing false positive rates, and maintaining network performance is demonstrated through comprehensive evaluations using simulation tools. This investigation

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

* *E-mail:* **dandotiyamonika@gmail.com (Corresponding Author)**
[#] *E-mail:* **ajay.khunteta@poornima.edu.in**
[$] *E-mail:* **ranjansingh06@gmail.com**

offers a solution that is adaptable, efficient, and robust to enhance the detection and mitigation of DDoS in SDN environments.

Subject Classification: *68M25, 68P25.*

Keywords: *Distributed denial of services (DDoS), Software defined networking (SDN), Mitigation, Attacks detection, Cyber security, Classification, CNN (Convolutional neural network), SHAP (Shapley additive explanations).*

1. Introduction

Due to the fast growth of internet technology over the past several years, upgrading to new network functions has proven difficult due to the old network's dispersed control and management approach [1]. This has made the implementation of network innovation difficult. By separating the conventional network architecture into a data plane, control plane, as well as application plane, SDN [2] is a revolutionary network design. To improve the flexibility and centralization of network control, it also makes use of the control layer's centralized management mode. Because of its programmability and openness, SDN has been a popular option for cloud computing, network virtualization, wireless local area networks, as well as cloud data centers [3].

The security issues associated with SDN have become more prevalent, even though its flexible network architecture offers convenience for network management. OpenFlow is a protocol that describes communication parameters between SDN controllers & SDN switches in SDN. It is a southbound interface protocol. Table misses are used to refer to data packets that do not align with flow rules in switch flow table in OpenFlow protocol [4][5]. The likelihood of the controller being targeted by deluge DDoS attacks is significantly elevated by this mode of operation. Several phoney IP packets are generated by attackers by exploiting the susceptibility of this working mode [6]. Consequently, the entire SDN network collapses as the controller's CPU and storage resources are swiftly depleted [7].

There are currently a multitude of methods available for detection & defense against DDoS attacks in SDN [8][9][10]. Consequently, it is imperative to resolve the issue of when to activate the detection device. Secondly, DDoS attacks will generate most of the packet_in messages in a short period and will swiftly deplete the controller's resources & impede detection equipment's functionality[11].

Numerous ML & DL methodologies have been implemented to identify DDoS attacks; however, DL demonstrated superior performance when contrasted with ML techniques [12] [13]. Consequently, the deep learning method is used in this research for classification. A DL approach is currently employed in a variety of computer science disciplines. One example is the widespread use of LSTM in speech recognition & NLP (Natural Language Processing) [14][15]. A CNN is employed for computer vision and image recognition. ML models utilize a limited no. of packet features; however, the accuracy & outcome results undergo a decline as no. of packet features increases [16-18]. This study aim's aims to generate a detection method, which can identify and mitigate DDoS attacks in real-time using CNNs' capabilities. This is done to improve the detection of attacks in SDN with the use of the DL framework. Our contributions to this paper are summarised below.

- Our methodology for detecting DDoS attacks in SDN using CNNs in DL has three primary contributions. Initially, we create a secure and efficient authentication mechanism that ensures that only legitimate nodes can access network services, while also balancing performance and security. We evaluate this mechanism to minimize performance degradation by assessing its impact on throughput, reliability, and network overhead.
- Subsequently, we developed a detection system based on CNNs to detect DDoS attacks. This entails the creation of an exhaustive attack database for model training, which enables CNN to differentiate between authentic & malicious traffic. The SDN controller incorporates the trained model to facilitate real-time detection and mitigation.
- Finally, we implement comprehensive assessments that quantify authentication speed, throughput, dependability, and network overhead through simulation tools. The advantages and prospective enhancements of our approach are underscored by a comparison of the results with existing methodologies.

The following paper is organized into several sections and subsections. In Section 2, the literature review recounts a study conducted by other researchers on this subject. The methodology offered in this study, as well as the tools & technologies employed, is detailed in Section 3. The proposed flowchart is also included. This section also addresses the CICDDoS2019 dataset, which is employed to train our model. The experimental setup

and investigations conducted to present results are detailed in Section 4. The project's conclusion & future work are discussed in Section 5.

