

Intrusion detection system for detecting distributed denial of service attacks using machine learning algorithms

Sabreen A. Zahra Mghames¹, Abdullahi Abdu Ibrahim²

¹Department of Scholarships and Cultural Relations, University of Information Technology and Communications, Baghdad, Iraq

²Department of Electrical and Computer Engineering, Altinbas University, Istanbul, Turkey

Article Info

Article history:

Received Oct 28, 2022

Revised Jun 9, 2023

Accepted Jun 17, 2023

Keywords:

Anomaly detection

Distributed denial of service attacks classification

Intrusion detection system

Machine learning

Services availability

ABSTRACT

Today, the creation of more effective intrusion detection system (IDS) has become crucial due to the rise in computer malware. Ensuring the availability of the system is an important component of information security and the most important requirement of any network. Recently the machine learning algorithm (ML) has been used to improve intrusion detection over the network. It is currently necessary to release an updated version of these systems. The presented work aimed to build a reliable and accurate IDS based on ML to classify and prevent distributed denial of service attacks to protect any system working on the network from temporary or complete system failure. We presented five ML models to create the proposed distributed denial-of-services attack (DDoS)-IDS, including (decision tree, random forest, logistic regression, support vector machine, and multi-layer neural network) which were trained and evaluated using the CIC-IDS-2018 dataset. Furthermore, principal component analysis (PCA) was used to reduce the dimensionality of the dataset. According to the classification results, the proposed multi-layer neural network model reached optimal performance for detecting DDoS attacks and achieved classification accuracy at 99.9992%.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Sabreen A. Zahra Mghames

Department of Scholarships and Cultural Relations

University of Information Technology and Communications

Baghdad, Iraq

Email: sabreenabd85@gmail.com

1. INTRODUCTION

In today's world, almost everyone has access to a computer, and network-based technology is rapidly evolving. As a result, network security has become a critical part, if not necessary, component of any computer system. A security attack or intrusion can be defined as any threat or unintentional attempt to destroy the availability, integrity, or confidentiality of any information resource or the information itself. Such threats could be limited by using an intrusion detection system (IDS) [1], [2]. Availability is a major part of information security, and it's the most fundamental requirement for any network. The network would cease to exist if its connection ports were unreachable or if its data routing and forwarding mechanisms were malfunctioning [3]. Therefore, Availability means that despite denial-of-service attacks, the network must always be accessible [4]. The proliferation of malware presents a serious problem for IDS architects to solve it. Since the creators of unknown and obfuscated malware typically employ multiple evasion techniques for information concealment in order to thwart detection by an IDS, spotting such threats can be a difficult task. The sophistication of malicious attacks has increased. Additionally, there has been an increase in security threats like zero-day attacks that target people who use the internet. Therefore, computer security has become paramount as the use

of information technology has permeated every aspect of our lives. The result is that the zero-day attacks have had a significant impact on many nations, including Australia and the US [5].

An IDS's goal is to quickly identify various malware types because a traditional firewall is unable to do so. The Literature survey which contains several related works are presented in this work, each study has a different methodology for Anomaly-based intrusion detection and attack classification. In the last year, IDS have a reputation for having a high accuracy and high detection rate. Furthermore, deploying and training them incurs a sizable computational cost. Kotpalliwar and Wajgi [6] they utilize support vectors machine (SVM) to classify attacks in KDD99 dataset and propose an IDS system that work on a single computer. Also, they achieved a validation accuracy of 89.8%. Subba *et al.* [7] the authors utilized the benchmark NSL-KDD 99 dataset with proposed model trains on different ML algorithms including SVM, artificial neural networks (ANN), and others methods. The overall average accuracy achieved at 98.6%. An *et al.* [8] they introduce unsupervised assassination analyses of IDS on distributed denial-of-services attack (DDos). Through this study they verify a higher scoring utilization rate of promoted these attacks. Tama *et al.* [9] they proposed the IDS model due to hybrid feature selection and ensembles of tow-levels classifiers, for reducing the dimensionality of the training set on (NSL-KDD and UNSW-NB15). Also, utilized three optimization methods which include Particle Swarm, Ant Colony, and genetic algorithm (GA), and the result of classification is 85.8% accuracy on the NSL-KDD dataset.

