HYBRID DEEP LEARNING APPROACH FOR ENHANCED DETECTION AND MITIGATION OF DDOS ATTACK IN SDN NETWORKS

Ahlam Alsufyani, Bashayer Alotaibi and Samah Alajmani

Department of Information Technology, College of Computer and Information Technology, Taif University, PO Box. 11099, Taif 21994, Saudi Arabia

ABSTRACT

The pervasiveness of (DDoS) Distributed Denial of Service attacks has intensified the demand for effective and dependable detection methods in Software-Defined Networks (SDNs). This proposed study introduces a hybrid Deep Learning framework designed to identify and address DDoS attacks in Software-Defined Networking (SDN) contexts. Due to the centralization of SDN control planes, these networks are especially susceptible to DDoS attacks, which can saturate system resources and disrupt critical services. Utilizing the CICDDoS2019 dataset, this research integrates Recurrent Neural Networks (RNN), Deep Belief Networks (DBN), and Adaptive Feature Dimensionality Learning (AFDL) to improve detection accuracy and efficiency. In order to appropriately differentiate between attack and normal traffic, the proposed hybrid model combines both temporal dependencies and feature correlations achieving an accuracy of 99.80%. This research enhances SDN security by offering a scalable and reliable DDoS detection solution capable of adapting to real-time network requirements, addressing the prospective of DL in protecting network infrastructures.

KEYWORDS

Deep Learning, Software Defined Networking (SDN), Distributed Denial of Service (DDoS)

1. INTRODUCTION

To investigate DDoS attacks in SDN, a DDoS attack definition must first be established. A type of attack as DDoS is a hostile and damaging network attack that exhausts system resources, causing the system to stop working. It poses a major threat to the network since it can disable the available network services for users. DDoS attacks overload the network with traffic, take up network resources, and create congestion. Normal services are disrupted because of the network and servers becoming congested [1]. The purpose of this attack is to interrupt normal traffic flows. As a result, the network's capacity is exceeded, disrupting service for valid traffic [2], [3].

A significant denial-of-service (DDoS) attack on a top DNS provider was executed by the Mirai botnet in October 2016. Several hours were spent without internet access in many areas of the United States and Europe because of this attack, which also brought down well-known websites including Twitter, Netflix, and GitHub. Through the utilization of several compromised devices, the Mirai botnet produced previously unheard-of levels of traffic, overwhelming Dyn's DNS servers and blocking access to several well-known websites [3]. In recent years, SDN has become a revolutionary approach to network administration enabling centralized control over network structure. Compared to conventional networking topologies, this offers greater adaptability, scalability, and automation by allowing network administrators

to administer, configure, and optimize networks programmatically. DDoS attacks can cause fundamental network disruption in SDN systems by overloading the system with malicious data, which puts a strain on important assets like processing power and bandwidth. Frequently, this leads to decreased network efficiency or even complete disruptions in service. SDN is particularly susceptible to DDoS attacks because it has a centralized control plane to administer the entire network, which allows the impact to propagate throughout the entire infrastructure rather than being localized. Because of this concentration, attackers can more easily inflict extensive harm by flooding the system with unauthorized requests. To detect DDoS attacks in SDN, several non-DL techniques have been applied, like packet transfer techniques and real-time detection techniques. All these techniques have been explored in research papers focusing on traditional, non-machine learning strategies for identifying DDoS traffic. For example, packet entropy techniques assess irregularities in traffic randomness, while time-based detection identifies sudden changes in traffic volume over specific intervals [4],[5], the implementation of DL methods in particular has the potential of greatly enhancing the efficacy of safety tools for SDN networks [6].

The algorithms presented in this research combine CNN and MLP architectures with feature selection and improvement techniques to increase the detection results of DDoS attacks. This method improves the model's DDoS attack detection capabilities, leading to high accuracy in the SDN context. Our method was competent to offer a more thorough and reliable examination of the security issues that SDN networks face. A hybrid DL approach that integrated several algorithms was an essential part of our research in order to increase the precision and effectiveness of our investigation.

This was in contrast to other systems that relied on a single algorithm, which may not have been as dependable or capable of dealing with the quality and volatility of real-time data. Our goal in employing a hybrid approach was to offer a more dependable and potent way to detect and mitigate DDoS attacks. Proposed study suggested a significance contribution to the detection and mitigation of attacks in SDN networks by introducing a hybrid approach DL method which integrates various methods and dataset to enhance both quality and result efficiency. The suggested method manages the complexity and unpredictability of real-world problems while detecting various DDoS attacks in a novel way. The consequences mention the possibilities for further developments in this area and show how well DL works to deliver the safety and security issues.

This paper's remaining portion is organized as follows: The collection of data, preparation methods, feature selection strategies, and the building of the hybrid DL approach—which combines (AFDL), (RNN), and (DBN)—are all covered in Section 2's research approach. **Section 3** presents the results of the model's results, focusing on detection accuracy and other metrics. **Section 4** concludes with a discussion of these findings, highlighting the practical implications for DDoS detection in SDN environments and suggesting avenues for future research.

1.1. Related Works

Standard DDoS attacks are a major threat to network security, disrupting by overwhelming network resources. Deep learning has become a very effective technology to detect these attacks by analyzing large datasets and identifying complex patterns in network traffic. In this chapter, we review the existing research work and discuss how various researchers have proposed deep learning-based solutions to detect and identify against DDoS attacks in Software-Defined Networking (SDN) environments. The review covers a range of techniques, including the integration of multiple algorithms to improve detection accuracy and efficiency.

Elsayed et al. [7] propose an advanced study to detecting (DDoS) attacks or attacks in Software-Defined Networking (SDN) environments. The primary innovation of the paper lies in its use of a deep learning methodology that merge a Recurrent Neural Network (RNN) with an autoencoder to detect malicious network traffic effectively. This addresses the boundary of traditional Machine Learning (ML) techniques, which often struggle with large and dynamically changing datasets and exhibit high false alarm rates when detecting previously unseen attack patterns.

