Mathematical Modelling of Engineering Problems
Vol. 11, No. 2, February, 2024, pp. 493-499
Journal homepage: http://iieta.org/journals/mmep

Evaluating Machine Learning and Deep Learning Models for Enhanced DDoS Attack Detection

Mohand Adnan Owaid, Asmaa Salih Hammoodi*

Electrical Department, Engineering College, Tikrit University, Tikrit 34001, Iraq

Corresponding Author Email: asmaaphd11@gmail.com

https://doi.org/10.18280/mmep.110221

Received: 1 August 2023
Revised: 22 October 2023
Accepted: 1 November 2023
Available online: 27 February 2024

Keywords:
distributed denial of service, machine learning, deep learning, network traffic, support vector machine

ABSTRACT

In the realm of network security, distributed denial of service (DDoS) attacks pose a formidable threat, often resulting in operational disruptions and substantial financial losses. Traditional methods for DDoS detection struggle to adapt to the rapidly evolving attack methodologies, leading to compromised detection robustness and accuracy. The urgent need for more sophisticated detection mechanisms is evident. This investigation explores the effectiveness of advanced deep learning and ensemble machine learning models in identifying DDoS threats. A comprehensive approach is employed, leveraging a multitude of base classifiers to construct a robust and precise detection system. Integral to this study is the application of convolutional neural networks (CNNs), a deep learning variant, adept at discerning complex patterns and relationships within network traffic data. These models excel in autonomously extracting pertinent features, thereby enabling efficient detection of intricate DDoS attacks. A critical step in this methodology involves the collection of a comprehensive network traffic dataset, encompassing both normal and DDoS attack scenarios. This dataset undergoes a rigorous preprocessing and enhancement phase to ensure a balanced and representative training set. Subsequently, the augmented data is utilized to train the proposed models. The performance of these models is evaluated using a variety of metrics. Results from the experiments demonstrate that both machine learning and deep learning models significantly surpass existing techniques in DDoS detection. By amalgamating the strengths of various classifiers and neural networks, the method enhances detection precision and resistance to diverse attack variations. Comparative analyses reveal impressive performance metrics, with models such as CNN 1D and Alex Net achieving high levels of accuracy and precision. The outcomes of this study underscore the superiority of deep learning models in identifying both prevalent and novel DDoS attack patterns, thereby highlighting their potential in countering evolving cyber threats. The findings advocate for the enhanced precision and adaptability of the proposed approach in DDoS detection, marking a significant advancement in the field.

1. INTRODUCTION

DDoS attacks represent a critical threat to network security, impacting various global sectors and organizations. These attacks, characterized by their service disruption capabilities, result in substantial financial losses, reputational damage, and customer dissatisfaction. Conventional DDoS detection methodologies, predominantly based on rule-based strategies and signature matching, are increasingly inadequate in addressing the evolving tactics employed by sophisticated adversaries. This ineffectiveness underscores the pressing necessity for advanced detection mechanisms capable of reliably identifying and mitigating DDoS attacks [1]. Figure 1 is a schematic representation of a DDoS attack. In recent years, deep learning and ensemble machine learning models have emerged as promising solutions to enhance the robustness and accuracy of DDoS detection. Ensemble learning, which amalgamates multiple basic classifiers or neural networks, aims to construct a more robust and reliable detection system. This approach potentially improves performance by mitigating the limitations of individual models and harnessing the diversity of multiple models. Conversely, deep learning models, utilizing neural networks with multiple layers, are adept at autonomously recognizing and extracting complex patterns and features from data streams, thereby effectively identifying intricate DDoS attacks [2].

The present study is focused on assessing the efficacy of deep learning and ensemble machine learning models in detecting DDoS attacks. By leveraging the collective strengths of various models, the ensemble approach is posited to enhance detection accuracy and fortify resistance against diverse attack variations. Deep learning models, particularly proficient in discerning complex patterns in network traffic data, are expected to efficiently detect sophisticated DDoS attacks owing to their advanced feature extraction capabilities [3].