He *et al.* [10] the authors suggested combining the method of utilizing LSTM and multi-models deep autoencoder. On three different datasets from 1999 to 2017, this innovative approach was tested and achieved accuracy scores for multi-labels at 80%, 86%, and 98.6%. Thakkar and Lohiya [11], reviewed to the last several datasets that include new attack categories and network attack attributes. This article describes recent improvements in IDS datasets which can be used by a wide range of research societies as a mission statement for creating efficient and appropriate ML and data mining-based IDS. Khammassi and Krichen [12] the author proposed a wrapper feature selection method on UNSW-N15 and KDD99 datasets that were implemented with GA and logistic-regression (LR). The results show accuracy at 80% on the unsw-15 dataset with 42 features and 99.9% on KDD99 dataset with 19 selected features. Saranya *et al.* [13] they evaluate a number of ML models' performances against the KDD-99 dataset, and random forest (RF) outperformed other methods like SVMs, Naive Bayes, and Logistic Regression with an accuracy score of 99.81%. Kasongo and Sun [14] the researcher utilizes the UNSW-NB15 dataset and analyzed through several ML methods, this study refers to apply features selection techniques to proposed models were trained and tested to improving the accuracy score of binary and multi-class classification. The XGboost- based feature selection method improves the accuracy from 88% to 90.8% in DT model. Oliveira *et al.* [15] researcher utilized the MLP and LSTM on CIDS-01 dataset to build an accurate malicious classification model on sequential viewpoint. This study shows the LSTM was highly accuracy in sequential information pattern and achieved 99.96% classification accuracy.

The research problem could be summarized as Handle dataset problems by understanding data statistics and preprocessing steps. Design a reliable model based on the classification of a proposed dataset by training it on various attacks and normal one. Selecting the best feature using feature selection methods. Improving the detection rate with the best classification results. The proposed IDS is used to ensure the availability of the network and services by detecting malware from inter to the system such as Dos attacks and similar types. Such kind of these security systems can learn from the experience by preventing these attacks before threats happened. IDS is also useful and effective to increase the power of the security of the system behind the firewall which is lead to insure the availability of the services at run time.

2. THE COMPREHENSIVE THEORETICAL BASIS

What is intrusion detection: The term "intrusion" refers to a group of connected malicious acts carried out by an internal or external invader in an effort to breach the targeted system [16]. Monitoring computer systems, network traffic, and analyzing activity are all part of intrusion detection, which entails looking for potential system invasions. IDS is a set of tools and methods used for this goal [17].

In general, the majority of IDS offer standard functionality to protect network security. Data from observed actions are first gathered by an IDS. It provides thorough event-related data logging and correlates events from many sources. The detection engine, which uses various approaches and associated techniques depending on the circumstance, is the heart of an IDS [18], [19]. Additionally, preventative skills can be offered. The system in question is referred to as an intrusion detection and prevention system (IDPS) [20]. The most widely utilized approaches for intrusion detection are anomaly and signature based detection. In order to improve the performance of the IDS model, they are frequently employed in combination, either integrated or independently. Due to the utilization of information integrated from previous intrusions and vulnerabilities, "signature-based detection" also refers to misuse or knowledge-based detection. Because their patterns are unknown, this method is insufficient to identify unknown intrusions and known intrusion variants. Another issue is keeping the knowledge updated because it is a laborious and time-consuming process [17]. Anomaly-based detection can be defined as Any departure from typical behavior that is considered an anomaly. The

process of comparing typical behavior to observed events in order to locate significant deviations is known as anomaly-based detection, also known as behavior-based detection [15]. Anomaly detection techniques can be divided into three categories based on the target system's "behavioral" model and type of process: statistical-based, knowledge-based, and ML based.

2.1. Denial of service attacks (DoS)

DoS is an active attack [21] that overloads the network with requests or packets, crashing servers, and systems. There may be a very large number of users available in the network given the current size of the network [22]. Any attack on a networking system that prevents a server from providing services to its clients is known as a denial of service (DoS) attack. Attacks can include overflowing a server with large packets of invalid data, sending requests with an incorrect or spoofed IP address, or sending millions of requests in an attempt to slow it down [23].

2.2. Distributed denial of service attacks (DDoS)

The master DDoS is a piece of malicious software that attackers install in an effort to take control of a collection of compromised machines situated within a similar network [24]. It also acts as a pioneer threat to service providers. A DDoS attack specifically aims to disturb and deny services to authorized users by deluging the target with a large volume of malicious requests Figures 1 and 2 shows the architecture and the process of DDoS attacks [25].