The authors leverage the recently released CICDDoS2019 dataset, which consists various DDoS attack types not commonly found in earlier datasets. By training the model on this comprehensive dataset, DDoSNet achieves high accuracy and minimizes the loss of temporal information, which is critical in detecting attacks in real-time network traffic. The evaluation of the model demonstrated superior performance with an accuracy rate of 99% and high precision, recall, and F1-score. These results significantly outperform classical ML approaches such as Decision Trees (DT), Support Vector Machines classification (SVM), Naive Bayes techniwue (NB), and Logistic Regression and classification (LR).

While the model demonstrates strong results, the authors acknowledge several areas for future research. Currently, the model is limited to binary classification, identifying only between normal and attack traffic, without identifying specific types of DDoS attacks. Expanding the model to handle multi-class classification could enhance its applicability in real-world scenarios. Additionally, the authors recommend testing the model on other datasets and simulating more diverse SDN environments to ensure the model's robustness across different network conditions.

One of the key strengths of this work is the advanced use of an RNN-autoencoder, which allows for effective anomaly detection in time-series data, a important feature of intrusion detection. Furthermore, the use of the CICDDoS2019 dataset ensures that the model is evaluated against the most recent and comprehensive types of DDoS attacks, making the findings relevant and up to date. However, the model’s dependency on a specific dataset and its limitation to binary classification highlight areas for improvement in future studies. In conclusion, the proposed DDoSNet model marks a significant advancement in the field of DDoS detection, especially in SDN environments, and sets the stage for future research aimed at enhancing multi- class detection capabilities and generalizing the model to diverse network traffic scenarios.

Alghazzawi et al. [8] propose an efficient detection system for (DDoS) attacks, utilizing a hybrid deep learning model enhanced with improved feature selection techniques. The authors highlight the increasing complexity and frequency of DDoS attacks, which overwhelm network resources and compromise the availability of services. Traditional DDoS detection methods, including statistical and machine learning approaches, often struggle with feature selection, leading to reduced performance in real- world scenarios. To address this, the recent model combines (CNN) with (BiLSTM), leveraging a chi-squared (χ^2) test to determine which traits are most essential to DDOS attack detection.

The CICDDoS2019 dataset, which comprises a range of DDoS attack types, was used to assess the model. According to the results, the CNN-BiLSTM hybrid model outperformed conventional machine learning classifiers like SVM and RF by a wide margin, achieving an accuracy of 94.52% with the improved feature selection procedure. The model’s overall advance performance is attributed to its ability to effectively capture both spatial and temporal features of the network traffic, thanks to the CNN’s feature extraction capabilities and

BiLSTM's ability to preserve sequential information. Additionally, the study emphasizes the importance of proper feature selection in improving detection accuracy.

Belarbi et al. [9] suggest an intrusion detection system (IDS) that uses Deep Belief Networks (DBNs) to detect cyber network attacks of connected devices. The research addresses the growing challenge of zero-day attacks, which traditional signature-based IDS methods struggle to detect due to the time-consuming process of generating new attack signatures. Instead, the authors employ DBNs, a type of deep learning model that excels at learning high-dimensional representations and detecting complex attack variants in real- time.

The study uses the CICIDS2017 dataset, which includes traffic and twelve different types of attacks. Given the inherent class imbalance in this dataset, where benign samples dominate, the authors applied various class balancing techniques, including (SMOTE) and random under sampling, to improve the model's performance in detecting minority attacks. The DBN-based IDS demonstrated superior performance, particularly in detecting underrepresented attack types, achieving an F1-score of 94%, a significant improvement over traditional Multi-Layer Perceptron (MLP) models, which achieved an 87.3% accuracy.

The authors conclude that DBNs offer a promising approach to intrusion detection, particularly in networks with class-imbalanced traffic. By pre-training DBNs in an unsupervised manner and finetuning them with backpropagation, the system achieves great accuracy in detecting both common and rare attacks. This approach is particularly effective in environments with connected devices, where attack patterns can vary widely, and real-time detection is essential for mitigating the impact of zero-day vulnerabilities.

Gebremeskel et al. [10] propose a hybrid approach to identify the increasing issue of Distributed Denial of Service (DDoS) attacks in Software-Defined Networks (SDN), specifically targeting multi-controller environments. Due to SDN's centralized control plane, DDoS attacks can overwhelm the controller, severely disrupting network functionality. The main objective of this study to improve both the detection and classification of these attacks. The proposed model begins with an entropy-based detection mechanism, which monitors traffic behavior in real-time by measuring the entropy of destination IP addresses. Significant variations in entropy indicate abnormal traffic patterns that are likely the result of a DDoS attack.

Once an anomaly is detected, the flagged traffic is passed to a deep-learning-based classifier, specifically a Long Short-Term Memory method (LSTM) network. This classifier distinguishes between various types of DDoS attacks, such as SYN floods and UDP floods, allowing for more precise mitigation strategies. The use of LSTM enhances the model's ability to identify patterns in sequential data, improving classification accuracy.

The study's experiments, conducted using the CICDDoS2019 dataset, show that the hybrid model performs exceptionally well, achieving an accuracy of 99.42% for attack detection. The integration of the chi-squared ($\chi 2$) test for feature selection further refines the model by reducing irrelevant data, enhancing both speed and efficiency. Compared to other models, the proposed LSTM-based classifier demonstrated superior performance in a multi-controller SDN environment.

Overall, the hybrid approach addresses key limitations in existing DDoS detection systems, particularly in multi-controller SDNs, by providing both high detection accuracy and scalability. The model's combination of entropy-based detection with deep-learning

classification ensures that attacks are detected early and categorized effectively, making it a valuable contribution to network security research.

Mansoor et al. [11] propose a hybrid deep learning approach objective to detection of (DDoS) attacks on the (SDN) controller. SDN offers significant flexibility and enhanced network management. However, its centralized control plane makes it highly accountable to DDoS attacks, which can overwhelm the controller, leading to service disruption. The authors address this issue by developing a robust detection mechanism utilizing Recurrent Neural Networks (RNNs).

The proposed method operates in three key stages: data preprocessing, feature selection, and the implementation of an RNN model. Data preprocessing prepares the dataset for analysis by cleaning and normalizing it. In the feature selection phase, techniques like Information Gain Ratio (IGR) and Chi-square are employed to identify the most informative features relevant to DDoS detection. This selection significantly enhances detection accuracy by eliminating irrelevant features.