2. Review of Literature

Recently, SDN has been frequently referred to as the "future of networking." The decoupling of the control plane from the data plane of networking devices is a primary reason for the rapid growth and massive success of this technology. The control plane enables the centralized administration of the whole network & switches, thus eliminating the necessity to configure every networking device. The data plane, which is composed of switching devices, enables the forwarding of network traffic by the policies established by the applications that operate above the programmed controller[19].

There have been numerous strategies for intrusion detection systems proposed by scientists in recent years, but there are scarcely any procedures for anomaly detection. These methods have been applied individually since early 2010 to detect attacks, resulting in increased false positive rates [20][21]. In 2015, they could detect DDoS attacks by integrating 2 intrusion detection methods, as we progressed to the next research phase [22]. The detection accuracy has been enhanced by these studies; however, the computational complexity and resource consumption have increased.

Subsequently, a study was conducted to identify and select appropriate features that decrease the detection time, thereby simplifying the process [23]. A different study [24] used a range of time series methodologies to forecast attacks using DDoS by forecasting the behavior of traffic characteristics during an attack via the use of anomaly scores. The model categorized traffic as either normal or an attack based on the scores. This paper [25] introduces a new method for the detection of DDoS attacks that employs Lattice Structural access rates. The method is referred to as S2RF2S for feature filtering and employs a "SxB2IN2 (Soft-Max Behaviour-Based Ideal Neural Network)" for classification. The work was able to detect DDoS attacks with 90 percent accuracy. In additional investigation [26], the algorithms of "Support Vector Machine (SVM), Logistic Regression (LR), Long-Short Term Memory (LSTM), K-Nearest Neighbour (KNN), and Random Forest (RF)" were implemented to emphasize the importance of featureselection to achieve precise & effective identification. In comparison to former research, the RF classifier was capable of achieving 99% accuracy in DDoS detection with eleven features. A model for detecting DDoS attacks in SDN was constructed using a Spark

utility [27]. The DT (Decision Tree) has demonstrated the highest accuracy among other algorithms, with a score of 93.6 percent. Consequently, DT was chosen for real-time deployment. In an additional investigation [28], the LSTM model, which is frequently employed, was implemented to

Table 1
Analysis of different State of Art Method in 5G Security

Title	Method	Outcome	Remarks
Fast Authentication in 5G HetNet through SDN Enabled Weighted Secure-Context-Information Transfer[31]	Weighted secure context information (SCI) transmission is used in a rapid authentication system provided by software defined networking (SDN) to increase authentication efficiency during changeover and satisfy 5G latency requirements.	99% accuracy in Authentication along with only 3% increase in latency	Authentication increases latency and may hamper the network performance
CRC-Based Message Authentication for 5G Mobile Technology[32]	Cyclic reundancy check based Authentication method	Up to two bit error correction and authentication	Change in user's Equipment location may hamper the authentication procedure due limited set of generator polynomial equations
IDS for mobile cloud computing in heterogeneous 5G[33]	Context information based intrusion detection system	Comparative analysis shows improved results of IDS detection	The results of IDS detection are limited with predefined synthetic dataset strategy
SDN in Wireless Mobile Networks[34].	SDN, authentication using , multiple features based on netowkr logs	Improved authentication process	Limited set of features are considered for authentication
An Extensible and Virtualization-Compatible IDS Management Architecture[35].	Intrusion detection management application	Improved IDS detection	Authentication process is limited with set of features considered

identify undesirable flows in distributed SDN-based edge computing. Through a collaborative prediction algorithm, the CoWatch framework achieved 93.30% accuracy in the prediction and detection of DDoS attacks also their corresponding attack patterns. This was demonstrated in extensive experiments conducted on 5 distinct datasets with 3 common attack categories.

SDN-based classification system with 3 models—a gated RNN, in particular, "as their primary model"—was created by the study done by [29].