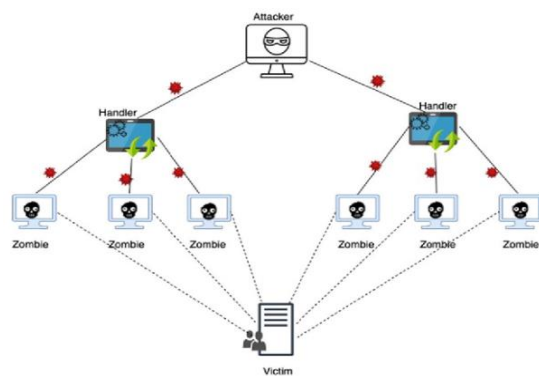


Figure 1. The architecture of DDoS

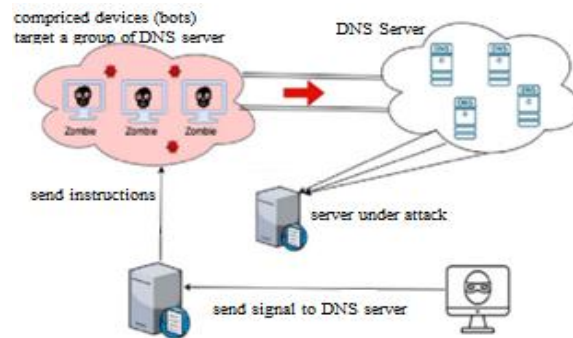


Figure 2. The process of DDoS

2.3. ML algorithms for attack classification

There are several ML algorithms are utilized in this work to create the proposed IDS models which include DT, RF, LR, SVM, and multi-layer artificial neural network (ML-ANN). The DT is a useful algorithm for finding solutions to problems involving classification and regression. This method is good for small datasets but, in the large dataset, the uses of DT caused overfitting problems. However, DT pruning with overfitting issues and it could be limited by using the tree pruning technique it will be affected by a small dataset. Another algorithm works with the same strategy as DT but utilizes multiple trees and split the task called RF [26]. The LR algorithm is among the simplest regression analysis methods. Although it is the simplest and most direct regression model, it is also the most popular and widely used in real-world applications [26]. SVM is one of the most powerful ML algorithms and it is used commonly to solve pattern recognition problems and a variety of classification and regressions tasks. It works by splitting the data samples using a hyperplane, the best hyperplane can fit the training set by computing the maximum distance between two support vectors which is called the "maximum margin" [27]. ML-ANN is a deep network that can represent functions of increasing the process complexity and solving the large data by adding more layers and more nodes within each layer. This algorithm can solve big data and large-scale tasks with accuracy and speed results [28].

3. METHOD

In this section, we present the research problems and the proposed solutions via sets of procedures were consisting of three phases: the first phase is concern with data acquisition. The CSE-CIC-IDS2018 dataset in [29], is a Canadian Institute for Cyber Security (CIC) that has released CSE-CIC-IDS2018, a new and comprehensive intrusion detection dataset built on Amazon Web Services (AWS) in 2018 it was amassed to facilitate actual attacks. This dataset is an enhancement version of the CSE-CICIDS2017 dataset, includes the

required specifications for the attack dataset, and extends protection against many common threats. The second phase is the preprocessing steps applied to the dataset includes understanding the data via statistic, missing values and outlier handling, features scaler, and data splitting. The used dataset contains 79 columns (78 features, 1 class label) and approximately 1,048,575 rows. The class names and distribution are shown in Table 1.

Table 1. The class names and distribution

Labels names	Number of samples
Benign	360833
DDOS attack-HOIC	686012
DDOS attack-LOIC-UDP	1730

The used dataset does not have any missing values and all features are in the same data type which is an integer or float 64bit and 32bit, except one column named (time-stamp) has time and date values. To address this issue, this column must be removed since it takes into account outliers from other columns and has an impact on how the ML algorithm is trained. The features were reduced by one after the time-stamp column was eliminated. Most likely, the attributes in our dataset have different scales, but we can't give the ML algorithm those data, so rescaling is necessary. Attributes are ensured to be scaled equally by data rescaling. Typically, attributes are rescaled to fall between 0 and 1. The dataset was divided into a 75% training set that used to train the proposed models and a 25% testing set are used for evaluating the models' performance. This splitting procedure is utilized for all proposed ML models. The third phase is related to building our proposed models. In order to start building the proposed models to classify and distinguish between each class in the CSE-CIC-IDS-2018 dataset. The dataset contains 78 features and 1 label (classes) and is formatted in a CSV file. The classes are (benign, DDOS attack-HOIC, DDOS attack-HOIC-UDP) and over 104,8575 samples. The group of ML algorithms is proposed to do this job which includes (DT, RF, LR, SVM, and MLP-N), our methodology divided into two phases: the first phase concerned with training the proposed ML model using all features to determine which ML algorithm are doing well and obtain higher detection rate. The second phase concerns applying the features selection method principal component analysis (PCA) in order to select the robust features and reduce the dimensionality of the dataset. The PCA works by sorting the feature variance from high to low, then the highest variance refers to robust features. After features are selected, the proposed ML models are re-trained using 15 selected features instead of all 78 features. Figure 3 illustrates the diagram of the workflow procedure.