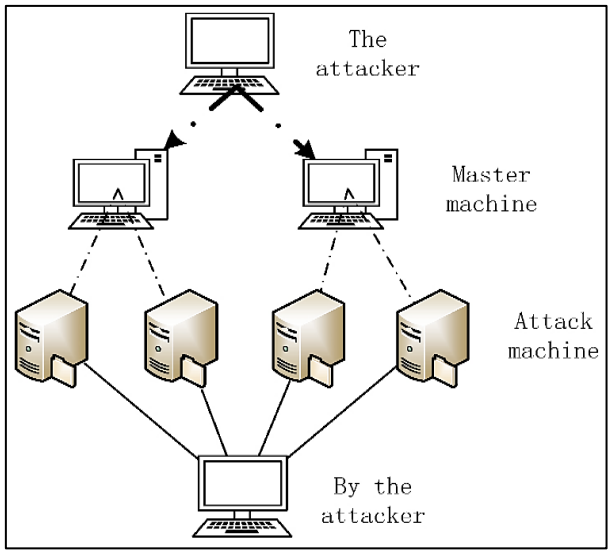

Figure 1. A schematic diagram of a DDoS attack

To achieve the research objectives, an extensive network traffic dataset, inclusive of standard and DDoS attack scenarios, is compiled. The dataset undergoes comprehensive preprocessing and enhancement to establish a balanced and representative training set. Subsequently, various ensemble models employing strategies such as bagging, boosting, and stacking are trained using the augmented dataset. Additionally, deep learning models, including CNNs, Recurrent Neural Networks (RNNs), and their variants, are deployed to identify complex correlations and patterns within network traffic data [4].

In evaluating the performance of both ensemble machine learning and deep learning models, metrics such as accuracy, precision, recall, and F1-score are employed. It has been observed that ensemble models exhibit superior performance over individual models, highlighting their effectiveness in enhancing the accuracy and resilience of DDoS detection. The deep learning models, through their adeptness at understanding complex patterns, have demonstrated high detection rates for both known and previously undetected types of DDoS attacks [5]. The primary objective of this research is to assess the efficacy of advanced machine learning techniques, specifically deep learning and ensemble machine learning models, in strengthening the accuracy and robustness of DDoS detection against dynamic and complex attack patterns. The findings of this study contribute significantly to the field of network security, advocating for the development of more sophisticated DDoS detection systems. This research underscores the potential of these models in advancing network security by enhancing the detection and mitigation of DDoS attacks.

The study underlines the role of ensemble machine learning and deep learning models in the realm of DDoS detection. By harnessing these models' enhanced accuracy, resilience, and automatic feature learning capabilities, a substantial stride forward is made in the field of network security. The insights gleaned from this research are instrumental in the development of advanced DDoS detection systems, thereby contributing to the fortification of network resilience and the effective mitigation of DDoS attacks. This advancement not only improves network security but also reduces the impact of such attacks, thereby benefiting various sectors reliant on network stability and security.

2. LITERATURE REVIEW

The study at hand notably advances the field of DDoS detection by building upon prior research. While previous studies have recognized the potential of deep learning and ensemble machine learning models in enhancing the accuracy and robustness of DDoS detection, this research marks a pioneering effort in integrating these two methodologies to formulate a comprehensive detection system. It addresses the limitations inherent in individual models by employing a synergistic approach, combining ensemble methods with deep learning techniques. This integration not only augments the detection capabilities but also introduces a more robust method for identifying DDoS attacks than relying solely on either approach. Moreover, this research extends beyond previous works by placing significant emphasis on feature engineering. Recognizing the importance of a representative and balanced training dataset, this study meticulously approaches data cleaning and enhancement. Prior research has acknowledged the necessity of a high-quality dataset for accurate DDoS detection; however, this study introduces a comprehensive methodology to ensure dataset quality, a critical factor for precise detection. By meticulously addressing the dataset's quality, this research provides a robust foundation for the proposed models, contributing a vital aspect to the domain of DDoS attack detection.

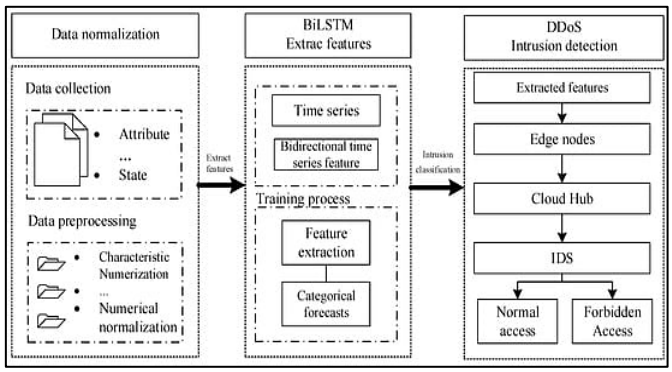

Figure 2. Schematic representation of the Bi-LSTM model for detecting DDoS [1]

