Journal of Innovations in Computer Science and Engineering
Shahid Beheshti Unversity

January 2025, Special Issue on AI 4 All- 2

LDA-ML: A Hybrid DDoS Detection Attacks in SDN Environment using Machine Learning

Alireza Rezaei✉, Code ORCID: 0009-0002-9916-3100
Department of Computer Engineering, Karaj Branch, Islamic Azad University, Karaj, Iran, alirezarezaie962@gmail.com
Amineh Amini, Code ORCID: 0000-0001-8427-5455
Department of Computer Engineering, Karaj Branch, Islamic Azad University, Karaj, Iran, aamini@kiau.ac.ir

Abstract—In today's world, DDoS attacks are becoming more common and complex; thus, they constitute a great challenge for network security under the auspices of SDN. The research effort described here proposes an integrated hybrid model called "LDA-ML," which leverages some state-of-the-art machine learning methods: LDA, naive bayes, random forest, and logistic regression. We optimize the data analysis process by leveraging LDA for feature selection and dimensionality reduction, followed by a sequential application of the classifiers to exploit their strengths. Evaluated on the CICDDoS-2019 dataset, the proposed model has achieved an outstanding accuracy of 98.98%, indicating the efficacy of the model in correctly classifying benign versus attack traffic. All of the above underlines the robustness of the proposed LDA-ML model, pointing to great potential for its application to continuously improve cybersecurity strategies against DDoS threats in SDN architectures. This holistic approach offers improvements in detection, while it also enriches diagnostic insights-an important contribution to finding effective security solutions in increasingly dynamic network environments.

Keywords— DDoS attack, SDN, Cybersecurity, Machine learning

I. Introduction

In the digital era, the security of online systems is paramount, with distributed denial of service (DDoS) attacks emerging as a formidable threat to internet stability and security. These attacks, designed to overwhelm a network or system to the point of inoperability, have evolved in complexity and scale, posing a continuous challenge to organizations worldwide [1].
In a DDoS attack, the intruder finds vulnerabilities in the network and injects a malicious program, known as Trojan Horse, in the computer systems without the awareness of users. By replicating this malicious program in the multiple devices connected to the network, intruder create an army of compromised computer systems which they control to initiate DDoS attacks. These compromised machines are often known as bots, and the group of these bots is called a botnet [2]. The advent of software defined networking (SDN), which enables a centralized controller to oversee and configure the entire network, has made SDN a prime target for DDoS attacks [3]. Defending against DoS and DDoS attacks is more challenging in SDN than in traditional networks. These types of attacks have become significant threats to computer networks, causing a decline in network performance by consuming available resources and disabling services [4]. However, because of the centralized management of SDN architecture, it is very easy to cause a single point of failure, resulting in the collapse of the entire network. The most common network threat is DDoS attack. Although the development of SDN has just started, in the future, SDN will be the mainstream network architecture. Based on this, the network security problems faced by SDN applications urgently need to be solved [5]
Machine learning (ML) and deep learning (DL) techniques have also been proposed as potential solutions to classify such attacks. Those techniques are employed to analyze the network traffic-flow patterns and detect abnormal traffic behaviors indicating DDoS attacks. However, there is a lack of consensus on the most effective ML, DL, and hybrid approaches to detecting DDoS attacks [6].
The "LDA-ML" hybrid model introduces a new methodology for DDoS detection in SDN. This will combine LDA with machine learning algorithms like naive bayes (NB), random forest (RF), and logistic regression (LR). It advances their detection by the sequential use of algorithms based on the strengths of each classifier. The salient innovations of the model involve the use of LDA for feature selection and dimensionality reduction, a tiered training strategy to enhance accuracy, and a comprehensive evaluation framework using a variety of performance metrics to assess effectiveness.
The rest of this paper is organized as follows: Section II reviews the basics of machine learning. Section III surveys the related literature concerning DDoS attack detection. Section IV elaborates on the proposed "LDA-ML" hybrid model. Section V presents some experimental results. Finally, Section VI summarizes the results of this research and underlines the contribution of the model to improving DDoS attack detection strategies.

