INSTITUTE OF INFORMATION
AND COMMUNICATION TECHNOLOGIES
BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **26**, No 2
Sofia • 2026 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2026-0020

Cross-Dataset DDoS Intrusion Detection Using Hybrid Welch-Point-Biserial Feature Selection and DenseMLP

Raghupathi Manthena[1], *Radhakrishna Vangipuram*[2]

[1]*Department of Computer Science and Engineering, JNTU Hyderabad, India*
[2]*Department of Information Technology, VNRVJIET Hyderabad, India*
E-mails: mraghu30@gmail.com radhakrishna_v@vnrvjiet.in (*corresponding author*)

***Abstract*:** *Distributed Denial-of-Service* (*DDoS*) *attacks are one of the major threats in the cybersecurity domain. Lightweight feature selection is vital for improving DDoS attack detection efficiency and computational efficiency by selecting the most relevant features. Recently, numerous machine learning and deep learning models have been developed to detect various types of DDoS attacks; however, their performance is often hindered by the presence of irrelevant features, which can lead to increased false positives and longer processing times. To address this problem, we propose the WPBS-MLP Intrusion Detection System* (*IDS*)*. The WPBS* (*Welch's t-Test and Point Biserial Test*) *feature selection method is integrated with an optimized MLP classifier to detect DDoS attacks. It was evaluated on the CICDDoS2019, CICIDS2018, and CICIDS2017 publicly available intrusion detection datasets. The WPBS method selected 39 significant features from the CICDDoS2019 dataset, and these 39 features are retained and considered for experimentation w.r.t all datasets. The DenseMLP model achieved a range of 99.59% to 100% accuracy for binary classification and 84% to 100% accuracy for low-rate and high-rate attack detection across the three datasets. Further, the Wilcoxon statistical test provided validation evidence that the proposed WPBS-MLP-based IDS model showed superior performance compared to the existing research studies.*

***Keywords*:** *DDoS, Low-rate, High-rate, Welch's t-Test, Point Biserial test, DenseMLP, CICDDoS2019.*

1. Introduction

Recently, the evolution of internet technologies has accelerated significantly, corresponding to the intensifying needs of modern human interactions such as communication, commerce, education, and intelligent automation, thereby transforming the global digital ecosystem. However, alongside these technological advancements, there has been a notable rise in complex and targeted cyberattacks, which have become major concerns for securing network infrastructures. Cyber

threats have increased with the emergence of interconnected digital systems. Among these cyberattacks, Distributed Denial-of-Service (DDoS) attacks are severe threats to the network infrastructures. [1-3]. Various reputed organizations like Twitter, Reddit, GitHub, Amazon, and Spotify are affected by these attacks [4-6]. The Intrusion Detection System (IDS) is a vital tool to protect the network infrastructure against DDoS attacks by monitoring network traffic and detecting malicious actions that take place [7-13].

Most of the research prioritizes the classification model over feature selection, even though feature selection is a key factor in developing IDS using ML models to enhance detection performance [14-18]. The conventional feature selection approaches are filter-based [19], wrapper-based, and embedded-based methods, which have their own limitations. In addition, there is limited research on validating feature relevance before detection; it raises issues like duplicate or irrelevant features, higher false positives, degraded performance, and increased computational overhead. These created a research gap to propose a statistical and correlation-based feature selection method and hinder the overfitting issue [20]. In addition to this, there was limited research on detecting the low-rate and high-rate DDoS [21, 22].

In this paper, we addressed the major key challenge in enhancing the effectiveness of IDS for DDoS detection. Effective preprocessing and feature selection are essential to minimize data complexity, accelerate model training, and enhance detection performance. We proposed a statistical and correlation-based feature selection method, which consists of Welch's t-test and the Point Biserial test (WPBS). The Welch's t-test will select the statistically significant features, and among these, the correlation problem will be addressed using the PBS test. The WPBS method is integrated with a customized DenseMLP classifier to accurately extract the complex relationships between the significant features for detecting DDoS and benign traffic. It was evaluated on the CICIDS2017, CICIDS2018, and CICDDoS2019 datasets. The paper analyzes deeply the capability of the model to detect DDoS attacks and compares it with the performance of the traditional ML classifiers and existing IDS works.