The evaluation of the proposed approach yielded promising results, with the RNN model attain an average detection of 94.18% accuracy, a precision of 92.15%, a false positive rate (FPR) of 8.11%, and an F1-score of 94.28%. These metrics indicate that the method is both effective and reliable in identifying DDoS attacks.

Overall, the study demonstrates that deep learning techniques, particularly RNNs, can significantly improve the detection of DDoS attacks on SDN controllers. However, the paper also acknowledges certain limitations, such as the need to explore different deep-learning models and improve hyperparameter tuning, which could enhance the model's performance in future research.

Zhou et al. [12] propose CoWatch, a framework for predicting and detecting DDoS attacks in Edge Computing environments, leveraging distributed (SDN) controllers and (LSTM) models. The primary goal of the framework is to address the vulnerability of edge nodes to DDoS attacks by providing a collaborative and predictive defense mechanism. CoWatch combines LSTM-based prediction models with distributed SDN controllers to detect suspicious network traffic patterns in real time, enabling proactive attack mitigation.

The framework introduces an optimal threshold model that reduces communication overhead between controllers, making the system more scalable without sacrificing detection accuracy. This feature ensures that controllers only exchange necessary information, improving synchronization efficiency across the network. By predicting potential DDoS attacks before they fully develop, CoWatch provides early detection and a timelier response to mitigate attacks.

While the results are promising, the authors acknowledge that further research is needed to optimize the system for more complex real-world environments. Particularly, refining the threshold model and exploring more advanced machine-learning techniques could enhance the system's adaptability and resilience in dynamic network conditions.

In conclusion, CoWatch provides a scalable and efficient solution for detecting and mitigating DDoS attacks in EC environments, with the added benefit of predictive capabilities, making it a valuable contribution to edge computing security.

A hybrid deep learning method for identifying (DoS) and Distributed Denial-of-Service (DDoS) attacks in SDNs is proposed by Elubeyd and Yiltas-Kaplan [14], Because of their centralized control design, SDNs are particularly vulnerable to DDoS attacks, which can cause network disruption by attacking the control plane. The authors created a hybrid model to tackle this problem by combining three different kinds of deep learning algorithms: Dense Neural Networks (DNN), (GRU), and 1D Neural Networks (CNN). By increasing both short-term feature extraction and long-term pattern identification in network data, this combination seeks to increase attack detection accuracy.

The CNN component of the model is used by feature selection, identifying patterns in the network traffic data that might indicate a potential DDoS attack. The GRU focuses on capturing long-term dependencies in the traffic, making it effective in detecting attacks that evolve. Finally, the DNN classifies the traffic as malicious based on the features learned by the CNN and GRU.

The model was tested on two datasets, including CIC-DDoS2019, where it achieved impressive accuracy measures of 99.8% and 99.82% on both datasets. These results indicate the model's ability to accurately distinguish between normal and malicious traffic in SDN environments. The hybrid model was shown to outperform individual models such as GRU and CNN-based approaches, further demonstrating its effectiveness in DDoS detection.

This study highlights the importance of combining different Machine learning models to improve detection accuracy. By investing the strengths of CNN for feature extraction, GRU for handling sequential data, and DNN for classification, the hybrid model provides a more robust solution for detecting both low-rate and high-volume DDoS attacks. The authors note that this approach significantly reduces false positives and can be effectively applied to real-world SDN environments.

In conclusion, this hybrid deep learning approach offers a scalable and highly accurate solution for detecting DoS attacks in SDNs, achieving superior results compared to traditional models. The authors suggest that further research could focus on refining the model to handle more complex network environments and adapting it to other types of cyberattacks.

Priyadarshini et al. [15] present a hybrid deep learning model, Given the exponential growth of IoT devices, which are typically less secure and more vulnerable to DDoS attacks, and the increasing reliance on SDNs, where the centralized control plane is a prime target, there is a pressing need for an effective detection mechanism. The proposed model integrates (Bi-LSTM), capable of capturing temporal dependencies in network traffic by analyzing sequences of data from both past and future traffic flows, with (CNN), which excels at extracting spatial features that help identify critical patterns in traffic. Additionally, an attention mechanism is incorporated, which prioritizes the most significant features in the data. The hybrid model was tested on two comprehensive datasets: the Application Layer DDoS Dataset and the SDN DDoS Dataset, achieving remarkable accuracy rates of 99.74% for application layer attacks and 99.98% for SDNbased DDoS attacks. The model's ability to detect both low-rate and volumetric DDoS attacks, which are often more challenging for conventional detection systems, is particularly noteworthy. By combining the strengths of Bi-LSTM for temporal analysis and CNN for feature extraction, alongside the attention mechanism, the model proves to be a highly efficient and scalable solution, suitable for deployment in real-world SDN and IoT environments, where the complexity and frequency of DDoS attacks are steadily increasing. The study concludes that this hybrid deep learning model offers significant promise in enhancing network security, providing a robust defense against a wide range of DDoS attacks.

Clinton et al. [16] introduce a deep learning-based solution to identify and classify Distributed Denial of Service (DDoS) attacks within (SDNs), which are particularly vulnerable to such attacks due to their centralized control plane architecture. The authors propose a unique method that converts raw network traffic data into image representations, which are then classified using a Convolutional Neural Network (CNN). By transforming network traffic into image data, the model leverages CNN's advanced feature extraction capabilities, enabling it to detect subtle patterns and anomalies that signify DDoS attacks. This approach allows for more accurate classification of network traffic, improving overall detection performance.

The proposed model was evaluated using three datasets: a simulated test-bed dataset, CTU-13, and InSDN. Across all three datasets, the model achieved an accuracy rate exceeding 99%, along with high precision, recall, and F1 scores classification evaluation metrics. This performance illustrates the model's robustness in distinguishing between benign and malicious traffic while minimizing false positives. The authors compare their approach to other CNN architectures, including VGG, ResNet, and EfficientNet, as well as traditional machine learning techniques. The results show that the proposed method consistently outperforms these existing models, demonstrating its superior ability to detect DDoS attacks in real-world SDN environments.

One of the key innovations of this paper is the use of CNN for classifying image-based representations of network traffic, a novel technique that greatly enhances the model's capacity for feature extraction. This allows for better detection accuracy while processing large volumes of traffic data, a critical need for real- time DDoS mitigation in SDNs. By effectively protecting both the control and data planes, the model addresses one of the key security challenges in SDN architectures, offering a scalable and efficient solution for safeguarding networks against DDoS threats.