Submit Date: 2024-12-07
Accept Date: 2025-05-18
✉ Corresponding author

II. Background

III. Machine Learning

Machine learning is a technique used to give computers the ability to automatically learn from previous data and make decisions like humans. ML involves training a model on training data and processing additional data to make a classification, detection, or prediction. there are two types of ML, supervised learning and unsupervised learning [7]. Supervised learning is a learning approach which is used to first train the model base upon labeled training data, and then to classify new test data that will belong to the any one of the class. Supervised learning is a two-step process. In the first step that is training step, it involves learning a classifier based upon the labeled data and second step is validation and verification or testing where a newly input data is tested against the trained model [8]. ML techniques are increasingly being applied in SDN to optimize various aspects of network management. The centralized architecture of SDN enables the collection of extensive network data, facilitating ML applications for tasks such as traffic classification, routing optimization, quality of service (QoS) and quality of experience (QoE) prediction, resource management, and security. By leveraging ML algorithms, SDN can improve efficiency, enhance security measures, and provide smarter, more adaptive networking solutions [9].

IV. Normalization and Standardization

Normalization and standardization are two important methods used in data preprocessing. Normalization rescales the data between 0 and 1, while Standardization is rescaling the data so that it has the same mean and the same standard deviation [10]. In this paper, the Min-Max method which is one of the most popular methods for normalization, was used. rescaling is the simplest method and consists in rescaling the range of features to scale the range in (0, 1) or (−1, 1) [11].

V. Normalization and Standardization

Feature selection, a crucial element of machine learning, entails strategically choosing a subset of relevant features from the original set. This process aims to enhance model performance, reduce computational complexity, and improve interpretability. Three main types of feature selection methods exist: filter methods, wrapper methods, and embedded methods [12].

VI. Dimension reduction

Dimensionality reduction, or dimension reduction, is the transformation of data from a high-dimensional space into a low-dimensional space so that the low dimensional representation retains some meaningful properties of the original data, ideally close to its intrinsic dimension. Working in high dimensional spaces can be undesirable for many reasons [13].

VII. Related Works

This section discusses the recent trend in detecting DDoS attacks using ML techniques. A review of recent related works on enhancing DDoS attack detection based on ML methods is summarized in Table 1. The authors in [14] applied machine learning classification algorithms such as RF, SVM, MLP, and KNN to detect and classify DDoS attacks in cloud computing, further strengthening the different security measures to safeguard data. They built classifier models and improved information within the dataset to attain high accuracy. In [15], an unsupervised IDS was developed for detecting zero-day DDoS attacks in IoT networks, using random projection for feature selection and an ensemble model of K-means, GMM, and one-class SVM, recording high accuracy on the CICDDoS2019 dataset. The authors in [16] trained Stochastic Gradient Boosting, decision tree (DT), KNN, NB, SVM, and LR on the CICDDoS-2019 dataset for proactive DDoS defense. In [17], data preprocessing, SMOTE, along with LR, DT, and RF algorithms, underlined that RF yields the highest predictive accuracy among others, considering the ensemble techniques and balancing.

TABLE I. REVIEW OF RELATED WORKS

S.No	*Reference*	*Year*	*Method*	*Dataset*	*Accuracy*
1	[14]	2024	RF, SVM, MLP, KNN	From Kaggle	99.80%
2	[15]	2024	GRP, K-means, SGD, SVM,GMM	CICDDoS-2019	94.50%
3	[16]	2024	DT, KNN, NB, SVM, LR	CICDDoS-2019	99.00%
4	[17]	2024	LR, DT, RF	From Kaggle	96.00%
5	[18]	2024	LSTM	InSDN Dataset	99.83%
6	[3]	2023	MLP-CNN	CICDDoS-2019	99.95%
7	[19]	2023	Swarm Optimized RF	CICDoS-2017	99.50%
8	[20]	2023	XGboost, LGBM, CatBoost, RF, DT	CICDoS-2017	99.77%
9	[21]	2023	RF, XGBoost, Ada Boost,LGBM	CICDDoS-2019	99.80%
10	[22]	2023	SVM, KNN	CICDoS-2017	99.00%