The interface GRU-RNN (Gated Recurrent Units-RNN) obtained 89% accuracy when using the NSL-KDD dataset & 99% when using the CICIDS2017 dataset. 2 DL models were implemented in CICDDoS2019 dataset in research of ref. [30].

Above table 1 provides a comparative analysis of various state-of-the-art methods aimed at enhancing security in 5G networks. It evaluates methods based on their approach, outcomes, and associated limitations.

2.1 *Research Gaps*

Several research gaps remain in SDN IDS, despite the tremendous progress in this area. Intrusion detection is the primary focus of numerous strategies, with anomaly detection receiving minimal attention. The intricacy and rapidity of contemporary malevolent behaviors, as well as the vast scope of contemporary networks, frequently present challenges to these extant strategies[36][37].

In this study, we employ CNNs to overcome the constraints of previous DDoS detection methods. The capacity of CNNs to autonomously learn and extract hierarchical features from raw input data renders them well-suited for the identification of complex patterns in network traffic data[38]. We aim to optimize the efficacy of DDoS detection in SDN by utilizing CNNs, thereby attaining a balance between real-time applicability, computational efficiency, and detection accuracy. This method addresses the identified research voids and offers a more comprehensive and adaptive solution to the challenges presented by DDoS attacks in SDN environments.

3. Research Methodology

This section presents the suggested methodology for detecting DDoS attacks in SDN. The study enhances the field by developing a DL-based

model for classification and aims to enhance the accuracy of detection. Additionally, this section reviews a proposed flowchart.

3.1 *Problem Statement*

SDN provides substantial improvements in network management by decoupling the control plane from the data plane, which facilitates centralized control and increased flexibility. The objective of this research is to resolve these obstacles by creating a detection system that is based on a CNN and that leverages automated feature extraction and adaptability to enhance the accuracy & efficacy of DDoS detection in SDN.

3.2 *Proposed Methodology*

In this study, we have implemented a secure authentication mechanism to prevent unauthorized nodes from accessing network services. This initial phase is essential because it guarantees that only verified nodes are permitted to engage in network activities, thereby minimizing the likelihood of unauthorized access and potential attacks.

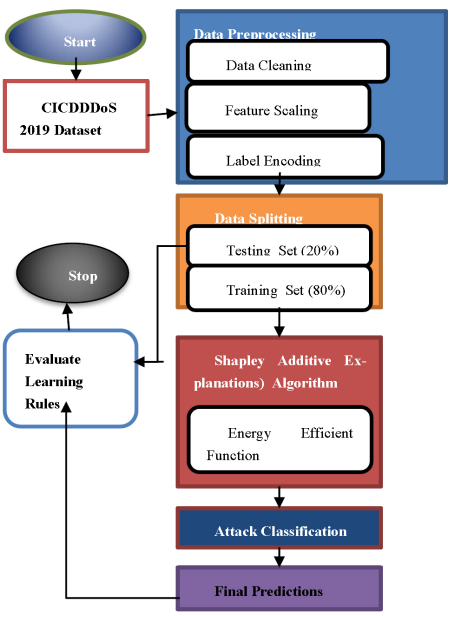

Figure 1

Illustration of the Proposed Methodology

By employing this comprehensive research methodology, we have created a DDoS detection system that is adaptable, efficient, and robust, thereby addressing the constraints of existing methods and improving the security of SDN environments.

In Figure 1 above, a flowchart of the suggested technique is shown. Consider several factors while evaluating possible authentication scenarios, including network overhead, authentication process speed (complexity), and throughput while adhering to dependability approaches. Consider the results with alternative approaches.

3.2.1 Data Gathering

The initial phase involves the acquisition of network data. This dataset, referred to as the CICDDoS2019 dataset, encompasses a variety of both legitimate and malicious network traffic.

3.2.2 Data Preprocessing

It is essential for the production of valuable and precise results in the field of ML. It improves the quality of data by addressing discrepancies, filtering out noise, and addressing missing or incomplete data.