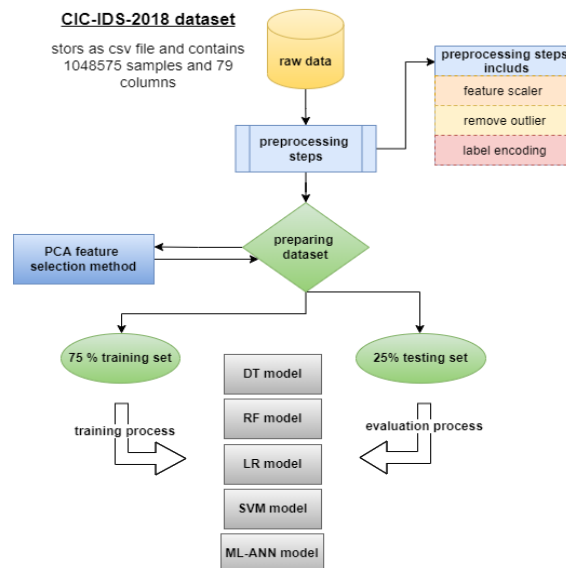


Figure 3. Illustrates the diagram of the workflow procedure

The information about the training process and the hyperparameters of the proposed models are described as follows: the DT model was created utilizing Gini-index criteria with min-samples-splits=2 and max-features=0.5, the RF model contains 30 trees and also used the same criteria of DT model, the LR model was trained on 100

iterations and optimized by “SGD” method, the SVM proposed model used linear as kernel and the proposed ML-ANN contained one input layer with 78 units fully connected with two hidden layers: first hidden contained 100 unit and the second contained 20 units, the activation function for all layers are (ReLU) and the optimization method utilized (Adam) and the number of epochs=300 finally, the regularization technique is early stop.

4. RESULTS AND DISCUSSION

This section related to shows the experimental results of the proposed ML algorithm that was used to build our DDoS-IDS. Table 2 illustrated the classification metrics including accuracy, mean square error (MSE), precision, recall, and F1-score were used for the evaluation process of the first phase on 262144 supported samples. The results in Table 2 show that the proposed DT and RF models were going through an overfitting problem because of a large number of features 78. The proposed DT model has a misclassification rate in class (0) according to a low precision rate or false positive fraction. The overfitting issue is limited in the testing performance of the RF model but, it still has a low detection rate at an accuracy of 82%. The other proposed models including (LR, SVM, and ML-ANN) are achieved very good classification results and the lowest MSE. Obviously, there is no overfitting problem even with all the features used because of the efficiency of regularization techniques (early stop) used. The next step is applying the PCA features selection method. As mentioned earlier, this method works by computing eigenvalues and an eigenvector with a covariance matrix for all features and then sorting the features according to highest variance to lowest variance. It's a very powerful method to identify robust features. The output of the second phase by applying PCA is illustrated in the Table 3.

Table 2. The classification results of IDS

ML-proposed models for IDS	Accuracy %	MSE	Avg precision	Avg recall	F1-score
DT	65.95	0.3405	0.7622	0.7711	0.7620
RF	82.82	0.1717	0.8824	0.8570	0.8754
LR	99.998	0.00023	0.9992	1	0.9996
SVM	99.999	0.000019	0.9992	1	0.9996
ML-ANN	99.998	0.000019	0.9999	0.9999	0.9999