DDoS attacks, known for causing service disruptions, financial losses, and reputational damage, pose a severe threat to network security. Traditional detection solutions, predominantly based on rule-based methodologies and signature matching, struggle to adapt to evolving attack tactics. To counter this challenge, the integration of ensemble machine learning and deep learning models has emerged as a promising solution, enhancing detection accuracy and robustness. Ensemble models, distinct from deep learning models, combine predictions from various base models, while deep learning models employ neural networks to autonomously recognize and extract complex patterns from network traffic data. Zhang et al. [1] proposed a bidirectional long short-term memory (BiLSTM)-based methodology for detecting DDoS attacks within edge computing environments. The BiLSTM model, proficient in capturing temporal relationships within data, is trained using network traffic information. This approach has demonstrated reliability in detecting DDoS attacks, a fact exemplified in Figure 2. Liu et al. [2] delved into the development of a DDoS detection method tailored for Software-Defined Networks (SDNs), employing machine

learning algorithms. This method effectively discerns DDoS attacks in SDN systems by extracting pertinent data from network traffic and deploying machine learning models to differentiate between legitimate and malicious traffic.

Varghese and Muniyal [3] introduced a comprehensive framework for an Intrusion Detection System (IDS) to identify DDoS attacks in SDN environments. This framework integrates traffic analysis, anomaly detection, and machine learning algorithms, thereby equipping it to recognize and mitigate DDoS attacks in SDN infrastructures. Mikhail et al. [4] suggested a machine learning-based technique for DDoS attack detection, which combines the random forest (RF) feature importance method with mutual information. This technique proficiently identifies DDoS attacks by analyzing patterns in network traffic data, assessing feature relevance through mutual information, and implementing a RF classifier.

Ali et al. [5] discussed the increased susceptibility of SDNs to DDoS attacks, attributed to their dynamic nature and centralized control. Traditional DDoS detection methods in SDNs are critiqued for their inadequacies, highlighting the imperative need for advanced machine learning techniques to augment detection accuracy and mitigate attack impacts. This detailed investigation evaluates various machine learning approaches for identifying DDoS attacks in SDN environments. The study categorizes these techniques into supervised and unsupervised learning models, examining their respective strengths and limitations within the context of SDN. The investigation encompasses a range of techniques, including support vector machine (SVM), RF, artificial neural networks (ANNs), and deep learning models such as CNNs and RNNs. Mansoor et al. [6] underscored the escalating threat of DDoS attacks on SDN controllers, noting their potential to compromise network security and disrupt operations. The limitations of conventional detection systems are highlighted, with the authors advocating for the adoption of deep learning approaches to refine the precision and efficacy of DDoS detection. Specifically, the utilization of CNNs is proposed for analyzing network traffic data to detect patterns indicative of DDoS attacks. The authors elaborate on the architecture and design of the CNN-based detection system, encompassing preprocessing stages, feature extraction, and model training. An empirical study is conducted using a publicly available DDoS dataset, with the findings compared against existing detection methodologies. Key performance metrics such as recall, accuracy, precision, and F1-score are employed to validate the effectiveness of the deep learning-based approach in accurately identifying DDoS attacks.

Yaser et al. [7] addressed the escalating threat of DDoS attacks and the urgent need for effective detection systems. An innovative architecture is proposed, combining feedforward and deep neural networks, and utilizing the autoencoder concept to enhance DDoS detection. This novel approach involves training feedforward and deep neural networks as autoencoders with benign network traffic data. These models are designed to discern underlying patterns and features by reconstructing the input data. During the detection phase, significant deviations between the reconstructed data and the original input signal the presence of DDoS attacks. Furthermore, the dynamic and programmable nature of SDNs renders them vulnerable to a spectrum of attacks. The authors discussed the challenges inherent in detecting DDoS attacks within SDN environments. A hybrid approach was suggested, amalgamating the benefits of autoencoders with one-class SVMs to detect DDoS attacks while minimizing false positives. The method involves training an autoencoder with standard network traffic data to learn patterns and features. The reconstruction error is then computed by rebuilding the input data using the autoencoder. A threshold based on the reconstruction error is established to distinguish between regular traffic and DDoS attacks [8]. The reconstructed data is further analyzed using a one-class SVM, trained on standard traffic data, to identify deviations from normal patterns. This combination of autoencoder and one-class SVM offers a robust and precise detection mechanism for DDoS attacks in SDN contexts.