In conclusion, the paper highlights the potential of deep learning, particularly CNNs, in enhancing the security of SDNs against DDoS attacks. The use of image-based traffic classification represents a significant step forward in the field, providing both accuracy and scalability for real-time network protection.

A deep neural network (DCNN) model is proposed by Vanlalruata Hnamte and Jamal Hussain [17] (2023) for identifying and preventing DDoS attacks in Software-Defined Networks (SDNs). The paper emphasizes the increasing vulnerabilities in SDN environments due to the centralization of the control plane, which becomes a prime target for DDoS attacks. The authors address this issue by developing a detection model trained using three prominent datasets: InSDN, CIC-IDS2017, and CIC-DDoS2019. The model effectively detects real-time network anomalies by analyzing traffic flows within the SDN and triggering defense mechanisms as soon as anomalies are detected.

The proposed DCNN model eliminates the pooling layers typically used in traditional CNNs to ensure reduced training time and better performance. Instead, it leverages ReLU as the activation function and Softmax for classification. The paper highlights the importance of using deep learning methods for feature extraction and anomaly detection within SDN, as traditional methods are not efficient enough for complex, real-time traffic patterns. The InSDN dataset, specifically developed for SDN environments, was extensively used due to its inclusion of up-to-date attack patterns, making it an ideal choice for the model training process. Additionally, the authors evaluated the model's performance using CIC-IDS2017 and CIC-DDoS2019, which include both traditional and modern attack types.

Kimanzi et al. [19] present a deep review of hybrid deep learning algorithms employed in Intrusion Detection Systems (IDS) to enhance network security. The paper emphasizes the growing necessity of sophisticated intrusion detection mechanisms due to the rising number of cyberattacks. Traditional methods, such as signature-based systems, are criticized for their inability to detect novel and evolving threats. To address this, the authors explore a range of deep learning models including (CNN), (RNN), (LSTM), (DBN), (MLP), and autoencoders. Additionally, the review discusses the datasets commonly used to evaluate these models, such as KDDCup99 and NSLKDD, and calls for more diverse and up-to-date datasets to improve real scenarios problems and suggest applications.

Aslam et al. [20] conduct an extensive analysis of (ML) and deep learning (DL) approaches to detect (DDoS) attacks in Software-Defined Networking (SDN) environments. The authors present a taxonomy of DDoS defense solutions and categorize over 132 research articles that specifically focus on ML/DL-based solutions for SDN environments. One key limitation identified in traditional statistical and policy-based methods is the high rate of false positives and inefficiency in real-world scenarios. In contrast, ML and DL methods provide dynamic and effective solutions for DDoS detection.

The paper further highlights the need for SDN-specific datasets to enhance the accuracy of DDoS detection models. Existing public datasets, such as KDD'99 and CICIDS 2017, are used to evaluate many of the proposed models but are often found to be outdated or not representative of modern SDN architectures. Feature selection plays a significant role in improving detection accuracy, with techniques like Chi-square, Information Gain, and Genetic Algorithms being commonly applied. Among the ML approaches, (SVM), (DT), and (NN) are frequently utilized, while (LSTM) and (RNN) dominate DL approaches for detecting abnormal traffic patterns.

The results demonstrate that DL methods, particularly those involving RNNs, exhibit superior performance in terms of detection accuracy, thanks to their ability to model temporal dependencies in network traffic. Furthermore, the study identifies several gaps in current research, including the lack of robust, real-world datasets tailored for SDN and the need for further exploration of feature selection techniques to optimize detection performance in dynamic network environments.

Wang et al. [21] propose a hierarchical abnormal traffic detection system designed specifically for (SDNs). Their approach leverages a two-stage detection method combining statistical port data and a deep learning-based classifier, aiming to enhance the accuracy and to identify real-world and time-based (DDoS) attacks in SDNs. The model integrates a wavelet transform technique with a (CNN) and a Long Short-Term Memory technique (LSTM) network to capture spatial and temporal features of traffic data. The primary objective of the study is to improve the detection of abnormal traffic in SDNs, which are highly susceptible to attacks due to their centralized control architecture.

The authors evaluate their system using the InSDN dataset, which simulates SDN traffic and includes DDoS and other common attack types. The model achieved a detection accuracy of 99.83%, outperforming traditional methods like CNN-SoftMax and CNN-LSTM in terms of accuracy, recall, and false positive rates. The system is notable for its ability to handle both coarse and fine-grained detection, with an initial rough detection stage based on port characteristics, followed by more precise detection using traffic data. The hierarchical design ensures low computational overhead while maintaining high accuracy, enabling quick localization of attack sources in SDNs.

This method is significant because it addresses the unique vulnerabilities of SDNs, particularly the control plane, which can be paralyzed by DDoS attacks. By incorporating a two-stage detection approach, the system improves both detection speed and accuracy compared to single-stage models. Moreover, the use of wavelet decomposition allows for multi-scale analysis, which enhances the model's ability to detect complex attack patterns.

Compared to other DDoS detection methods, Wang et al.'s approach stands out for its hybrid use of CNN and LSTM, as well as its multi-scale analysis through wavelet transform. This combination allows the model to extract more intricate temporal and spatial features from network traffic, leading to superior performance in abnormal traffic detection. The study highlights the system's potential for real-time identification and mitigation of DDoS attacks in SDNs, contributing to the growing body of research on deep learning applications in cybersecurity.

The strengths of this approach include its attaining high accuracy, and the innovative use of wavelet transforms for feature extraction. However, the model requires substantial computational resources, particularly during the wavelet decomposition and CNN-LSTM processing stages. Future study could be focusing on optimal system's efficiency and applying it to larger, more diverse datasets to further validate its scalability.

This work contributes to the literature by providing a scalable and effective abnormal traffic detection system for SDNs, balancing real-time detection capabilities with high accuracy, which is essential for maintaining the security and stability of SDN environments.

Wang et al [23] propose a two-stage detection and mitigation system for Distributed Denial of Service (DDoS) attacks in (SDN) environments. The system tackles the high computational overhead and underutilization of features that often challenge traditional DDoS detection methods in SDN. The authors introduce a method that first performs coarse detection by analyzing statistical data from SDN switch ports and then refines the detection using a Multi-Dimensional Deep Convolutional Classifier (MDDCC) based on wavelet decomposition and convolutional neural networks (CNN). The MDDCC extracts time, frequency, and spatial features from suspicious traffic, enabling more precise anomaly detection.