3.2.3 Design and Development of the SHAP (Shapley Additive Explanations) Model

Attack Database Creation. Create an exhaustive database that catalogs the various known patterns of DDoS attacks by compiling the attack database [39]. The CNN model *is* trained to accurately recognize and classify various categories of attacks using this database as its foundation.

SHAP (Shapley Additive Explanations) *Architecture Design.* We have *implemented* a CNN architecture that has been expressly designed to analyze network traffic. SHAP (Shapley Additive Explanations) are a kind of Neural Network that has demonstrated exceptional performance in a variety of computer vision and image processing challenges [40].

In the architecture illustrated in figure 2, the subsequent definitions pertain to distinct layers. SHAP (Shapley Additive Explanations) is a form of DL algorithm that is employed to analyze data that is spatially or temporally related.

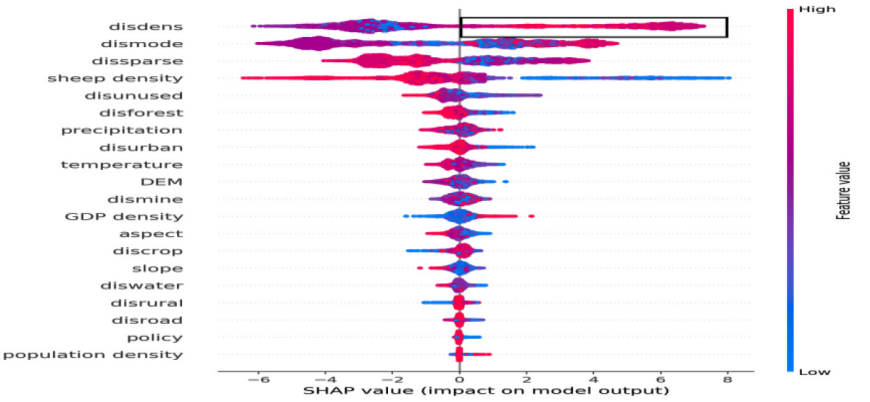

Figure 2

SHAP (Shapley Additive Explanations)

Implementation in SDN Environment

Pseudo-code for Proposed (SHAP (Shapley Additive Explanations) Algorithm

Input: Best Features (χ_{best})

Output: Attack classification

Step 1-Begin

Step 2-Initialize the parameters $\omega_{xy}, \eta_x, \varsigma_y,$ maximum iteration $Itr_{\max}$

Step 3-Set iteration $Itr = 1$

$$\text{While } (Itr \le Itr_{\max})$$

Step 4-For each layer do

Step 5-Evaluate attack detection function $\varepsilon(v(\chi_{best}), \tau, \delta)$

$$\varepsilon(v(\chi_{best}), \tau, \delta) = -\sum_{x=1}^{n} \eta_x v_x - \sum_{y=1}^{m} \varsigma_y \tau_y - \sum_{x=1}^{n} \sum_{y=1}^{m} v_x \omega_{xy} \tau_y \delta_z$$

Step 6-Compute joint probability function $P(v, \tau, \delta)$

Step 7-Evaluate Learning rules

$$\frac{\partial \log P(v|\phi)}{\partial \omega_{xy}} = \langle v_x \tau_y \rangle_{\text{data}} - \langle v_x \tau_y \rangle_{\text{model}}$$

Step 8-End For

Step 9-End While

Step 10-Return Attack classification

Step 11-End

Here (χ_{best}) =Best Features

$\omega_{xy}, \eta_x, \varsigma_y$ = Parameters

$Itr_{\max}$ = Maximum fitness evaluation

$\varepsilon(v(\chi_{best}), \tau, \delta)$ = Attack Detection Function

$\rho f_{uv}^{T+1} = u^{th}$ flamingo in the v^{th} dimension

4. Evaluation and Testing

This section presents the evaluation and testing of the study with different subsections i.e., simulation tools, performance metrics, and experimental results.