Sumathi et al. [9] recognized the increasing threat of DDoS attacks and the necessity for efficient detection systems to safeguard network infrastructures. The potential of deep learning models and RNNs for detecting and mitigating DDoS attacks is explored. The study provides a comprehensive overview of DDoS attacks, delineating their characteristics and impact on network performance. It also critiques conventional detection methods and underscores the advantages of employing RNNs and deep learning models for DDoS attack detection. The research introduces long short-term memory (LSTM) and CNN models based on neural networks. The LSTM model is proficient in capturing temporal dependencies and sequential patterns in network traffic data, whereas the CNN model is focused on extracting spatial features from packet payloads.

Table 1. Comparison of several methodologies

Ref.	Publishing Year	Methodology	Result
[11]	2020	Deep CNN ensemble framework	Detecting DDoS attacks effectively in SDNs
[12]	2023	Optimisation-enabled deep learning-based DDoS attack detection	Detecting DDoS attacks in cloud computing
[13]	2022	Machine learning, mutual information RF feature importance method	Using RF to detect DDoS attacks
[14]	2021	Optimised extreme learning machine	DDoS attack detection in cloud computing
[15]	2022	Majority vote-based ensemble approach	Detecting DDoS Attacks in cloud computing
[16]	2020	Distributed deep learning system	Detecting web attacks on edge devices
[17]	2020	Fuzzy-Taylor-elephant herd optimization Inspired deep belief network	Deep Belief DDoS attack detection
[18]	2017	Machine learning techniques	Cloud computing DDoS attack detection
[19]	2022	Detection of DDoS attacks using IDS mechanism	A review
[20]	2021	Survey of authentication and privacy schemes	Automotive ad hoc networks
[21]	2022	Analysis of machine learning classifiers	Early detection of DDoS attacks on IoT devices

The study provides a comprehensive summary of various deep learning architectures employed in the detection of DDoS attacks. It encompasses an array of models including LSTM, Autoencoders, CNNs, RNNs, and generative adversarial

networks (GANs). Each methodology is described, with a focus on its specific advantages in identifying DDoS attacks. The report elucidates on the evaluation metrics used to assess the effectiveness of these deep learning models in DDoS detection. Common metrics such as accuracy, precision, recall, F1-score, and the area under the Receiver Operating Characteristic curve (AUC-ROC) are detailed. The literature review includes findings from various experimental studies that have applied deep learning techniques to detect DDoS attacks. It presents results from this body of research, outlining the efficacy of different deep learning models and offering a comparative analysis of their outcomes [10]. This comparison is instrumental in elucidating the relative strengths and weaknesses of each model in the context of DDoS attack detection (Table 1).

3. METHODOLOGY

The escalating prevalence of attacks targeting domain name system (DNS) security, particularly distributed reflective denial of service (DRDoS) attacks, has necessitated heightened attention in this domain. Unlike conventional DDoS attacks, DRDoS attacks exploit the DNS infrastructure, leveraging its vulnerabilities to amplify the impact of the assaults. Consequently, these attacks pose a distinct and significant threat to DNS security, necessitating specialized defense mechanisms and heightened vigilance for mitigation. This study concentrates on detecting DRDoS DNS attacks within substantial network traffic volumes. A key aspect of the methodology as shown in Figure 3 involves DNS-based DRDoS attack detection through the analysis of DNS traffic behavior. By monitoring and analyzing network data, the model aims to identify occurrences of DRDoS DNS attacks. It necessitates the examination of diverse packet traffic traversing the network, enabling the precise detection and response to these assaults, thereby bolstering the network infrastructure's security and resilience.

Integral to enhancing network security in detecting DNS-based DRDoS attacks is the strategic selection of machine learning and deep learning models. Models such as the stochastic gradient descent (SGD) classifier, SVM, RF, and deep learning architectures like CNNs and transfer learning utilizing AlexNet have been chosen for their distinctive attributes and capabilities. The SGD Classifier, known for its scalability and efficiency with large datasets, is apt for processing the extensive network traffic data required for DRDoS attack detection. SVM is deployed for its robustness in handling intricate data connections, effectively differentiating between legitimate and malicious network traffic. RF is selected for its proficiency in managing high-dimensional data and feature selection, crucial for accurate DRDoS detection. Deep learning models, including CNNs and AlexNet-based transfer learning, are employed owing to their ability to discern complex patterns in network traffic data, adept at identifying anomalies and differentiating between regular traffic and DDoS attacks.