Authors of [18], proposes a new solution for DDoS attack detection SDN by using entropy-based anomaly detection with deep learning approaches. It attained a remarkable accuracy of utilizing an LSTM model. In [3], a model coupled with MP and CNN was presented that would improve DDoS detection in SDN by the selection of features using SHAP and hyperparameter tuning using Bayes optimization to obtain high accuracy over two datasets. Authors in [19], a DDoS detection model utilized swarm optimization-based feature selection with a Random Forest classifier, achieving high accuracy with 40 out of 75 features.
In [20], the authors performed a hierarchical ML-based hyperparameter optimization approach for DDoS detection in financial

networks using CICIDS 2017 and LASSO feature selection. In [21], the authors emulated Slowloris attacks in D2D communication to develop a dataset and trained different ML algorithms, such as RF and XGBoost for the detection of DDoS and DoS attacks. Authors of [22] proposed a two phase authentication system using packet filtration and ML algorithms such as SVM and KNN to mitigate DoS attacks in SDN environments.

VIII. Proposed Model

The proposed "LDA-ML" is a hybrid and sequential model, which is developed to enhance the detection of DDoS attacks in SDN environments.
In the model, several supervised ML methods such as NB, RF, and LR algorithms, together with the LDA dimension reduction method are used.

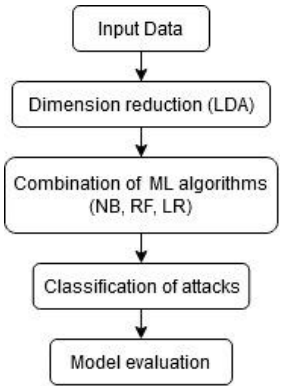

Fig. 1. Proposed Attack Classification Model

IX. Linear Discriminant Analysis

Linear Discriminant Analysis (LDA) is a statistical approach in classifying objects (people, things, events, etc.) based on their set of features that can be placed in two or more characteristic groups. A feature must be defined as an observation, property, attribute, variable or measurement of an object [23].

X. Naïve Bayes

The Bayes' Theorem is used to generate naive Bayes classifiers, which are a group of classification methods. It consists of a number of algorithms which all work on the same principle: each pair of features to be categorized is independent [24].

XI. Random Forest

The random forest classifier consists of a combination of tree classifiers that each tree classifier generates using a random vector sampled individually from the input vector, which in combination would make up the random forest classifier. Each tree calculates a unit vote for the most popular class to classify an input vector [25].

XII. Logistic regression

Regression is a popular supervised learning method. In this case, the dependent variable is categorical. Statistics forecasts the outcomes of dependent variables. As a result, the product must be definite. Yes, or No, 0 or 1, true or false, but always between 0 and 1. Logistic Regression is used in the same way that linear regression is [26].

XIII. LDA-ML Model

The proposed hybrid model presents an efficient methodology in DDoS attack detection based on the combined analysis by means of machine learning techniques, including LDA, Naive Bayes, Random Forest, and Logistic Regression. The model aims to enhance the quality of data, enhance detectability, and give a full diagnosis for the kind of possible attack. The process begins with the pre-processing of data; hence, irrelevant and redundant features are removed, and the dataset is normalized using the Min-Max-Scaler method.
After the preprocessing steps, the data is then divided into training and testing sets to prepare for modeling. Subsequently, LDA will be done for dimensionality reduction, hence optimizing the data for further analysis. We reduce the dimensionality of the data through LDA, which will have a better effect on other analysis methods such as classification, clustering, or regression. Therefore, reducing the dimensions decreases noise and irrelevant features, increasing the accuracy and speed of the analysis. During this model training phase, training of a Naive Bayes classifier using chosen features takes place to detect potential DDoS attacks. We perform an initial attack detection using an NB model, which is used as a base state of target detection. If the NB detects an attack, the system classifies it as such. Those data samples that could not be classified as attacks by the Naive Bayes classifier utilize the Random Forest algorithm for further analysis to find patterns that the NB classifier might have missed. (As shown in Figure 2).