Table 3. The output of PCA and features variance

Number of features component	PCA variance values	Number of features component	PCA variance values
1	3.24814350e-01	12	1.47061227e-02
2	2.09720689e-01	13	1.32074744e-02
3	1.08312813e-01	14	1.08842327e-02
4	7.18553917e-02	15	9.59272758e-03
5	5.86990076e-02	16	7.28700519e-03
6	4.45226107e-02	17	3.40671053e-03
7	2.97387519e-02	18	2.71322876e-03
8	2.76632665e-02	19	2.35216019e-03
9	2.39571375e-02	20	1.17911601e-03
10	1.75332157e-02
11	1.47702502e-02	78	1.31804761e-33

From Table 3, the results refer to the robust features in the dataset, and it is clear we don't need all 78 features to reach the optimal detection rate. Furthermore, the first sorted 15 features from the Table 4 could be more reliable and accurate classification results even with the weak models (DT, RF). Let's present the classification results in Table 4 after applying the PCA features selection method.

According to the comparison results mentioned in Table 4, this experiment improved the classification accuracy of weak models (DT, RF) shown in Table 2. Furthermore, the strong models (LR, SVM, ML-ANN) still have the same strong classification performance after applying PCA (15 features) and also, the model size is smaller than using all features (78 features). In addition, the proposed ML-ANN model has optimal performance at an accuracy of 99.9992% and the lowest MSE of 0.000007. Table 5 illustrates the comparison results of the proposed IDS based on ML-ANN and other related works.

Table 4. The comparison results of the proposed ML model after PCA

ML-proposed models for IDS	Testing accuracy %	Testing MSE
DT	99.9950	0.000095
RF	99.9984	0.000015
LR	99.9927	0.000095
SVM	99.9935	0.000076
ML-ANN	99.9992	0.000007

Table 5. The comparison results of the proposed IDS and other related works

ML-methods for IDS	Used dataset	Results of the accuracy %
In [6] used SVM	KDD99	89.8
In [7] used ANN	KDD99	99.8
In [9] used Particle Swarm, Ant Colony, and genetic algorithm (GA)	(NSL-KDD and UNSW-NB15)	85.8
In [13] SVMs, Naive Bayes, LR, and RF	KDD99	99.81
Proposed IDS based on ML-ANN	CSE-CIC-IDS2018	99.9992

To visualize the obtained results, Figure 4 show the comparing results in confusion matrix (CM) of the week model (DT) and the density curve of the actual and the predicted class of evaluation process before/after applying feature selection method PCA. In Figure 4(a) CM before PCA and Figure 4(b) CM after PCA. While Figure 4(c) shows the distribution classes before PCA and Figure 4(d) the distribution classes after PCA.