The decision to utilize a diverse array of models allows for a comprehensive approach, enhancing the likelihood of successful DRDoS DNS attack detection. Each model contributes unique advantages to the detection process, ensuring a robust and comprehensive strategy to safeguard DNS systems against this specific and formidable threat. This study addresses a critical need in DNS security by maximizing the potential for accurate detection and thereby fortifying the security and stability of network infrastructures through the combined application of machine learning and deep learning models. The following delineates the utilization of machine learning and deep learning techniques for the analysis of the DRDoS DNS dataset, aimed at facilitating detection:

- Data preprocessing: Prior to analysis, the DRDoS DNS dataset undergoes a preprocessing phase, essential for extracting relevant information from the network traffic data. This stage involves tasks such as packet parsing, flow identification, and feature engineering, thereby rendering the traffic data suitable for application of machine learning or deep learning algorithms.
- Feature selection: Subsequent to preprocessing, the selection of a subset of features is imperative. These features must be indicative of anomalies and attacks within the dataset. The process incorporates a thorough analysis of the dataset and the application of domain expertise to identify features characterizing anomalous or malicious behavior.
- Model development: Various machine learning and deep learning methodologies are employed to develop detection models using the preprocessed data and selected features. Techniques such as the SGD classifier, SVM, RF, and deep learning architectures including CNNs and transfer learning with AlexNet are commonly utilized.
- Model evaluation: The efficacy and efficiency of the trained models in detecting abnormalities and attacks in the DRDoS DNS dataset are assessed using metrics like accuracy, precision, recall, and F1-score. This evaluation phase is crucial for determining the models' performance.
- Fine-tuning and optimization: The models undergo further optimization and fine-tuning. This involves adjustments of hyperparameters, exploration of various architectural configurations, and the application of methods such as cross-validation and ensemble learning. The goal of this iterative process is to enhance the models' generalization ability and detection accuracy.
- Detection and analysis: Upon completion of training and optimization, the models are applied to analyze real network traffic data. Capable of recognizing and categorizing suspicious or malicious activities, the models provide insights into potential security threats, facilitating prompt mitigation actions.

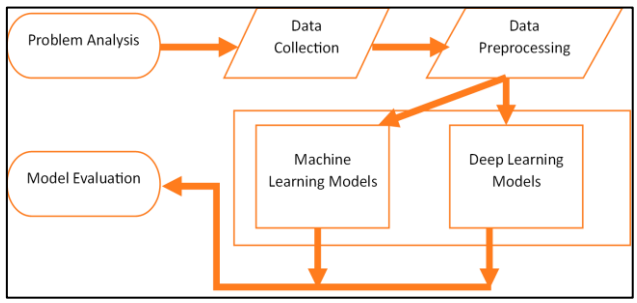

Figure 3. Process of the proposed methodology

4. RESULTS AND ANALYSIS

This section presents an exploration and development of a machine learning-based methodology for the detection of DRDoS within DNS environments, utilizing a meticulously curated dataset. The detection model, underpinning this research, underwent comprehensive training, testing, and

evaluation phases using this dataset. Despite the absence of explicit dataset details in the referenced link, the publication is presumed to delineate the dataset's characteristics and composition [22]. The dataset is characterized by the following attributes:

- Dataset characteristics and composition: The dataset is inferred to be composed of DNS logs and real-world network traffic data, sourced from diverse network configurations. This composition ensures diversity and enhances the generalizability of the model.
- Dataset specification: The study likely delineates the dataset's size, encompassing the number of samples (network traffic incidents) and features (attributes) per sample. The significance of a sizable dataset for effective training of machine learning models is acknowledged.
- Attributes: It is anticipated that the dataset comprises a multitude of attributes extracted from DNS logs and network traffic, encompassing various aspects of DNS packet behavior and communication patterns.
- Labeling: The dataset is expected to be categorized, with samples distinctly labeled as part of a DRDoS DNS attack or regular traffic. Such labeling is crucial for the application of supervised machine learning techniques in training the detection model.
- Data preprocessing: The preprocessing steps employed for refining, normalizing, and transforming the dataset into a format amenable to machine learning algorithms are likely detailed in the study.
- Data segmentation: A typical approach involves dividing the dataset into training, validation, and testing subsets. This division, adhering to a specific ratio, facilitates an unbiased evaluation of the model's performance.
- Evaluation metrics: The study is expected to elaborate on the evaluation metrics used, such as accuracy, precision, recall, F1-score, and AUC-ROC, to assess the efficacy of the detection model.