There are four contributions.

- A lightweight feature selection method, WPBS, is proposed to reduce the feature space and minimize the overburden on the IDS system.
- The WPBS method was evaluated on modern IDS datasets CICDDoS2019, CICIDS2018, and CICIDS2017, and optimized the feature space from 87 features to 39 features.
- The WPBS method integrated with the DenseMLP classifier improved the detection of DDoS attacks and classification of low-rate and high-rate attacks.
- The WPBS-MLP model achieved 99.59% average accuracy over the CICDDoS2019, CICIDS2018, and CICIDS2017 datasets.

The structure of the paper is as follows: The related works section covers existing IDS works based on ML and DL techniques; the methodology section briefly discusses the proposed framework; and the results and discussion section evaluate the WPBS-MLP model on CICDDoS2019 while comparing it to state-of-the-art methods.

2. Related work

Network traffic data usually contains high-dimensional features. Therefore, proper data visualization techniques are needed to select a suitable IDS model [23], as they help in identifying patterns and anomalies in the high-dimensional features that are crucial for effective DDoS attack detection. The detection of DDoS attacks presents an important problem for network security and has been an active area of research. The use of Machine Learning (ML) and Deep Learning (DL) in Intrusion Detection Systems (IDS) has received a lot of attention in recent years. This section discusses some of the important contributions, with particular attention to applying deep neural networks and Multi-Layer Perceptrons (MLPs) to intrusion detection.

2.1. Machine learning-based IDS

These methods have traditionally utilized models like decision trees, naive Bayes, Support Vector Machines (SVM), and random forests. Indicatively, T a v a l l a e e et al. [24] tested the base classifiers using the NSL-KDD dataset, and they noted the need to develop models that can be applied successfully to new attacks. Equally, M o u s t a f a and S l a y [7] presented the UNSW-NB15 dataset and used standard ML methods to show that they can identify various types of attacks. G. K i m, L e e and S. K i m [10] designed a hybrid IDS using C4.5 and SVM ML classifiers to tackle the training and testing time complexity. Furthermore, M o u s t a f a, T u r n b u l l and C h o o [25] also furthered this debate by assessing IDS models in IoT settings and using data that comprises UNSW-NB-15, which deals with new security issues in connected devices. Other works have focused on mining the multifaceted spatial-temporal characteristics of network traffic to increase detection rates. A y a d, N e h a l and H i k a l [26] suggested a hybrid feature selection approach that consists of PCC and SCC correlation ranking methods. In their work, they used an ML classifier to detect and classify network attacks. And they achieved 99.94% accuracy on the CICIDS2019 dataset. Another author, H a l l e d y et al. [28], suggested 25 time-based features, which achieved 98.58% accuracy using the XGB classifier. To improve the DDoS detection accuracy, [29] suggested DDADA and DDAML algorithms based on the degree of attack using four handcrafted flow features. Though it achieved a 99.4% detection rate, it may limit their performance in complex and real-world networks with diverse traffic patterns and evolving DDoS attack strategies, particularly because these environments can introduce unpredictable variables that challenge the effectiveness of static detection methods.