Experimental results demonstrate that this method can quickly and accurately identify DDoS attacks using minimal statistical information, with superior accuracy compared to conventional detection techniques. Once the attack is detected, the system employs graph theory to trace the source of the attack and mitigates its impact by isolating the affected nodes, ensuring that legitimate traffic continues to flow through the SDN. The two-stage method effectively enhances the network’s resilience against cyber-attacks, while providing a robust mechanism for realtime detection.

2. METHOD

The Detection of (DDoS) attacks in (SDN) environments is improved by a hybrid dl model developed in this research. The methodology is inclusive of all the stages ranging from dataset collection to data preprocessing, feature selection, model design, and performance evaluation.

2.1. Problem Definition and setting Objectives

SDN is prone to significant hazard by (DDoS) attack due to the centralized control plane's susceptibility to overload. This study focuses on enhancing security in SDN by implementing a

hybrid model that can accurately and efficiently detect DDoS attacks, maintaining network performance and resilience**.**

This article presents important benefits in various fields. Especially in SDN environments, the hybrid method shows strong potential for practical applications while maintaining high accuracy in DDoS detection.

The paper introduces a hybrid DL model that effectively detects and decrease DDoS attempts in SDN environments. By combining RNN, DBN, and AFDL, the model can accurately quantify attacks. Leading to a 99.80% accuracy rate, this innovative approach enhances network security by providing a scalable and reliable solution.

2.2. Dataset Collection

The Canadian Institute for Cybersecurity's CICDDoS2019 dataset was studied in this research, which records a range of network traffic types, including both benign and DDoS attack situations, is used in the study. This dataset, which depicts actual traffic patterns and DDoS attack behaviors, serves as the primary source of information for training and testing the model. The dataset's comprehensiveness attributable to inclusion of a variety of traffic types such as TCP, UDP, and ICMP packets, made it well-suited for DL research, providing a comprehensive representation of real-world network situations. This study benefits from an extensive feature set by including the CICDDoS2019 dataset, which improves the analysis's robustness through increased variability and real-world application.

2.3. Data Preprocessing

Preparation of the data for model training, the undermentioned data preprocessing steps were applied:

- Handling Missing Data: The dataset did not contain any missing values, eliminating the need for imputation. This ensured consistency in the data without requiring additional processing steps.
- Categorical Feature Handling: Imputed with the most frequent category, which helps maintain data integrity without introducing bias.
- Standardization: Numerical features were scaled to a mean of 0 and a standard deviation of 1, ensuring optimal performance of deep learning models sensitive to feature scales.

2.4. Feature Selection

The Adaptive Feature Dimensionality Learning (AFDL) technique was applied to select the top 30 most relevant features from the initial set, reducing data dimensionality and focusing the model on essential feature as shown in the figure 1. The AFDL process ranked features based on statistical significance, enhancing the model's capacity to detect attack patterns effectively.

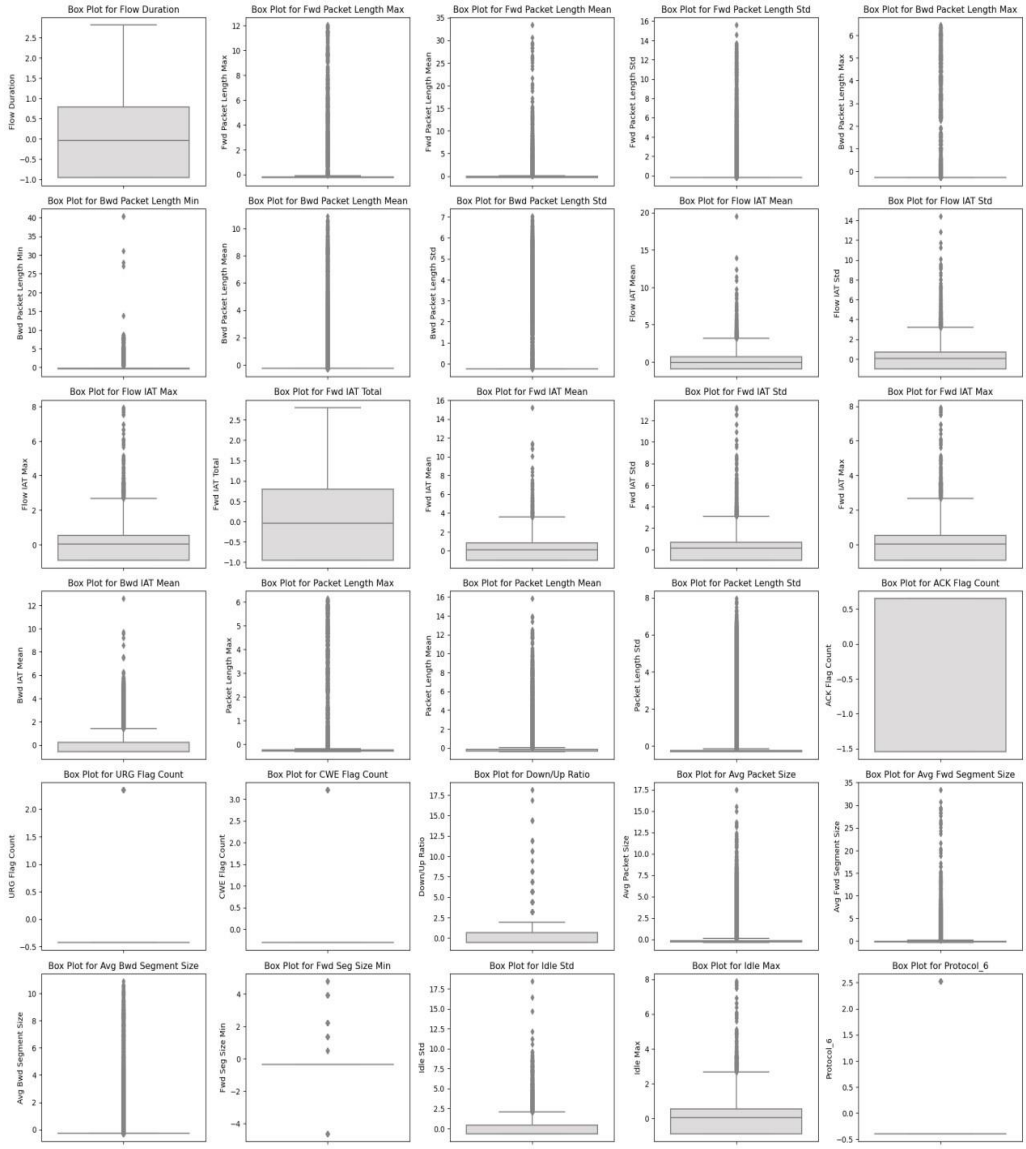

Figure 1: Feature selection using AFDL

2.5. Hybrid Model Design

The hybrid model as shown at Figure 2 combines three deep learning components to leverage both temporal and spatial data characteristics:

- **Recurrent Neural Network (RNN)**: RNNs are employed for analyzing sequential traffic data, capturing temporal dependencies that characterize DDoS attack behaviours.
- **Deep Belief Network (DBN)**: The DBN processes feature correlations by learning hierarchical data representations, capturing complex interactions between selected features.
- **Concatenation Layer**: Outputs from the RNN and DBN are merged to create a unified feature representation, combining both static and sequential data insights for enhanced classification accuracy.

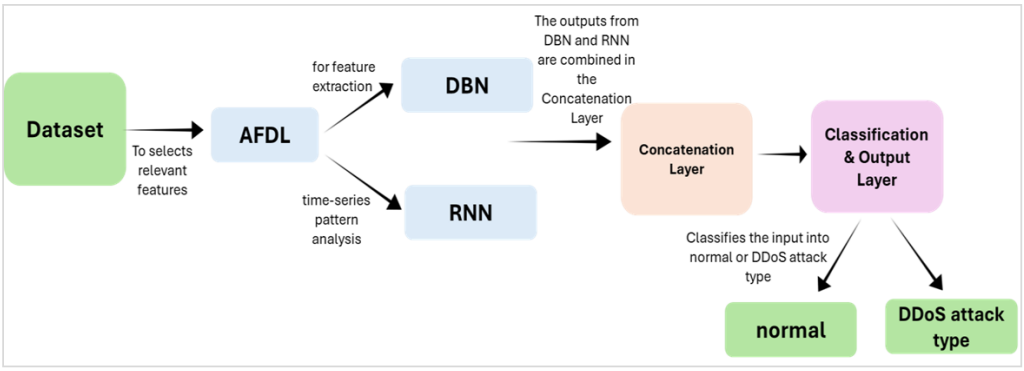

Figure 2: Proposed Architectural Model

2.6. Training and Testing

By using an 80-20 train-test split of the pre-processed dataset, the model was trained and verified. The model's performance was verified using unseen data to evaluate generalizability.

2.7. Performance Evaluation

The hybrid model's performance was evaluated using key metrics, including Precision, Recall, F1-Score, and Accuracy. These metrics provide a comprehensive assessment of the model's ability to classify DDoS attacks effectively within SDN environments. The results, as shown in Figure 3, demonstrate the hybrid model's exceptional performance:

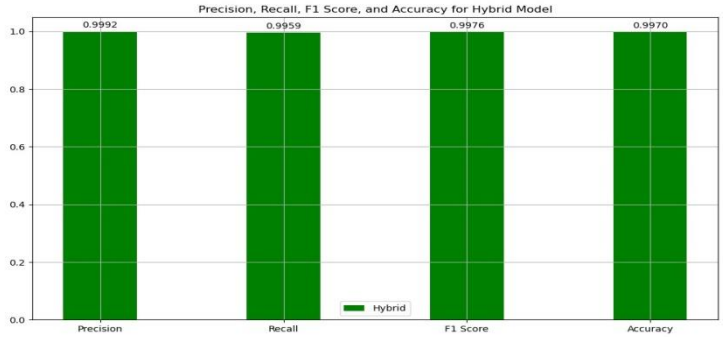

Figure 3: Performance Evaluation

These results as shown in the figure 3 indicate that the hybrid model excels in accurately detecting DDoS attacks with minimal classification errors. While the evaluation focuses on these core metrics, further studies may incorporate additional metrics such as response time and resource efficiency to assess the model's suitability for real-time applications.

3. RESULTS

This results section presents the performance analysis of the proposed hybrid model for detecting (DDoS) attacks in (SDN) setup scenarios. The model's evaluation performance was assessed using key metrics.

3.1. Confusion Matrix Analysis

The following **Figure 4** depicting confusion matric provides deep results into the classification presentation of the hybrid model. The matrix shows:

- True Positives (TP): 8607 DDoS attack cases were accurately classified as attacks.
- True Negatives (TN): 5426 normal traffic were accurately classified as non-attacks.
- False Positives (FP): Three instances of regular traffic were inaccurately categorized as attacks.
- False Negatives (FN): 29 DDoS attacks cases had been incorrectly identified as normal traffic.

These values highlight the model's quality to accurately classify both attacks and non-attack traffic, with minimal misclassification.

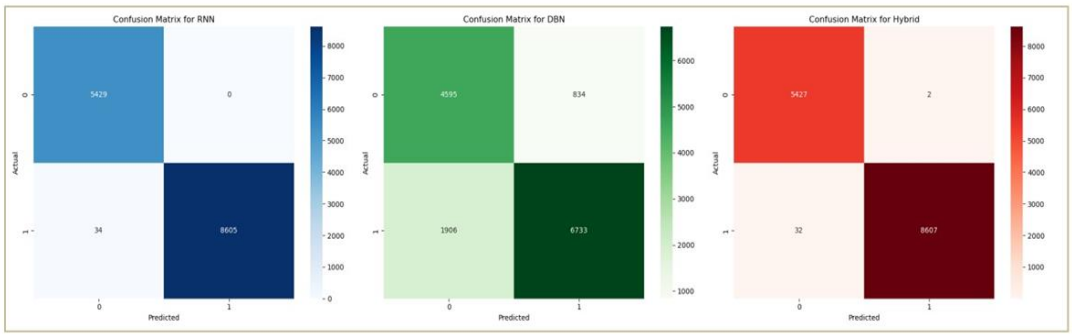

Figure 4: Confusion matrix of models

3.2. Performance Metrics

1. Accuracy:

$$\text{Accuracy} = TN+TP / TN+FP+TP+FN \approx 99.80\%$$

This high accuracy indicates that the model correctly classified a vast majority of instances.