The study is expected to provide an exhaustive description of the dataset attributes, including diverse network traffic scenarios and types of DNS attacks, along with any data privacy concerns. Such detailed documentation is pivotal in fostering reproducibility and further research in network security and DRDoS DNS attack detection. Utilizing scikit-learn's train_test_split function, the dataset is bifurcated into training and testing sets. The target (label) is binary, classified as DrDoS_DNS=1 and BENIGN=0, with the test set constituting 20% of the total data. Repeatability is ensured through the use of a predetermined random seed (random_state). A range of models, including decision tree (DT), SVM, RF, CNN, and transfer learning with AlexNet, are applied in the proposed detection approach.

The RF classifier's predictions are quantified for accuracy, and this metric is stored in the variable RF_accuracy. Post the discovery of optimal hyperparameters, a new SGD classifier is trained, and its efficacy is evaluated using the test data, culminating in the determination of model accuracy with these hyperparameters. SVM models are subjected to testing with different kernels on a test dataset to ascertain their performance. The accuracy of each model is tracked, and the kernel yielding the highest accuracy is identified. The SVM model with this optimal kernel is then retrained using all training data, and its final accuracy is presented. A 1D CNN, tailored for the binary classification task, is deployed. It utilizes convolutional and pooling operations on input data of dimensions (15, 1), followed by fully connected layers for outcome prediction. The model is developed and trained employing suitable loss and optimization methods for the DRDoS detection task. A binary classification neural network, akin to AlexNet, is prepared using binary cross-entropy loss and the Adam optimizer. The model is trained on the training data and evaluated on various metrics, including accuracy, using the test data.

The performance of various models including CNN 1D, Alex Net, SGD, SVM, and logistic regression (LR) is quantified using standard metrics such as accuracy, precision, recall, and F1-score. These metrics are fundamental in evaluating the models' prediction capabilities:

- Accuracy is measured as the ratio of correctly predicted instances to the total number of instances, reflecting the overall effectiveness of the model's predictions.
- Precision indicates the proportion of correct positive predictions out of all positive predictions made by the model.
- Recall, also termed sensitivity, evaluates the fraction of correct positive predictions among instances of positive behavior.
- F1-score, the harmonic mean of precision and recall, provides a balanced comparison of these two metrics.

Table 2 succinctly encapsulates the performance of each model/method. For instance, CNN 1D manifests an F1-score of 1, with accuracy, precision, and recall each at 0.999. In a similar vein, the effectiveness of other models is appraised using these criteria. Results from other studies [23-25], are also included in the table, albeit without precise metric values. This inclusion is vital for a comprehensive comparison.

Table 2. Comparative analysis of proposed models

Method	Accuracy	Precision	Recall	F1-score
CNN 1D	0.999	0.999	0999	1
Alex Net	1	1	1	1
SGD	0.992	0.992	0.992	0.992
SVM	0.992	1	0.996	0.994
LR	0.999	0.996	0.989	0.992
GRU-RNN [23]	0.890	NA	NA	NA
CNN [24]	NA	0.9507	0.9483	0.9438
XGBoost [25]	0.983	NA	NA	NA

Table 2 serves as an efficient and clear summary of each proposed model's performance, providing a basis for an in-depth comparative analysis of the models in terms of accuracy, precision, recall, and F1-score.

Table 2's results offer a detailed evaluation of various deep learning and machine learning models applied in the detection of DRDoS DNS attacks. Key metrics such as precision, recall, accuracy, and F1-score provide insights into each model's performance. Notably, the CNN 1D and Alex Net models exhibited exceptional performance, achieving scores of 0.999 or 1 in all evaluated metrics. This suggests a near-perfect capability of these models in accurately predicting and identifying DDoS DNS attacks. The results underscore the enhanced effectiveness of machine learning and deep learning models in detecting DDoS DNS attacks compared to other approaches. The high F1-score and accuracy of these models demonstrate their proficiency in distinguishing between legitimate and malicious network traffic, underlining their

value in augmenting DNS security. The findings correspond with the study's goal of developing efficient detection techniques for DRDoS DNS attacks. Moreover, these results contribute to the existing body of research, showcasing the potential of deep learning and machine learning models in addressing the unique challenges posed by DDoS DNS attacks.