To address the dimensionality issue and detect attacks at an early stage, G a u r and K u m a r [30] suggested a NIDS combination of ANOVA and XGBoost classifier. The ANOVA test identified 15 relevant features that achieved 98.84% accuracy on the CICDDoS2019 dataset. H i r s i et al. [31] achieved an accuracy of 97.62% with the RF model using Chi-square to select 26 features from the CICDDoS2019 dataset. These models have some limitations, like scalability, robustness, and overfitting and underfitting issues due to the absence of hyperparameter tuning of the detection model, which can affect their overall performance and generalizability in real-world applications. And R a n i et al. [32]

suggested another RF model approach to detect DDoS attacks, using 6 features and achieving an accuracy of 99.12%. It was limited to SYN DDoS attack detection. Kumari and Jain [33] suggested a hybrid feature selection and detection model consisting of RFE and PCA for feature selection and LDA and GNB for detection. It achieved 99.98% accuracy, though it has several limitations, such as dataset dependency, real-time implementation challenges, the need for adaptive defense mechanisms, and difficulties in integration with existing network security frameworks, which may hinder its practical application in diverse environments.

2.2. Deep learning-based IDS

Recently, deep learning techniques have been in the spotlight as they have been empowered by their ability to automatically derive complex feature representations out of raw data. Shone et al. [12] designed a Non-symmetric Deep Auto-Encoder (NDAE) network-based framework that uses deep auto-encoders to extract the unsupervised features. Similarly, Ashiku l and Dagli [34] used Long Short-Term Memory (LSTM) networks to extract temporal correlations in network traffic to achieve higher detection of subtle and stealthy attacks. In intrusion detection applications, a dense multi-layer perceptron, a form of fully connected feedforward neural network, has been popular, especially where structured tabular data is a factor. Dhanabal and Shantharajah [35] showed that MLPs have better precision and recall than the traditional shallow classifiers on KDD data. These contributions to the IDS implementation are valuable. The expansion of the cyber-attack landscape necessitates updating these models with the current IDS datasets. Lopez-Martin et al. [36] used the CICIDS2017 dataset in MLPs and achieved excellent results, i.e., the model is capable of dealing with the class imbalance and demonstrates its resilience. Additional training benefits, such as dropout, batch normalization, and ReLU activation functions, have also helped in the better generalization and training stability of the MLP-based IDS models. Even though Convolutional Neural Networks (CNNs) and recurrent neural networks (RNNs) are more popular than MLPs in the field of IDS, they have disadvantages in computational performance and their use with fixed-length tabular data, typical of network traffic analysis. Lansky et al. [37] state that MLPs represent a compromise of model complexity and detection performance, especially when used with efficient feature selection and preprocessing. Several studies have used the CICDDoS2019 dataset to develop useful intrusion detection systems. Javaid et al. [38] suggested a deep learning-based IDS that uses neural networks to detect DDoS attacks and showed better detection accuracy when compared to traditional machine learning IDS. Ebtihal and Abbass [39] used a set of machine learning classifiers on this dataset, demonstrating the strengths and weaknesses of each of the approaches in classifying various attack vectors.

Haider et al. [40] used the RF regressor and Deep CNN model to extract rich features for detection tasks, aiming to improve DDoS detection accuracy. More advanced hybrid and deep learning architectures have been investigated, in addition to the traditional ML models. Elubeyd and Yiltas-Kaplan [41] proposed a hybrid deep learning model for DDoS detection, achieving significant performance

gains through a multi-stage approach. Elsayed et al. [42] introduced a DDoSNet to identify DDoS attacks on the CICDDoS2019 dataset, which deals with the aspect of feature redundancy and model complexity. Sharafaldin et al. [43] generated the realistic intrusion detection dataset CICDDoS2019 with various DDoS attacks in the context of the development of an IDS system. Bakro et al. [44] designed a GOA bioinspired feature selection method for selecting important features, and they achieved 98.54% accuracy on the CICDDoS2019 and CICIDS2017 datasets using a random forest model. Aktar and Nur [45] suggested a DCEA model to detect the DDoS attacks; it achieved 97.58% accuracy on the CICDDoS2019 dataset and 92.45% accuracy on the CICIDS2017 dataset.