2. Precision (for DDoS detection):

$$\text{Precision} = TP / TP+FP \approx 99.97\%$$

The precision score demonstrates the model's ability to prevent false positives, which is critical for minimizing unwanted alarms in real-world applications

3. Recall (for DDoS detection):

$$\text{Recall} = TP / TP+FN \approx 99.66\%$$

The high recall value indicates the model’s sensitivity, ensuring that most DDoS attacks are detected and minimizing the likelihood of missed attacks.

4. F1-Score:

F1 Score = 2×Precision×Recall / Precision+Recall
≈ 99.81%

The F1-score highlights the model's overall efficiency in DDoS detection by offering a balanced metric that takes into account both precision and recall.

3.3. Comparative Analysis

The hybrid model's metrics were compared against traditional detection methods, revealing superior performance across all evaluated metrics as shown in the Table 1. This improvement underscores the strength of the hybrid model approach architecture in accurately distinguishing DDoS traffic from normal network traffic in SDN environments.

Table 1: Performance metrics comparison for RNN, DBN and Hybrid models

Model	Accuracy	Precision	Recall	F1 Score
RNN	99.30%	99.31%	99.61%	99.46%
DBN	80.50%	88.98%	77.94%	83.09%
Hybrid	99.80%	99.97%	99.66%	99.81%

The following Figure 5 shows a comparison of the performance of the RNN, DBN, and hybrid models across important metrics. The results show that the hybrid model beats both solo models (RNN and DBN) across all evaluated metrics. This superior performance suggests that the hybrid model's architecture, which integrates RNN for temporal analysis and DBN for complex feature extraction, offers a more robust approach to DDoS detection. The combination of these components enables the hybrid model to better capture both temporal dependencies and intricate feature correlations, resulting in improved adaptability and accuracy for detecting various DDoS attack types.

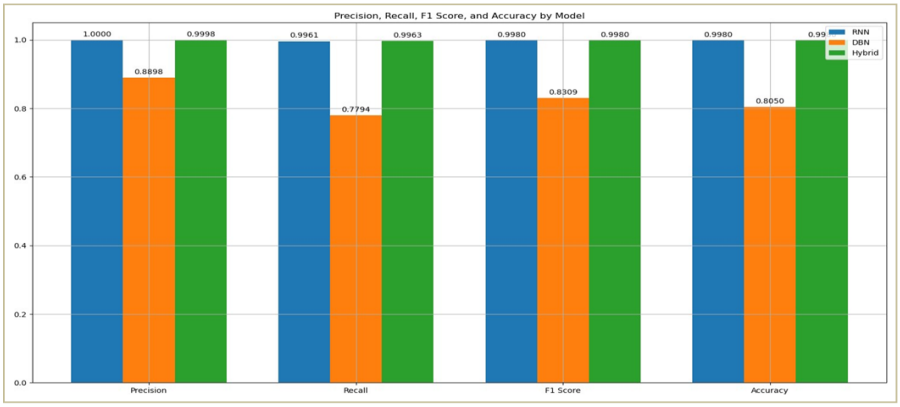

Figure 5: The results of our proposed hybrid method with the RNN and DBN method regarding the CICDDoS2019 dataset.

3.4. ROC Curve and AUC

The hybrid model, which combines (DBN) and (RNN), detects DDoS attacks with an impressive 99.80% high accuracy rate. The model's efficacy in identifying network traffic is assessed using

key performance indicators, such as a confusion matrix and ROC curve. This approach enhances predictive power by leveraging both temporal dependencies and feature correlations.

The model's (ROC) curve and (AUC) present its strong discriminative ability, with an AUC value close to 1.0 as shown at Figure 6, further validating the model's practical applicability in high-security environments.

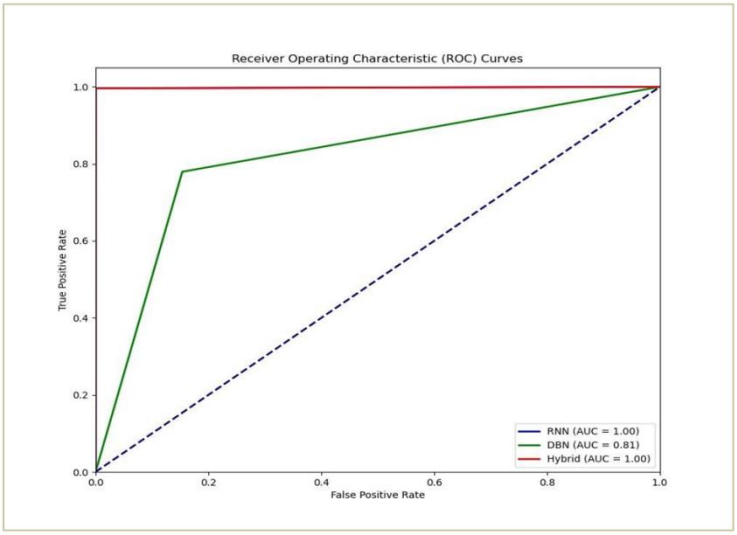

Figure 6: ROC curve related to CICDDoS2019 dataset

4. DISCUSSION

4.1. Interpretation of Findings

The hybrid DL model, which combines (RNN) and (DBN), achieves a high level of accuracy (99.80%) in detecting DDoS attacks on the CICDDoS2019 dataset. The RNN component effectively captures temporal dependencies in network traffic, revealing patterns common to DDoS attacks, whereas the DBN component extracts complicated, non-linear feature correlations. This integration improves the detection of different attack patterns, outperforming typical machine learning methods commonly employed in DDoS detection.

4.2. Comparison with Related Work

As shown in the Figure 5 above compares the hybrid model's performance against standalone RNN and DBN models across performance evaluation metrics approach consistently outperforms both standalone models, with particular improvements noted in recall and F1-score, indicating enhanced detection sensitivity and balanced classification performance. This improvement is related to the hybrid architecture's quality to leverage both temporal feature-based insights, providing an edge over simpler, singular models for DDoS detection within SDN environments.