4.1 *Simulation Tools*

Simulation tools are implemented to establish a controlled SDN environment to comprehensively assess the performance of a SHAP (Shapley Additive Explanations)-based DDoS detection system. These tools simulate real-world network conditions by generating both normal and malicious traffic.

4.2 *Experimental Results*

This DDoS detection technique based on SDN should be more suitable for real-world business applications, for example intricate process interactions or a multitude of probable explanations, that necessitate extended simulations, a greater population of optimization candidates, and further optimization repetitions.

The Low Rate Attack Scenarios of SDN-based DDoS assaults are illustrated in the graph. Figure 3 illustrates how the range of DDoS attack traffic rates in each scenario permits variations between average rate and low-rate assault scenarios.

The figure 4 compares DDoS attack rates, successful mitigation percentages, and failure rates across Traffic Analysis, Server Seizures, Deanonymization, and SDN Flood Rate. Success Rate of Shaply Additive

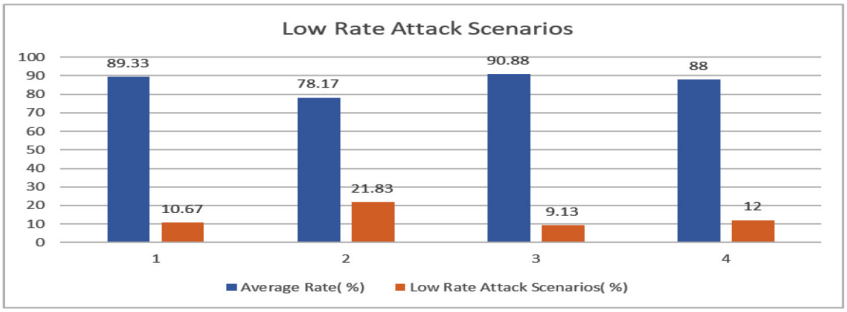

Figure 3

SDN-based DDoS attack scenarios with low attack rates

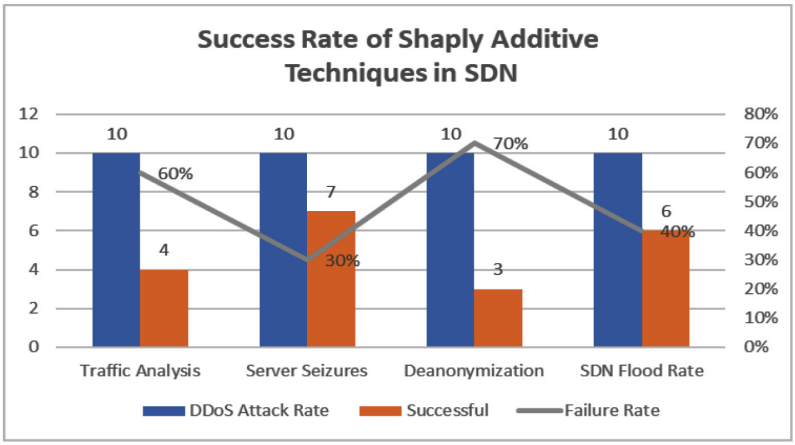

Figure 4

Success Rate of Shaply Additive Techniques in SDN for Different Attack Scenarios

Techniques in SDN for Various Attack Scenarios: This figure represents the success rate of Shaply Additive Techniques in countering different attacks in Software-Defined Networking (SDN). The bar chart indicates the DDoS attack rates (in blue), the rates of successful mitigation (in orange), and failure rates (in gray) for four types of attacks: Traffic Analysis, Server Seizures, Deanonymization, and SDN Flood Rate. Notable trends include a very high success rate of 70% for Deanonymization and a well-balanced success-to-failure ratio for SDN Flood Rate.