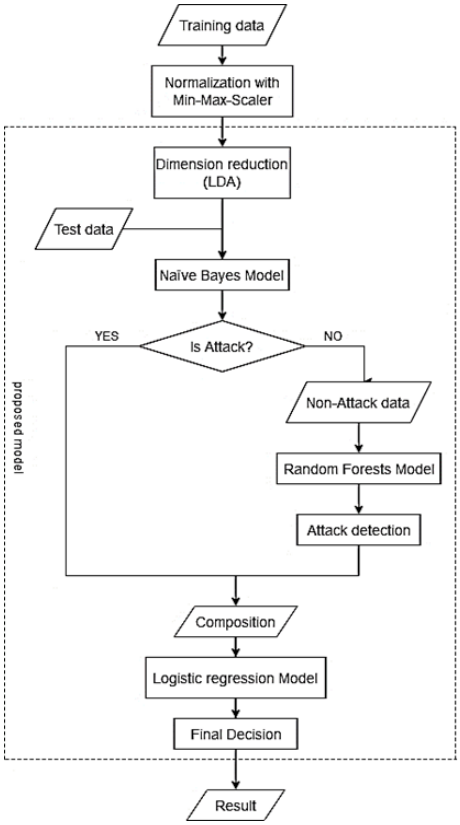

Fig. 2. Summary of the LDA-ML flowchart

Then, the output of both RF and NB models is combined for an overall diagnosis. Combining the outputs of NB and RF algorithms using a simple logic like logistic regression would improve the overall accuracy of the model. This is because different algorithms have different strengths and weaknesses; combining them may allow their limitations to be overcome. In this way, the process of detection becomes more accurate and reliable in a sequential manner, by capitalizing on the strengths of each algorithm for an overall better performance. Figure 2 displays a flowchart mapping out the workflow of the LDA-ML model, providing a step-by-step and structured roadmap from data preprocessing and dimensionality reduction right through to model training.

This LDA-ML architecture algorithm is implemented in two phases. The first phase of the algorithm, as depicted in Algorithm 1, composes the data normalization process with the MinMaxScaler method.

	Algorithm 1: Data normalization
	Require: *Dataset*
1	Convert the 'Class' column to binary values (1 for 'Attack', 0 for 'Normal') Filter out numeric data from the dataset
2	Convert integer data to float type for normalization
3	Use MinMaxScaler to normalize the numeric and integer data separately
4	Concatenate the normalized numeric and integer data into a single dataframe
5	Display the shape of the normalized dataframe to check for consistency

	Algorithm 2: LDA-ML
	Require: *Dataset with features and target label*
1	Load the dataset
2	Split the dataset into training and testing sets
3	Perform dimensionality reduction and feature selection using LDA
4	Train the Naive Bayes model on the training set
5	If (Naive_Bayes_Model.predict(test_set) == "not_attack"): Random_Forest_Model.predict(test_set)
6	Train the Random Forest model on the training set
7	Combine the outputs of both models using Logistic Regression
8	Evaluate the model performance using various metrics on the testing set
9	Display the confusion matrix, accuracy score, precision score, recall score, F1 score, and ROC AUC score

Implementation of the proposed model using Python programming language is performed within an Intel Core i5-480M processor, with 4GB of RAM and a Windows operating system. The comparison of results is performed with the most recent advanced methods to validate the effectiveness of the proposed model. These tests have been done in VS-Code notebook, written in Python, and using libraries such as scikit-learn, and Pandas. The obtained results confirm the ability and effectiveness of the proposed model.