While the effectiveness of the models in identifying DRDoS DNS threats is established, the study's reliance on a specific dataset might raise questions about the generalizability of the findings to other datasets and network environments. Future research could explore the performance of these models across diverse datasets from different network settings to assess their robustness and applicability in real-world scenarios. The study focused on a particular set of evaluation metrics, namely accuracy, precision, recall, and F1-score. Future research endeavors could broaden the range of evaluation metrics, offering a more comprehensive assessment of model performance and capturing the nuances of DRDoS DNS attack detection more accurately. Such an expansion would deepen the understanding of the models' strengths and limitations, guiding their practical implementation in network security.

5. CONCLUSIONS

The study substantially contributes to the broader context of mitigating DRDoS attacks, specifically targeting DNS infrastructure. These attacks exploit vulnerabilities within the DNS framework, posing a distinct and critical threat to DNS security. By introducing a machine learning-based methodology, the research accentuates the importance of specialized defenses and heightened vigilance in safeguarding DNS systems against these dynamic threats. The application of this methodology to large-scale network traffic underlines its potential in efficiently detecting DRDoS DNS attacks. The effectiveness of deep learning and machine learning models, such as CNN 1D and Alex Net, equips network administrators and cybersecurity professionals with robust tools for the rapid detection and mitigation of DDoS DNS attacks. The research endorses a machine learning-based approach to counteract these threats effectively. The proposed model integrates several machine learning and deep learning techniques, including SGD, SVM, RF, CNNs, and transfer learning using AlexNet. These methods are applied to a dataset predominantly comprising DNS logs and real-world network traffic from various network configurations. The preprocessing and labeling of the dataset for supervised learning enable the models to distinguish between normal traffic and DRDoS DNS attacks accurately.

Notably, the CNN 1D and Alex Net models demonstrate exceptional performance, with perfect recall and F1-score, indicative of their efficiency in identifying DRDoS DNS attacks. This finding underscores the necessity of specialized defenses and increased vigilance to protect DNS systems from these evolving dangers. The study offers valuable insights into potential security vulnerabilities, facilitating prompt mitigation actions to safeguard network infrastructure. By leveraging machine learning techniques and conducting a thorough analysis of DNS traffic behavior, the research advances understanding in DNS security and DRDoS DNS attack detection. This work has significant implications for researchers, network administrators, and cybersecurity experts in enhancing the resilience of DNS systems against complex attacks.

REFERENCES

[1] Zhang, Y.Y., Liu, Y.Y., Guo, X.Y., Liu, Z., Zhang, X.K., Liang, K. (2022). A BiLSTM-Based DDoS attack detection method for edge computing. Energies, 15(21): 7882. https://doi.org/10.3390/en15217882

[2] Liu, Z.P., Wang, Y.H., Feng, F., Liu, Y.F., Li, Z.L., Shan Y.W. (2023). A DDoS detection method based on feature engineering and machine learning in software-defined networks. Sensors, 23(13): 6176. https://doi.org/10.3390/s23136176

[3] Varghese, J.E., Muniyal, B. (2021). An efficient IDS framework for DDoS attacks in SDN environment. IEEE Access, 9: 69680-69699. https://doi.org/10.1109/ACCESS.2021.3078065

[4] Mikhail, D.Y., Hawezi, R.S., Kareem, S.W. (2023). An ensemble transfer learning model for detecting Stego images. Applied Sciences, 13(12): 7021. https://doi.org/10.3390/app13127021

[5] Ali, T.E,. Chong, Y.W., Manickam, S. (2023). Machine learning techniques to detect a DDoS attack in SDN: A systematic review. Applied Sciences, 13(5): 3183. https://doi.org/10.3390/app13053183

[6] Mansoor, A., Anbar, M., Bahashwan, A.A., Alabsi, B.A., Rihan, S.D.A. (2023). Deep learning-based approach for detecting DDoS attack on software-defined networking controller. Systems, 11(6): 296. https://doi.org/10.3390/systems11060296

[7] Yaser, A.L., Mousa, H.M., Hussein, M. (2022). Improved DDoS detection utilising deep neural networks and feedforward neural networks as autoencoder. Future Internet, 14(8): 240. https://doi.org/10.3390/fi14080240

[8] Mhamdi, L., McLernon, D., El-Moussa, F., Zaidi, S.A.R., Ghogho, M., Tang, T. (2020). A deep learning approach combining autoencoder with one-class SVM for DDoS attack detection in SDNs. In Proceedings of the 2020 IEEE Eighth International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, pp. 1-6. https://doi.org/10.1109/ComNet47917.2020.9306073