U. Chanu, K. Singh and Y. Chanu [46] identified nine important features using the Ensemble Feature Selection (EFS) method (Information Gain, Gain Ratio, Chi, OneR, and Symmetrical Uncertainty Ranking) and detected DDoS attacks using the MLP-GA model with 98.9% accuracy using the CICIDS 2017 dataset. The [47] and [48] works achieved 98% and 99.6% accuracies using DNN models. The DNN models were trained using the important features selected by the EFS methods. These works detected DDoS attacks but overlooked the importance of feature relevance during feature selection, and their methods are complex for large or high-dimensional datasets. To handle the overfitting and improve the detection performance, Thakkar, and Lohiya [49] suggested a combined feature ranking method integrating with the DNN model. Although this method achieved more than 99% accuracy on three different datasets, it is limited by its reliance on simple statistical measures, which may overlook complex feature interactions and exhibit dataset-dependent performance, even with reduced execution time. Pandey and Mishra [50] developed a two-tier hybrid model to address the entropy-based and machine learning-based detection limitations and achieved excellent accuracies across the CICDDoS2019 and CICIoT2023 datasets using the EXT classifier with 20 selected features.

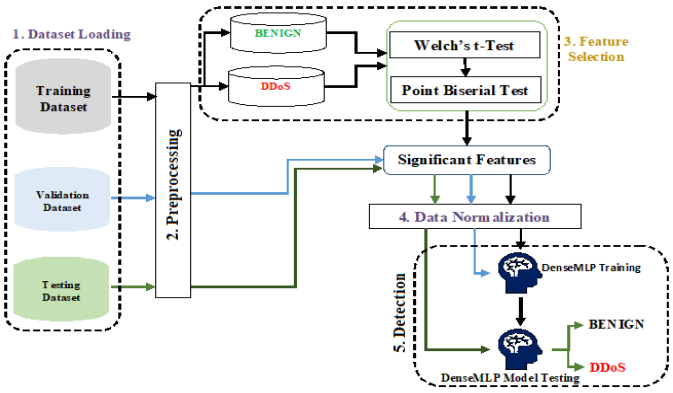


Fig. 1. Integrated WPBS-MLP framework for DDoS attack detection

Hanmate and Hussain [51], using feature transformation, extracted relevant information and developed a deep CNN-based robust IDS system, and achieved an accuracy range from 99.79% up to 100%. However, the model's

generalization and transferability across diverse network environments remain limited. Hussain et al. [53] suggested a hybrid IDS system that consists of Q-learning feature selection and a deep ANN. It achieved 99% accuracy on BoT-IoT, Ton-IoT, and CICIDS 2017 for detecting various attacks. Nevertheless, these could not address the generalization and scalability of an IDS system. Although these advantages exist, several issues persist in the use of MLP-based IDS models; these include the inability to cope with vastly unbalanced data sets, the absence of real-time detection benchmarks, and the overfitting due to over-deep structure models. In this study, we build upon other studies by creating an optimized DenseMLP classifier integrating the WPBS feature selection method to overcome these problems.

3. Methodology

In this paper, we present a DenseMLP framework for detecting DDoS attacks named WPBS-MLP. The proposed approach for detecting DDoS attacks contains four phases: 1. Dataset loading; 2. Dataset preprocessing; 3. Feature selection using the WPBS method; 4. Data normalization; 5. Detection.

3.1. Dataset loading

In the first phase, the intrusion detection dataset is given as input to the algorithm. The experiments were conducted using the publicly available CICDDoS2019, CICIDS2018, and CICIDS2017 datasets, which contain real-time network traffic traces comprising both benign and DDoS activities. The dataset may contain missing values, unsupported data format values, and socket features. These types of information need to be processed; for this purpose, the loaded dataset is forwarded to the data preprocessing phase.