XIV. Dataset

This article uses a real-world dataset, These datasets are collected from actual SDN networks and contain real traffic patterns and attack behaviors. The dataset used in this article is the CIC-DDoS2019 dataset, which was collected from a large enterprise network and includes benign and DDoS attack traffic. This dataset has been widely used in research on DDoS attack detection and prevention in SDN networks [27].

This dataset, comprises the most recent and popular DDoS attacks, which are based on real-world information. Data from CICFlowMeter-V3 network traffic analysis, including flow labels based on timestamps and the source and destination IP addresses and ports, protocols, and attack types are also included [28]. This dataset included 79 features and a total of 431371 data.

XV. Data Split

The total number of data points in the dataset was 431,371; 80%, that is, 345,096 data points, were used as the training set, while the remaining 20%, amounting to 86,275 data points, were reserved for testing the model. This dataset contained a total of 333,540 instances of attacks and 97,831 benign ones. Such a distribution of data allowed for an extensive analysis and performance evaluation of the model in distinguishing between attacks and benign activities. The use of such a huge and varied dataset allowed for a strong training process and comprehensive testing in terms of the model's precision and effectiveness.

XVI. Feature Scaling and reduction

Feature scaling is a very important step in the performance optimization of machine learning algorithms. Normalization of data at the input training stage helps prevent overfitting and reduces training time. Further, after the division of a dataset into a training set and a test set, the application of data normalization techniques should be considered to standardize feature values.

In this paper, the scaling of every feature in the range of 0 to 1 was made using the MinMaxScaler transformation. Then, LDA was applied to reduce the dimensionality such that the input data model could be reduced to one dimension only. This not only makes the data easy to visualize in a low-dimension space but also prepares the data for other machine learning algorithms.

XVII. Performance Metrics

Evaluating the effectiveness and accuracy of the DDoS detection model is paramount. The literature consistently employs a set of well-established evaluation metrics based on four fundamental elements: true positive (TP), false positive (FP), true negative (TN), and false negative (FN) [3]. The Confusion Matrix takes the classification results and groups them into four categories:

- True Positive (TP): when both the actual and predicted values are 1.
- True Negative (TN): when both the actual and predicted values are 0.
- False Positive (FP): when the actual value is 0 but the predicted value is 1.
- False Negative (FN): when the actual value is 1 but the predicted value is 0 [29].

Accuracy is the most straightforward metric. Precision focuses on the fraction of relevant instances among the retrieved instances. Recall measures the ability of the classifier to find all the relevant cases within a data set. F1-score is the harmonic mean of precision and recall, providing a balanced measure that considers both false positives and false negatives. The receiver operating characteristic (ROC) curve plots the true positive rate (recall) against the false positive rate for different thresholds. The area under the ROC curve (AUC) provides an aggregate measure of performance across all thresholds. ROC curves and AUC are particularly useful in binary classification tasks to understand the trade-offs between true positives and false positives at different decision thresholds [29], [3]. Leveraging a variety of performance evaluation metrics, including accuracy, precision, recall, F1-score, and AUC-ROC, enables a comprehensive assessment of a model's effectiveness.

XVIII. results

The metrics for the LDA-ML Model, as shown in Figure 3, give a broad overview of the performance of the model in categorizing text data. The metrics provide insight into the model's precision, recall, accuracy, ROC-AUC, and F1-score, all crucial when evaluating the effectiveness of the model in the proper classification of text data into predefined categories.