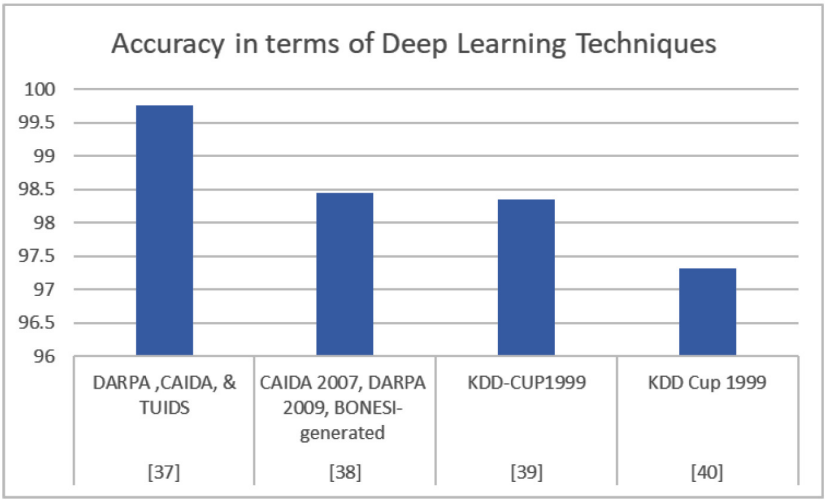

Figure 5

Methods of detecting DDoS attacks

Detection rates of various IDS with various dataset are shown in figure 5. The results demonstrate the model's good detection performance across many datasets, with the first study achieving the highest detection rate in comparison to others.

Table 2

Encoding and Decoding time comparison of EB-SFE

Method	Encoding Time (ms)	Decoding Time (ms)
Proposed SHAP (Shapley Additive Explanations)	3214	3219
Symbolic Feature Extraction and Encoding	7658	7753
Feature Extraction	8897	8779
Manual Encoding	12672	12314
ASCII-based Encoding	15647	15245

Here, to improve the Migration Behaviour, an Interpolation technique will be used in the existing SFE Encoding Algorithm as shown in table 2. And also, this proposed algorithm will be compared with some other existing algorithms such as Frequency Encoding, Manchester Encoding,

Grey wolf Optimization Algorithm, and ASCII Encoding using result parameters such as Encoding Time vs Decoding Time and Memory Usage, etc. After that, selected feature data will be split into 80% of training data and 20% of testing data.

5. Conclusion and Future Scope

This research effectively establishes a comprehensive methodology for improving the security of SDN environments in the face of DDoS attacks. The initial phase was dedicated to the creation of a secure authentication mechanism that would restrict network services to verified nodes, thereby minimizing the likelihood of unauthorized access. Evaluations have verified that this mechanism has a minimal impact on network throughput as well as overhead, and it was intended to be both efficient and robust. A sophisticated DDoS detection system was devised in the subsequent phase, which was based on SHAP (Shapley Additive Explanations).

Furthermore, it would improve the overall security of SDN environments by broadening the detection system's scope to encompass other types of network attacks, in addition to DDoS. A more comprehensive defense strategy could be achieved by integrating the proposed methodology with other security measures, like anomaly-based IDS.

References

[1] R. Priya, R. Selvakumari, K. R. Chandrakala, S. Krithika, H. Rai, and K. Binith Muthukrishnan, "Analyzing cryptographic protocols to strengthen HR information security," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 8, pp. 2495–2509 (2024). DOI: 10.47974/JDMSC-2134.

[2] K. Kavita, R. Kulkarni, A. H. Prasad, B. Jeyakumar, M. Thaile, and S. Gore, "A novel optimization-based blockchain technology using health care data for enhancing security and privacy in the medical system," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 8, pp. 2483–2494 (2024). DOI: 10.47974/JDMSC-2132.

[3] M. Shrestha, Y. Kim, J. Oh, J. Rhee, Y. R. Choe, F. Zuo, M. Park, and G. Qian, "ProvSec: Open cybersecurity system provenance analysis benchmark dataset with labels," *International Journal of Network*

and Distributed Computing, vol. 11, pp. 112–123 (2023), doi: 10.1007/s44227-023-00014-9.