3.2. Dataset preprocessing

This stage takes responsibility for identifying the missing and unsupported data, like NaN or inf-containing instances, and removes them from the dataset if and only if those instances are less than 0.05% of the total dataset population. Following this phase, the socket features (SourceIP, DestinationIP, Source Port, Destination Port, Protocol, etc.) were removed, which have standard values and make less contribution to differentiating DDoS attacks and normal traffic. The pre-processed dataset is given as an input to the feature selection stage.

3.3. Feature selection

A successful data pre-processing strategy focuses on selecting the most important and relevant features for building a predictive model. This process reduces computational complexity and speeds up execution, which improves the model's overall performance. Feature selection methods are typically divided into filter, wrapper, and embedded approaches. The filter-based methods rank the features quickly using statistical criteria but may fail to notice feature interactions. Wrapper methods evaluate feature subsets with a learning algorithm for higher accuracy, but

they are computationally expensive. Embedded methods select important features during model training, which speeds up the process but means that the chosen features depend heavily on the specific model's inherent biases.

In this work, a WPBS feature selection approach is designed for selecting significant features, which combines the Welch's t-test [54-57] and the point biserial test [58, 59]. The algorithm explains the step-by-step process of this approach. The proposed WPBS feature selection finds the most important features for intrusion detection. This reduces the number of features and improves how well the system detects intrusions. The method evaluates each feature's importance using a hypothesis test and by looking at how features are related to each other. The Welch's t-test and Point Biserial (PBS) test were used for hypothesis testing, followed by testing the correlation among the features.

As depicted in Algorithm Step 2, the pre-processed dataset is divided into two groups, BENIGN and DDoS, based on the class label, such as: if the class label contains benign, those are assigned to the BENIGN group; otherwise, assigned to the DDoS group. The DDoS group instances contain various types of DDoS attacks like DrDNS, DrLDAP, DrNTP, etc. In the WPBS method, first, Welch's t-test will be performed to select the important features, then the point biserial test will be performed on the important features to get the best-ranked features.

3.3.1. Welch's t-Test

To perform the Welch's t-test, we formulated two hypotheses: The Null Hypothesis (NH) is that there is no significant difference between the two groups, and the Alternative Hypothesis (AH) is that there is a significant difference between the two groups. If the NH is accepted and the AH is rejected, then the feature is not important. If AH is accepted and NH is rejected, then the feature is considered important. The decision of rejection or acceptance is based on the Welch's t-test score (Ws) and p-value.

As presented in algorithm Step 3, from the BENIGN and DDoS group, at a time one feature is selected and the mean and variance are computed using Equations (1) and (2). Based on the mean and variance, the W_s score will be calculated using Equation (3), and the p-value will be calculated using Equation (4). If the p-value is less than 0.05, for those features, it represents that NH is rejected and determines that the feature is significant; otherwise, the feature is insignificant. This procedure will continue until the last feature of the dataset and the significant feature subset are obtained.

The above procedure is performed iteratively for all DDoS attack labels from the DDoS group, comparing with the BENIGN group. For each DDoS attack label, the significant feature subset is obtained. On those individual feature subsets, the union operation is performed to discard the duplicate features. After performing the union operation on the feature subsets, we select the Important Features (IFs) and retain only those features in the dataset. Then, the selected important features were given as input to the PBS test,

(1) $$\text{mean} = \frac{\sum_{i=1}^{n} x_i}{n},$$

(2) $$\text{Variance} = \frac{\sum_{i=1}^{n}(x_i - \text{mean})^2}{n-1},$$

(3) $$W_s = \frac{\text{DDoS}_{\text{GroupMean}} - \text{Benign}_{\text{GroupMean}}}{\sqrt{\frac{\left(\text{DDoS}_{\text{GroupVariance}}\right)^2}{N} + \frac{\left(\text{Benign}_{\text{GroupVariance}}\right)^2}{M}}},$$

(4) $$\text{p-value} = 2 \times \left(1 - \Phi(|\text{statistic\_value}|)\right).$$