TABLE II. RESULTS OF EVALUATION CRITERIA

Dataset	***Accuracy***	***Precision***	***Recall***	***F1***	***ROC***
CICDDoS-2019	0.9898	0.9907	0.9961	0.9934	0.9823

The evaluation metrics for the CICDDoS-2019 dataset are shown in Table IV. The approximate accuracy of our model on this dataset is 98.99%, meaning it generally gives very correct predictions. Precision stands at 99.07%, which out of all the actual positives predicted, few were false positives. On the other hand, the Recall is 99.62%, indicating that most of the true positives were captured by the model. In addition, the F1 score is 99.35%, which is a good balance between precision and recall. The high

ROC score of 98.23% also indicates the efficiency of the model for separation in a class. Overall, these results suggest that our model is effective for the CICDDoS-2019 dataset.

The evaluation metrics for the CICDDoS-2019 dataset are shown in Table II.

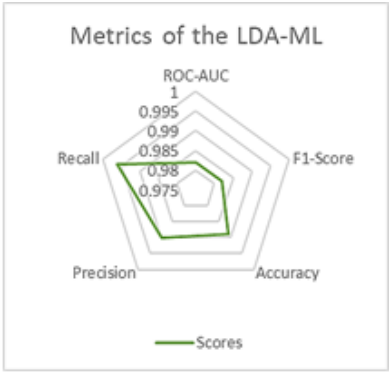

Fig. 3. Metrics of the LDA-ML Model

The approximate accuracy of our model on this dataset is 98.99%, meaning it generally gives very correct predictions. Precision stands at 99.07%, which out of all the actual positives predicted, few were false positives. On the other hand, the Recall is 99.62%, indicating that most of the true positives were captured by the model. In addition, the F1 score is 99.35%, which is a good balance between precision and recall. The high ROC score of 98.23% also indicates the efficiency of the model for separation in a class. Overall, these results suggest that our model is effective for the CICDDoS-2019 dataset.

Training Set			
TARGET / OUTPUT	Bengin	Attack	SUM
Bengin	19000 22.02%	619 0.72%	19619 96.84% 3.16%
Attack	255 0.30%	66401 76.96%	66656 99.62% 0.38%
SUM	19255 98.68% 1.32%	67020 99.08% 0.92%	85401 / 86275 98.99% 1.01%

Fig. 4. Confusion matrix of the LDA-ML Model

Compared to contemporary works, the hybrid model seems to show promising results. From these excellent accuracies, precision recalls, and F1-scores on various datasets, it is clear that the model performs impressively and can promote further research in the detection of DDoS attacks. Employing a combination of machine learning models in terms of feature selection, and optimized hyperparameters, the proposed model can boast its robustness and efficiency against emerging threats.

TABLE III. COMPARISON WITH RECENT LITERATURE

Reference	***Method***	***Dataset***	***Accuracy***
[15]	GRP, K-means, SGD, SVM,GMM	CICDDoS-2019	94.50%
[16]	DT, KNN, NB, SVM, LR	CICDDoS-2019	99.00%
[3]	MLP-CNN	CICDDoS-2019	99.95%
[21]	RF, XGBoost, Ada Boost,LGBM	CICDDoS-2019	99.80%
LDA-ML Model	LDA, NB, RF, LR	CICDDoS-2019	98.98%

XIX. Conclusions

In summary, the proposed hybrid model "LDA-ML" offers a very strong enticing advantage toward DDoS attack detection in SDN environments. The proposed model combines several ML techniques, such as LDA, NB, RF, and LR, which allows it to reap the advantages of each of these different algorithms and presents the most robust and efficient methods to meet all such challenges posed by DDoS. The adaptiveness of the model is particularly suited for the SDN environment where centralized control requires the immediate identification and mitigation of DDoS attacks. SDN infrastructures are highly dynamic, and the ability of the LDA-ML model to effectively preprocess data, reduce dimensionality, and enhance feature selection ensures that it can handle the sophisticated and varied patterns in data which are many times associated with cyber threats. Its high accuracy value of 98.98% is indicative that the model not only identifies attacks but also minimizes false alarms, a dire prerequisite to maintain integrity in network operations. Being trained on real data from the CICDDoS-2019 dataset, the model, upon demonstrating efficiency in practical scenarios, has provided further proof of its applicability in real-time detection mechanisms within SDN.