[4] H. C. Huang, C. H. Tsai, and H. C. Lin, "Development of 5G Cyber-Physical Production System," *International Journal of Network and Distributed Computing*, vol. 11, pp. 9–19 (2023). DOI: 10.1007/s44227-022-00003-4.

[5] S. K. Zaw and S. Vasupongayya, "Enhancing Case-based Reasoning Approach using Incremental Learning Model for Automatic Adaptation of Classifiers in Mobile Phishing Detection," *International Journal of Network and Distributed Computing*, vol. 8, pp. 152–161 (2020).

[6] M. Dandotiya and R. R. S. Makwana, "DDoS Attack Detection and Mitigation in SDN Environment: A Deep Learning Perspective," 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), vol. 2, pp. 1–6 (2024).

[7] M. Dandotiya, P. Rahi, A. Khunteta, A. Anushya, and S. S. Ahmad, "SAFE: A Secure Authenticated & Integrated Framework for E-learning," in Proceedings of the 4th International Conference on Information Management & Machine Intelligence (ICIMMI '22), Association for Computing Machinery, New York, NY, USA, Article 89, pp. 1–9 (2023). DOI: 10.1145/3590837.3590926.

[8] S. Arvind, B. Unhelkar, S. S. Shankar, P. Chakrabarti, and S. V. Devika, "Advancing cyber threat detection through deep learning in management information systems," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 8, pp. 2409–2417 (2024). DOI: 10.47974/JDMSC-2014.

[9] K. Kaur, S. Chakraborty, and A. K. Sagar, "Unleashing a cascade of machine learning for turbocharged sequence alignment in discrete mathematical sciences using GPU," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 4, pp. 1129–1138 (2024). DOI: 10.47974/JDMSC-1968.

[10] M. J. Jaber, Z. J. Jaber, and A. J. Obaid, "An efficient hybrid chaotic map-based encryption technique for multiple image security systems," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 5, pp. 1507–1522 (2024). DOI: 10.47974/JDMSC-1934.

[11] S. Agha and O. Rehman, "Improving Discrimination Accuracy Rate of DDoS Attacks and Flash Events," (2020).

[12] C. Li, Y. Wu, X. Yuan, Z. Sun, W. Wang, X. Li, and L. Gong, "Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN," *International Journal of Communication Systems,* vol. 31, no. 2, p. e3497 (2018), doi: 10.1002/dac.3497.

[13] O. Rahman, M. A. G. Quraishi, and C. H. Lung, "DDoS attacks detection and mitigation in SDN using machine learning," (2019).

[14] A. Örsdemir, H. Nazari, and D. Akgün, "DDoS Attack Detection on SDN with Conv1D and LSTM," EasyChair Preprint (2022).

[15] N. P. Mwanza and J. Kalita, "Detecting DDoS Attacks in Software Defined Networks Using Deep Learning Techniques: A Survey," *International Journal of Network Security* (2023).

[16] G. Nawaz et al., "Detecting and Mitigating DDoS Attacks in SDNs Using Deep Neural Network," *Computers, Materials & Continua* (2023).

[17] D. M. Rajan and D. D. J. Aravindhar, "Detection and Mitigation of DDoS Attack in SDN Environment Using Hybrid CNN-LSTM," Migration Letters (2023).

[18] 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 (2023).

[19] V. K. Singh, "DDoS attack detection and mitigation using statistical and machine learning methods in SDN," M.S. thesis, Coll. Irel. (2020).

[20] S. Sadeghpour, N. Vlajic, P. Madani, and D. Stevanovic, "Unsupervised ML based detection of malicious web sessions with automated feature selection: Design and real-world validation," (2021).

[21] S. Lee, G. Kim, and S. Kim, "Sequence-order-independent network profiling for detecting application layer DDoS attacks," *Eurasip Journal on Wireless Communications and Networking* (2011).

[22] M. A. Ribeiro, M. S. Pereira Fonseca, and J. de Santi, "Detecting and mitigating DDoS attacks with moving target defense approach based on automated flow classification in SDN networks," *Computers & Security* (2023).