4.3. Implications

The model's high precision and recall rates imply that it can minimize both false positives and negatives, crucial for reducing unnecessary alerts and missed detections in operational

networks. This characteristic makes the hybrid model particularly advantageous in SDN environments, where accurate detection is vital for protecting centralized control planes from DDoS attacks. The findings suggest that deploying this hybrid model can enhance network stability and security by offering precise, real-time attack detection capabilities

4.4. Limitations

While the findings are encouraging, the study's reliance on the CICDDoS2019 dataset limits its generalizability to different network conditions and novel attack types. Furthermore, the hybrid model's computational demands may complicate real-time application in resource-constrained contexts. Future adaptations of the model may consider optimization techniques to enhance performance under varied network and hardware conditions.

4.5. Future Work

should explore testing the model on additional datasets to ensure robustness across diverse SDN architectures and attack scenarios. Furthermore, developing effective mitigation strategies that can be deployed in conjunction with the detection model would improve the network's response capabilities to detected threats. Exploring lightweight, computationally efficient versions of the model can also address deployment challenges in environments with limited resources.

5. CONCLUSION

This work proposes a hybrid DL method for DDoS attack detection in SDN systems by combining the advantages of RNN and DBN. With a 99.80% detection accuracy on the CICDDoS2019 dataset, the model outperforms conventional models by capturing both complicated feature correlations and sequential dependencies.

The hybrid model's high detection accuracy and stability emphasize its potential for real-world applications in SDN security. While promising, further research is recommended to assess the model on a variety of datasets and network configurations to validate its generalizability and effectiveness in mitigating DDoS attacks across SDN networks. This study contributes significantly to the industry by presenting a good strategy for strengthening SDN security, paving the way for future improvements in network security and DDoS defensive systems.

REFERENCES

[1] C. Fan, N. M. Kaliyamurthy, S. Chen, H. Jiang, Y. Zhou, and C. Campbell, "Detection of DDoS Attacks in Software Defined Networking Using Entropy," *Applied Sciences (Switzerland)*, vol. 12, no. 1, Jan. 2022, doi: 10.3390/app12010370.

[2] K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges," Aug. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/jsan12040051.

[3] "DDoS_in_the_IoT_Mirai_and_Other_Botnets".

[4] Q. Tian and S. Miyata, "A DDoS Attack Detection Method Using Conditional Entropy Based on SDN Traffic," *Internet of Things*, vol. 4, no. 2, pp. 95–111, Jun. 2023, doi: 10.3390/iot4020006.

[5] G. Lalitha Devi and K. Vijay Kumar, "Time-Based Feature Analysis for DDoS Attack Detection and Classification," 2023.

[6] 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, Dec. 2023, doi: 10.3390/network3040024.

[7] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet: A Deep-Learning Model for Detecting Network Attacks," Jun. 2020, [Online]. Available: http://arxiv.org/abs/2006.13981

[8] D. Alghazzawi, O. Bamasaq, H. Ullah, and M. Z. Asghar, "Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection," *Applied Sciences (Switzerland)*, vol. 11, no. 24, Dec. 2021, doi: 10.3390/app112411634.

[9] O. Belarbi, A. Khan, P. Carnelli, and T. Spyridopoulos, "An Intrusion Detection System based on Deep Belief Networks," Jul. 2022, doi: 10.1007/978-3-031-17551-0_25.

[10] T. G. Gebremeskel, K. A. Gemeda, T. G. Krishna, and P. J. Ramulu, "DDoS Attack Detection and Classification Using Hybrid Model for Multicontroller SDN," *Wirel Commun Mob Comput*, vol. 2023, pp. 1–18, Jun. 2023, doi: 10.1155/2023/9965945.

[11] A. Mansoor, M. Anbar, A. A. Bahashwan, B. A. Alabsi, and S. D. A. Rihan, "Deep Learning-Based Approach for Detecting DDoS Attack on Software-Defined Networking Controller," *Systems*, vol. 11, no. 6, Jun. 2023, doi: 10.3390/systems11060296.

[12] 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*, vol. 225, Apr. 2023, doi: 10.1016/j.comnet.2023.109642.

[13] H. Elubeyd and D. Yiltas-Kaplan, "Hybrid Deep Learning Approach for Automatic DoS/DDoS Attacks Detection in Software-Defined Networks," *Applied Sciences (Switzerland)*, vol. 13, no. 6, Mar. 2023, doi: 10.3390/app13063828.

[14] I. Priyadarshini, P. Mohanty, A. Alkhayyat, R. Sharma, and S. Kumar, "SDN and application layer DDoS attacks detection in IoT devices by attention-based Bi-LSTMCNN," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 11, Nov. 2023, doi: 10.1002/ett.4758.

[15] U. B. Clinton, N. Hoque, and K. Robindro Singh, "Classification of DDoS attack traffic on SDN network environment using deep learning," *Cybersecurity*, vol. 7, no. 1, Dec. 2024, doi: 10.1186/s42400-024-00219-7.

[16] V. Hnamte and J. Hussain, "An EEcient DDoS Attack Detection Mechanism in SDN Environment An Efficient DDoS Attack Detection Mechanism in SDN Environment," *International Journal of Information Technology*, 2023, doi: 10.21203/rs.3.rs-2393388/v2.

[17] R. Kimanzi, P. Kimanga, D. Cherori, and P. K. Gikunda, "Deep Learning Algorithms Used in Intrusion Detection Systems -- A Review," Feb. 2024, [Online]. Available: http://arxiv.org/abs/2402.17020

[18] 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, Mar. 2024, doi: 10.1007/s13369-023-08075-2.

[19] K. Wang, Y. Fu, X. Duan, T. Liu, and J. Xu, "Abnormal traffic detection system in SDN based on deep learning hybrid models."

[20] K. Wang, Y. Fu, X. Duan, and T. Liu, "Detection and mitigation of DDoS attacks based on multi- dimensional characteristics in SDN," *Sci Rep*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024- 66907-z.

[21] H. Wang and Y. Li, "Overview of DDoS Attack Detection in Software-Defined Networks," *IEEE Access*, vol. 12, pp. 38351–38381, 2024, doi: 10.1109/ACCESS.2024.3375395.