[9] Sumathi, S., Rajesh, R., Lim, S. (2022). Recurrent and deep learning neural network models for DDoS attack detection. Journal of Sensors, 2022: 8530312. https://doi.org/10.1155/2022/8530312

[10] Mittal, M., Kumar, K., Behal, S. (2022). Deep learning approaches for detecting DDoS attacks: A systematic review. Soft Computing, 27: 13039-13075. https://doi.org/10.1007/s00500-021-06608-1

[11] Haider, S., Akhunzada, A., Mustafa, I., Patel, T.B., Fernandez, A., Choo, K.K.R., Iqbal, J. (2020). A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. IEEE Access, 8: 53972-53983. https://doi.org/10.1109/ACCESS.2020.2976908

[12] Balasubramaniam, S., Vijesh Joe, C., Sivakumar, T.A., Prasanth, A., Satheesh Kumar, K., Kavitha, V., Dhanaraj, R.K. (2023). Optimization enabled deep learning-based DDoS attack detection in cloud computing. International Journal of Intelligent Systems, 2023: 2039217. https://doi.org/10.1155/2023/2039217

[13] Mona, A., Waqas, K.Q., Muhammad, T., Muhammad, S., Mai, A., Fazila, M. Machine-learning-based DDoS attack detection using mutual information and RF feature

importance method. Symmetry, 14: 1095. https://doi.org/10.3390/sym14061095
[14] Kushwah, G.S., Ranga, V. (2021). Optimised extreme learning machine for detecting DDoS attacks in cloud computing. Computers and Security, 105: 102260. https://doi.org/10.1016/j.cose.2021.102260
[15] Alqarni, A.A. (2022). Majority vote-based ensemble approach for distributed denial of service attack detection in cloud computing. Journal of Cyber Security and Mobility, 11(2): 265-278. https://doi.org/10.13052/jcsm2245-1439.1126
[16] Tian, Z.H., Luo, C.C., Qiu, J., Du, X.J., Guizani, M. (2020). A distributed deep learning system for web attack detection on edge devices. IEEE Transactions on Industrial Informatics, 16(3): 1963-1971. https://doi.org/10.1109/TII.2019.2938778
[17] Velliangiri, S., Pandey, H.M. (2020). Fuzzy-Taylor-elephant herd optimisation inspired deep belief network for DDoS attack detection and comparison with state-of-the-arts algorithms. Future Generation Computer Systems, 110: 80-90. https://doi.org/10.1016/j.future.2020.03.049
[18] Zekri, M., El Kafhali, S., Aboutabit, N., Saadi, Y. (2017). DDoS attack detection using machine learning techniques in cloud computing environments. In 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), pp. 1-7. https://doi.org/10.1109/CloudTech.2017.8284731
[19] Agarwal, A., Singh, R., Khari, M. (2022). Detection of DDoS attack using IDS mechanism: A review. In 2022 1st International Conference on Informatics (ICI), Noida, India, pp. 36-46. https://doi.org/10.1109/ICI53355.2022.9786899
[20] Al-Shareeda, M.A., Anbar, M., Hasbullah, I.H., Manickam, S. (2021). Survey of authentication and privacy schemes in vehicular ad hoc networks. IEEE Sensors Journal, 21(2): 2422-2433. https://doi.org/10.1109/JSEN.2020.3021731
[21] Gaur, V., Kumar, R. (2022). Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices. Arabian Journal for Science and Engineering, 47(2): 1353-1374. https://doi.org/10.1007/s13369-021-05947-3
[22] Nuiaa, R.R., Manickam, S., Alsaeedi, A.H. (2021). Distributed reflection denial of service attack: A critical review. International Journal of Electrical and Computer Engineering, 11(6): 5327-5341. http://doi.org/10.11591/ijece.v11i6.pp5327-5341
[23] Tang, T.A., Mhamdi, L., McLernon, D., Zaidi, S.A.R., Ghogho, M. (2018). Deep recurrent neural network for intrusion detection in SDN-based networks. In 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), Montreal, QC, Canada, pp. 202-206. https://doi.org/10.1109/NETSOFT.2018.8460090
[24] Zheng, W.F. (2020). Intrusion detection based on convolutional neural network. In 2020 International Conference on Computer Engineering and Application (ICCEA), Guangzhou, China, pp. 273-277, https://doi.org/10.1109/ICCEA50009.2020.00066
[25] Gaur, V., Kumar, R. (2022). Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices. Arabian Journal for Science and Engineering, 47: 1353-1374. https://doi.org/10.1007/s13369-021-05947-3