[23] B. Venkatesh and J. Anuradha, "A review of Feature Selection and its methods," *Cybernetics and Information Technologies* (2019).

[24] R. F. Fouladi, O. Ermiş, and E. Anarim, "A DDoS attack detection and defense scheme using time-series analysis for SDN," *Journal of Information Security and Applications* (2020).

[25] K. Karthick, G. Kiruthiga, P. Saraswathi, B. Dhiyanesh, and R. Radha, "A Subset Scaling Recursive Feature Collection Based DDoS Detection Using Behavioural Based Ideal Neural Network for Security in A Cloud Environment," (2022).

[26] H. Alubaidan, R. Alzaher, M. AlQhatani, and R. Mohammed, "DDoS Detection in Software-Defined Network (SDN) Using Machine Learning," *International Journal of Cybernetics and Informatics* (2023).

[27] S. S. Samaan and H. A. Jeiad, "Feature-based real-time distributed denial of service detection in SDN using machine learning and Spark," Bulletin of Electrical Engineering and Informatics (2023).

[28] H. Zhou, Y. Zheng, X. Jia, and J. Shu, "Collaborative prediction and detection of DDoS attacks in edge computing: A deep learning-based approach with distributed SDN," Computer Networks (2023).

[29] T. A. Tang, D. McLernon, L. Mhamdi, S. A. R. Zaidi, and M. Ghogho, "Intrusion detection in SDN-based networks: Deep recurrent neural network approach," *Advanced Sciences and Technologies for Security Applications* (2019).

[30] T. Khempetch and P. Wuttidittachotti, "DDoS attack detection using deep learning," *IAES International Journal of Artificial Intelligence* (2021).

[31] X. Duan and X. Wang, "Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer," in Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, pp. 1–6 (2016).

[32] E. Dubrova, M. Näslund, and G. Selander, "CRC-Based Message Authentication for 5G Mobile Technology," in Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, pp. 1–8 (2015).

[33] K. Gai, M. Qiu, L. Tao, and Y. Zhu, "Intrusion detection techniques for mobile cloud computing in heterogeneous 5G," Security and Communication Networks (2015).

[34] A. Y. Ding, J. Crowcroft, S. Tarkoma, and H. Flinck, "Software defined networking for security enhancement in wireless mobile networks," *Computer Networks*, vol. 66, pp. 94–101 (2014).

[35] S. Roschke, F. Cheng, and C. Meinel, "An Extensible and Virtualization-Compatible IDS Management Architecture," in Proceedings of the 2009 Fifth International Conference on Information Assurance and Security (IAS), Xi'an, China, pp. 130–134 (2009).

[36] C. V. Gonzalez Zelaya, "Towards explaining the effects of data preprocessing on machine learning," 2019 IEEE 35th International Conference on Data Engineering (ICDE) (2019).

[37] T. Peng, C. Leckie, and K. Ramamohanarao, "Proactively detecting distributed denial of service attacks using source IP address monitoring," in Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 1–12 (2004).

[38] J. Cheng, J. Yin, C. Wu, B. Zhang, and Y. Liu, "DDoS attack detection method based on linear prediction model," Emerging Intelligent Computing Technology and Applications: 5th International Conference on Intelligent Computing, ICIC 2009, Ulsan, South Korea, September 16-19 (2009).

[39] M. Dandotiya and R. R. S. Makwana, "Secured DDoS Attack Detection in SDN Using TS-RBDM With MDPP-Streebog Based User Authentication," *Transactions on Emerging Telecommunications Technologies*, vol. 36, no. 2,p. e70052 (2025), doi: 10.1002/ett.70052.

[40] A. Naithani, S. N. Singh, K. Kant Singh and S. Kumar, "Machine Learning forCloud-Based DDoS Attack Detection: A Comprehensive Algorithmic Evaluation," 2024 14th International Conference on Cloud Computing, DataScience & Engineering (Confluence), Noida, India, pp. 561-567 (2024), doi: 10.1109/Confluence60223.2024.10463504.

Received October, 2024