The hybrid approach provides greater flexibility to the operators, who can answer more effectively to the new emerging threats by implementing richer diagnostic capabilities. The sequential model leverages at first the predictions obtained from the NB classifier, which are subsequently refined by the RF algorithm. The layered defense model is quite in line with the architecture of SDN.

This approach allows for fast analysis and neutralization of multiple attack vectors. Besides this, unlike deep learning methods that require enormous computational resources and large labeled datasets, the LDA-ML model gives real-time responses with a smaller number of training samples, making it particularly well-suited for implementation in resource-constrained SDN environments. Further research and practical applications of this methodology might lead to greatly improved cybersecurity postures within SDN frameworks and position the work as a key tool in the fight to protect critical data and infrastructure from malicious traffic. Hence, the proposed hybrid model is a robust candidate for network security enhancement and well-suited for the challenges thrown up by SDN environments.

References

[1] Merkebaiuly, M. (2024). Overview of Distributed Denial of Service (DDoS) attack types and mitigation methods. Scientific Collection «InterConf+», (43 (193)), 494-508.

[2] Singh, J., & Behal, S. (2020). Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. Computer Science Review, 37, 100279.

[3] Setitra, M. A., Fan, M., Agbley, B. L. Y., & Bensalem, Z. E. A. (2023). Optimized MLP-CNN model to enhance detecting DDoS attacks in SDN environment. Network, 3(4), 538-562.

[4] Eliyan, L. F., & Di Pietro, R. (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. Future Generation Computer Systems, 122, 149-171.

[5] Wang, H., & Li, Y. (2024). Overview of DDoS attack detection in software-defined networks. *IEEE Access*.

[6] Bahashwan, A. A., Anbar, M., Manickam, S., Al-Amiedy, T. A., Aladaileh, M. A., & Hasbullah, I. H. (2023). A systematic literature review on machine learning and deep learning approaches for detecting DDoS attacks in software-defined networking. Sensors, 23(9), 4441.

[7] Alahmadi, A. A., Aljabri, M., Alhaidari, F., Alharthi, D. J., Rayani, G. E., Marghalani, L. A., ... & Bajandouh, S. A. (2023). DDoS attack detection in IoT-based networks using machine learning models: a survey and research directions. Electronics, 12(14), 3103.

[8] Verma, K. K., Singh, B. M., & Dixit, A. (2022). A review of supervised and unsupervised machine learning techniques for suspicious behavior recognition in intelligent surveillance system. International Journal of Information Technology, 14(1), 397-410.

[9] Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., Wang, C., & Liu, Y. (2018). A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges. *IEEE Communications Surveys & Tutorials*, *21*(1), 393-430.

[10] Baydoğmuş, G. K. (2021). The effects of normalization and standardization an Internet of Things attack detection. Avrupa Bilim ve Teknoloji Dergisi, (29), 187-192.

[11] Han, J., Kamber, M., & Pei, J. (2011). Data transformation and data discretization. Data mining: Concepts and techniques, 111-118.

[12] Sultan, F. R., Abdelmaksoud, I. R., & El-Bakry, H. M. (2024). Classification of DoS Attacks in IoT using Different Feature Selection Methods and Deep Learning.

[13] Van Der Maaten, L., Postma, E. O., & Van Den Herik, H. J. (2009). Dimensionality reduction: A comparative review. Journal of machine learning research, 10(66-71), 13.

[14] Mohammed, A. (2024). The Web Technology and Cloud Computing Security based Machine Learning Algorithms for Detect DDOS Attacks. Journal of Information Technology and Informatics, 3(1).

[15] Roopak, M., Parkinson, S., Tian, G. Y., Ran, Y., Khan, S., & Chandrasekaran, B. (2024). An Unsupervised Approach for the Detection of Zero-Day DDoS Attacks in IoT Networks. Authorea Preprints.