3.3.2. Point Biserial (PBS) test

The PBS test measures the correlation (r) between two groups using Equation (5), then calculates the p-value based on the t-statistic value of them. The r-value will be in the range of –1 and +1. A positive value indicates strong support for the feature, while a negative value suggests support in the opposite direction. After keeping the important features from both groups, we choose a feature from them, and then calculate the average. This is shown in the Equation (5), the r value of that feature will be measured using the mean values, where n_1 is the number of DDoS group instances, n_2 is the number of benign group instances, and N is the total number of instances in both groups. Then, after the t-statistic value is calculated, the p-value is calculated based on the t-statistic value. Based on the r-value and p-value, we determine if the feature is significant or insignificant. If the feature r-value is positive and greater than zero, and the p-value is less than 0.05 (if +r>0 and the p-value<0.05), then that feature is considered for further steps. Likewise, determine the feature subset by iterating over all the features. Select the features from the subset whose r-values are more than the mean r-value. This procedure is performed over all the attack classes, and the feature subsets are found w.r.t each DDoS attack label. On the feature subset, a union operation is to be performed to extract the significant features

(5) $$r = \frac{\text{Mean}_{\text{DDoSGroup}} - \text{Mean}_{\text{BenignGroup}}}{\text{Mean}_{\text{Total}}} \left(\sqrt{\frac{n_1 \times n_2}{N}}\right).$$

Algorithm: WPBS feature selection method

Input: Dataset $D_{X \times Y}$ where X is instances, Y is features

Output: Significant features list F

Start

Step 1. Preprocess the dataset D

→Remove Socket Features like {Flow ID, Source IP, Destination IP, Protocol, etc.}

→Remove instances with NaN or Infinity values.

→Remove Duplicate Features

Step 2. Split the Dataset D into $\text{Benign}_{\text{Group}}$ and $\text{DDoS}_{\text{Group}}$ groups

Step 3. Apply Welch's t-Test on $\text{Benign}_{\text{Group}}$ and $\text{DDoS}_{\text{Group}}$ groups

→Obtain the $\text{DDoS}_{\text{GroupMean}}$, $\text{Benign}_{\text{GroupMean}}$ using Equation (1) and $\text{DDoS}_{\text{GroupVariance}}$, $\text{Benign}_{\text{GroupVariance}}$ using Equation (2) for a feature.

→Compute the W_s value

$$W_s(\text{feature}) = \frac{\text{DDoS}_{\text{GroupMean}} - \text{Benign}_{\text{GroupMean}}}{\sqrt{\frac{\left(\text{DDoS}_{\text{GroupVariance}}\right)^2}{N} + \frac{\left(\text{Benign}_{\text{GroupVariance}}\right)^2}{M}}}$$

→ Obtain the p-value

$$\text{p-value} = 2 \times \left(1 - \Phi(|W_s(\text{feature})|)\right)$$

→Determine whether the feature is important.

If (p-value (feature) $<$ 0.05)

Repeat for all features and select important features

Step 4. Retain the important features from the dataset *D*

Step 5. Apply the Point Biserial Test

→Obtain the $\text{Mean}_{\text{DDoSGroup}}$, $\text{Mean}_{\text{BenignGroup}}$, $\text{Mean}_{\text{Total}}$, n_1, n_2 and N for a feature

→Compute the $r(\text{feature})$ value

$$r(\text{feature}) = \frac{\text{Mean}_{\text{DDoSGroup}} - \text{Mean}_{\text{BenignGroup}}}{\text{Mean}_{\text{Total}}} \left(\sqrt{\frac{n_1 \times n_2}{N}}\right)$$

→ Obtain the p-value

$$\text{p-value} = 2 \times \left(1 - \Phi(|\text{r(feature)}|)\right)$$

→Determine the feature as significant.