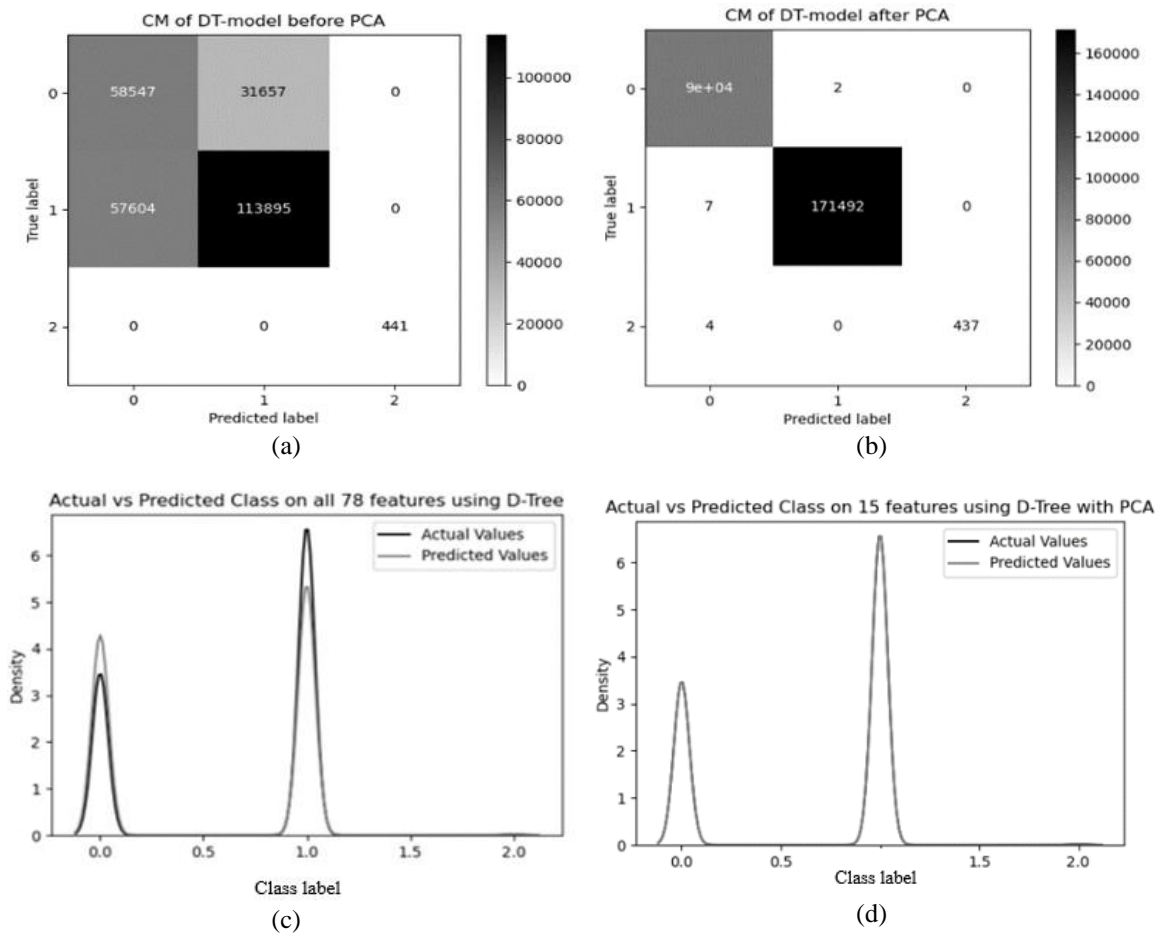


Figure 4. Comparing the results of the proposed DT-model in confusion matrix and the class distribution density in (a) CM before PCA, (b) CM after PCA, (c) distribution classes before PCA, and (d) distribution classes after PCA

To visualize the strongest proposed model (ML-ANN) which achieved a magnificent detection rate and lowest MSE, Figure 5 show the comparing results in CM and the density curve in evaluation process before/after applying feature selection method PCA. In Figure 5(a) CM before PCA and Figure 5(b) CM after PCA. While Figure 5(c) shows the distribution classes before PCA and Figure 5(d) the distribution classes after PCA.