[16] Salama, A. M., Mohamed, M. A., & AbdElhalim, E. (2024). Enhancing Network Security in IoT Applications through DDoS Attack Detection Using ML. Mansoura Engineering Journal, 49(3), 10.

[17] Airlangga, G. (2024). Analysis and Comparison of Machine Learning Techniques for DDoS Attack Classification in Network Environments. Jurnal Informatika Ekonomi Bisnis, 38-46.

[18] Narayan, D. G., Heena, W., & Amit, K. (2024). A Collaborative Approach to Detecting DDoS Attacks in SDN Using Entropy and Deep Learning. Journal of Telecommunications and Information Technology.

[19] Babu, R. S. ., & Radhika, K. . (2023). DDoS Attack Detection using Swarm Optimized Random Forest Classification. International Journal of Intelligent Systems and Applications in Engineering, 12(8s), 231–238.

[20] Dasari, S., & Kaluri, R. (2024). An effective classification of DDoS attacks in a distributed network by adopting hierarchical machine learning and hyperparameters optimization techniques. IEEE Access.
[21] Rani, S. J., Ioannou, I., Nagaradjane, P., Christophorou, C., Vassiliou, V., Charan, S., ... & Pitsillides, A. (2023). Detection of DDoS attacks in D2D communications using machine learning approach. Computer Communications, 198, 32-51.
[22] Nisa, N., Khan, A. S., Ahmad, Z., & Abdullah, J. (2024). TPAAD: Two-phase authentication system for denial of service attack detection and mitigation using machine learning in software-defined network. International Journal of Network Management, 34(3), e2258.
[23] Thapngam, T., Yu, S., & Zhou, W. (2012, January). DDoS discrimination by linear discriminant analysis (LDA). In 2012 International Conference on Computing, Networking and Communications (ICNC) (pp. 532-536). IEEE.
[24] Sheth, V., Tripathi, U., & Sharma, A. (2022). A comparative analysis of machine learning algorithms for classification purpose. Procedia Computer Science, 215, 422-431.
[25] Tan, H. (2021, August). Machine learning algorithm for classification. In Journal of Physics: Conference Series (Vol. 1994, No. 1, p. 012016). IOP Publishing.
[26] Mondal, B., Koner, C., Chakraborty, M., & Gupta, S. (2022). Detection and investigation of DDoS attacks in network traffic using machine learning algorithms. Int. J. Innov. Technol. Explor. Eng, 11(6), 1-6.
[27] Elubeyd, H., & Yiltas-Kaplan, D. (2023). Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks. Applied Sciences, 13(6), 3828.
[28] Aldhyani, T. H., & Alkahtani, H. (2023). Cyber security for detecting distributed denial of service attacks in agriculture 4.0: Deep learning model. Mathematics, 11(1), 233.
[29] Pure Storage. (2023). What are machine learning performance metrics?, from https://www.purestorage.com/knowledge/machine-learning-performance-metrics.html

Alireza Rezaei
Orcid number: https://orcid.org/0009-0002-9916-3100
Alireza Rezaei received his bachelor's degree in electrical engineering from Imam Khomeini International University of Qazvin in 2023 and has been studying for a master's degree in computer engineering (artificial intelligence orientation) at Islamic Azad University, Karaj Branch since 2024. He is a researcher in the field of electricity and computers and has so far registered articles in the fields of control electricity, electronic city, artificial intelligence and machine learning, weather forecasting, quantum image encryption, etc.

Amineh Amini
Orcid number: https://orcid.org/0000-0001-8427-5455
Amineh Amini received her PhD from University of Malaya in 2014. Afterwards, she was a postdoctoral research fellow in University of Malaya. During her research, she has published several papers in well-known conferences and journals and she was nominated for the best paper award and she was winner of the best paper presentation award. She is currently an Assistant Professor and Head of Department of computer engineering in Karaj Azad University in Iran. She has successfully supervised a number of candidates and acted as Examiner as well. Her research interests include Data Stream Mining, and Software remodularization.