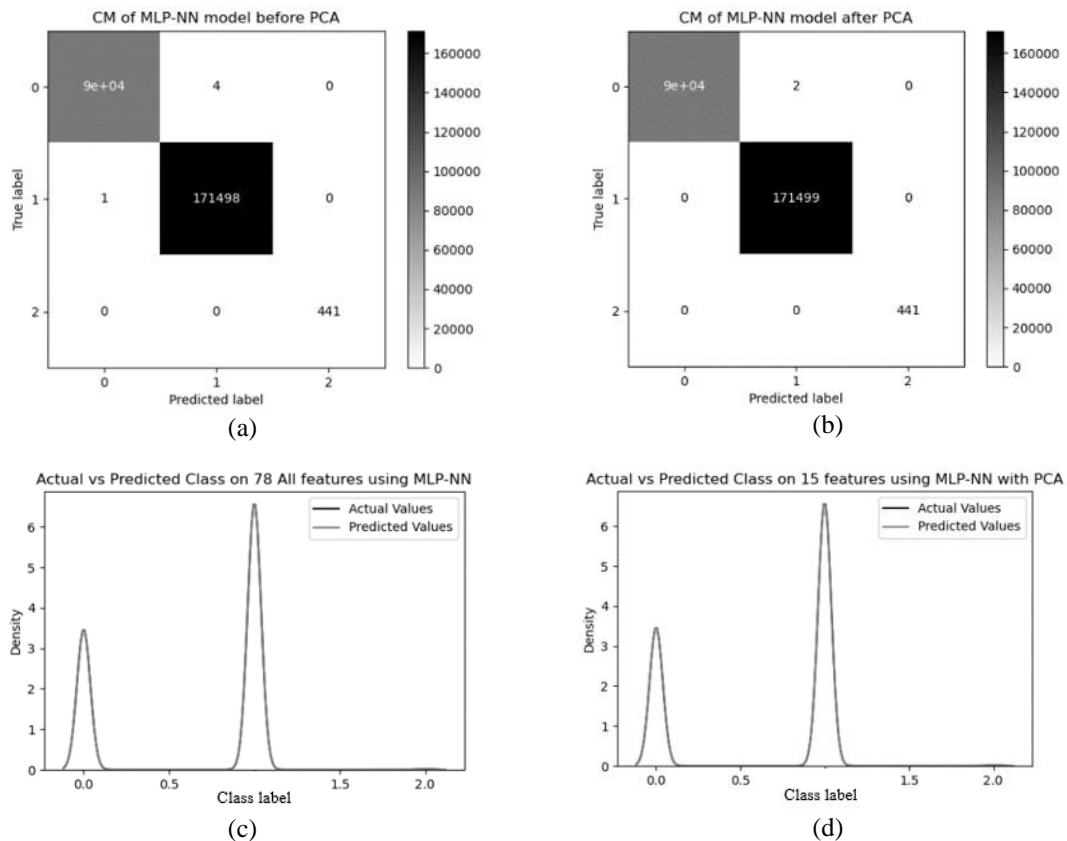


Figure 5. Comparing the results of MLP-NN model in CM and the class distribution density in (a) CM before PCA, (b) CM after PCA, (c) distribution classes before PCA, and (d) distribution classes after PCA

5. CONCLUSION

In this work, we present five proposed models that have the ability to classify DDoS attacks and insure the availability of the systems that provides online services. The proposed methodology of building DDoS-IDS is done perfectly and the conclusions of the presented work can be summarized as follows: The statistical summary was useful to better understand the dataset and identify the problems. It also refers to the variation of feature values. The standard scaler preprocessing technique improved the training and testing set by limiting the variety of features. The PCA feature selection method improves the classification results and prevents the overfitting problem in the DT model. The proposed ML-ANN model achieved a magnificent testing performance even when utilizing all the features in the dataset. For the future work, we propose to increase the model capacity by applying additional types of DoS attacks in order to increase the reliability of the proposed ML-ANN model.





REFERENCES

- [1] S. K. Wagh, V. K. Pachghare, and S. R. Kolhe, "Survey on intrusion detection system using machine learning techniques," *International Journal of Computer Applications*, vol. 78, no. 16, pp. 30–37, Sep. 2013, doi: 10.5120/13608-1412.
- [2] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, "A survey of moving target defenses for network security," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1909–1941, 2020, doi: 10.1109/COMST.2020.2982955.
- [3] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. K. Bashir, "A survey of security and privacy issues in the Internet of Things from the layered context," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 6, 2022, doi: 10.1002/ett.3935.
- [4] N. Shah and S. Valiveti, "Intrusion detection systems for the availability attacks in ad-hoc networks," *International Journal of Electronics and Computer Science Engineering (IJECSSE, ISSN: 2277-1956)*, vol. 1, no. 3, pp. 1850–1857, 2012.
- [5] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, Jul. 2019, doi: 10.1186/s42400-019-0038-7.
- [6] M. V. Kotpalliwar and R. Wajgi, "Classification of attacks using support vector machine (SVM) on KDDCUP'99 IDS database," in *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, Apr. 2015, pp. 987–990, doi: 10.1109/CSNT.2015.185.
- [7] B. Subba, S. Biswas, and S. Karmakar, "A neural network based system for intrusion detection and attack classification," in *2016 Twenty Second National Conference on Communication (NCC)*, Mar. 2016, doi: 10.1109/NCC.2016.7561088.
- [8] X. An, J. Su, X. Lü, and F. Lin, "Hypergraph clustering model-based association analysis of DDOS attacks in fog computing intrusion detection system," *Eurasip Journal on Wireless Communications and Networking*, vol. 2018, 2018, doi: 10.1186/s13638-018-1267-2.





- [9] B. A. Tama, M. Comuzzi, and K. H. Rhee, "TSE-IDS: a two-stage classifier ensemble for intelligent anomaly-based intrusion detection system," *IEEE Access*, vol. 7, pp. 94497–94507, 2019, doi: 10.1109/ACCESS.2019.2928048.
- [10] H. He, X. Sun, H. He, G. Zhao, L. He, and J. Ren, "A novel multimodal-sequential approach based on multi-view features for network intrusion detection," *IEEE Access*, vol. 7, pp. 183207–183221, 2019, doi: 10.1109/ACCESS.2019.2959131.
- [11] A. Thakkar and R. Lohiya, "A review of the advancement in intrusion detection datasets," *Procedia Computer Science*, vol. 167, pp. 636–645, 2020, doi: 10.1016/j.procs.2020.03.330.
- [12] C. Khammassi and S. Krichen, "A NSGA2-LR wrapper approach for feature selection in network intrusion detection," *Computer Networks*, vol. 172, p. 107183, May 2020, doi: 10.1016/j.comnet.2020.107183.
- [13] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. Khan, "Performance analysis of machine learning algorithms in intrusion detection system: a review," *Procedia Computer Science*, vol. 171, pp. 1251–1260, 2020, doi: 10.1016/j.procs.2020.04.133.
- [14] S. M. Kasongo and Y. Sun, "Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset," *Journal of Big Data*, vol. 7, no. 1, Nov. 2020, doi: 10.1186/s40537-020-00379-6.
- [15] N. Oliveira, I. Praça, E. Maia, and O. Sousa, "Intelligent cyber attack detection and classification for network-based intrusion detection systems," *Applied Sciences (Switzerland)*, vol. 11, no. 4, pp. 1–21, Feb. 2021, doi: 10.3390/app11041674.
- [16] A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3211–3243, Oct. 2021, doi: 10.1007/s11831-020-09496-0.
- [17] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," *National Institute of Standards and Technology*, 2007, doi: 10.6028/nist.sp.800-94.
- [18] S. Ponmaniraj, R. Rashmi, and M. V. Anand, "IDS based network security architecture with TCP/IP parameters using machine learning," in *2018 International Conference on Computing, Power and Communication Technologies, GUCON 2018*, Sep. 2019, pp. 111–114, doi: 10.1109/GUCON.2018.8674974.
- [19] A. Kim, M. Park, and D. H. Lee, "AI-IDS: application of deep learning to real-time web intrusion detection," *IEEE Access*, vol. 8, pp. 70245–70261, 2020, doi: 10.1109/ACCESS.2020.2986882.
- [20] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowledge-Based Systems*, vol. 189, p. 105124, Feb. 2020, doi: 10.1016/j.knosys.2019.105124.
- [21] Q. Chen, H. Chen, Y. Cai, Y. Zhang, and X. Huang, "Denial of service attack on IoT system," in *Proceedings - 9th International Conference on Information Technology in Medicine and Education, ITME 2018*, Oct. 2018, pp. 755–758, doi: 10.1109/ITME.2018.00171.
- [22] S. Shanmuga Priya, M. Sivaram, D. Yuvaraj, and A. Jayanthiladevi, "Machine learning based DDOS detection," in *2020 International Conference on Emerging Smart Computing and Informatics, ESCI 2020*, Mar. 2020, pp. 234–237, doi: 10.1109/ESCI48226.2020.9167642.
- [23] K. M. Elleithy, D. Blagovic, W. K. Cheng, and P. Sideleau, "Denial of service attack techniques: analysis, implementation and comparison," *Journal of Systemics, Cybernetics, and Informatics*, vol. 3, pp. 66–71, 2005.
- [24] H. Sinanovic and S. Mrdovic, "Analysis of Mirai malicious software," in *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Sep. 2017, doi: 10.23919/SOFTCOM.2017.8115504.
- [25] A. Aljuhani, "Machine learning approaches for combating distributed denial of service attacks in modern networking environments," *IEEE Access*, vol. 9, pp. 42236–42264, 2021, doi: 10.1109/ACCESS.2021.3062909.
- [26] D. Sarkar, R. Bali, and T. Sharma, *Practical machine learning with Python*. Apress, 2018.
- [27] A. Pradhan, "Support vector machine-a survey," *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, no. 8, pp. 82–85, 2012.
- [28] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*. MIT press, 2016.
- [29] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, vol. 2018-January, 2018, pp. 108–116, doi: 10.5220/0006639801080116.

BIOGRAPHIES OF AUTHORS



Sabreen A. Zahra Mghames     she has M.Sc. in information technologies in Altinbas University at Istanbul/Turkey. Interested in research areas are image processing, bioinformatics, medical image analysis, machine learning and pattern recognition. She is work at University of Information Technology and Communications (UoITC) at Baghdad/Iraq. She can be contacted at email: sabreenabd85@gmail.com.



Abdullahi Abdu Ibrahim     he is an Enthusiastic and passionate Academia with a strong interest in teaching and research. Obtained a bachelor's and M.Sc. in computer engineering from Eastern Mediterranean University (North Cyprus) and a Ph.D. in electrical and computer engineering from Altinbas University (Turkey). Research interests include computer networks, wireless sensor networks, wireless body area network, machine learning and internet of things. He can be contacted at email: abdullahi.ibrahim@altinbas.edu.tr.