If (p-value (feature) $<$ 0.05 && $r(\text{feature}) > 0$)

Repeat for all features and store significant features to *F*

Step 6. Return the significant features list *F*

Stop

3.4. Data normalization

The data normalization takes the input as a dataset with significant features and transforms all the data points to a single scale. In this process, we utilized the min-max scaling to transform the data on a scale of 0 and 1 using Equation (6). The multi-class labels are converted into binary class labels, such as BENIGN and DDoS.

(6) $$\text{min}-= \frac{X - \text{Min}(X)}{\text{Max}(X) - \text{Min}(X)}.$$

3.5. Detection

The goal is to detect DDoS attacks with better accuracy and reduce the false positive rates. In this detection phase, we utilized the customized multi-layer perceptron classifier (DenseMLP) to detect the DDoS attacks. The DenseMLP classifier architecture consists of one input layer, one output layer, and five hidden layers. After each hidden layer, perform the batch normalization followed by the ReLU activation function. The hidden layers having 1024, 512, 256, 128, and 64 neurons were used as consequent hidden layers. During classifier training, a batch size of 1024 was used, and the learning rate and beta_1 parameters were set to 0.001 and 0.999, respectively. The output layer uses the sigmoid activation function. This layer takes a single value from the last hidden layer and applies the sigmoid function to it. If the resulting sigmoid value is 0.5 or higher, the instance is classified as a DDoS attack; otherwise, it's classified as BENIGN.

4. Results

This section presents the evaluation results of the WPBS-MLP framework for DDoS detection over the three intrusion detection datasets: CICDDoS2019, CICIDS2017, and CICIDS2018. All the experiments were executed on a Lenovo system, which consists of 192 GB RAM and a 1.96 GHz speed Intel processor with a Windows operating system. To simulate the proposed work, we utilized the Jupyter IDE tool and Python scripts. The experiments were conducted with the WPBS method and without the WPBS method.

4.1. Datasets

The publicly available intrusion detection datasets CICIDS2017, CICIDS2018, and CICDDoS2019 were utilized for evaluating the WPBS-MLP framework performance. The population of the CICIDS2017 dataset is more than 30 lakhs with 79 features, which were captured on seven weekdays. It covered the 14 different types of attack classes and one benign class. In this paper, we utilized the Friday collected network traffic CSV file, which contains 225,711 instances of DDoS and benign traffic. Due to the unavailability of a separate distribution for training and testing, we split the sample into an 80-10-10 percentage of the dataset. Table 1 presents information about the training, validation, and testing datasets.

The CICIDS2018 dataset population is more than 16 lacs with 80 features. This dataset covered nine types of intrusion attack classes related to network traffic. Among all the classes, the benign class has the majority of instances, with 83% of the dataset. The Wednesday network traffic file has been taken for experimentation, which contains the DDoS and benign flows. The detailed information of the sample dataset is depicted in Table 1.

Table 1. The sampled dataset information

SN	Dataset	Class label	Number of instances		
			Training	Validation	Testing
1	CICIDS2017	BENIGN	78,148	9785	9753
		DDoS	102,420	12,786	12,819
	Total		180,568	22,571	22,572
2	CICIDS2018	BENIGN	139,946	30,022	30,032
		DDoS HOIC	138,839	29,732	29,699
		DDoS LOIC	1215	246	269
	Total		280,000	60,000	60,000
3	CICDDoS2019	BENIGN	56,425	56,425	56,306
		DrWebDDoS	439	NA	NA
		DrUDP_Lag	31,194	5068	1873
		DrNetBIOS	31,194	5068	9072
		DrLDAP	31,194	5068	9072
		DrMSSQL	31,194	5068	9072
		DrDNS	31,194	5068	NA
		DrSYN	31,194	5068	9072
		DrUDP	31,194	5068	NA
		DrTFTP	31,194	5068	NA
		DrNTP	31,194	5068	NA
		DrSNMP	31,194	5068	NA
		DrSSDP	31,194	5068	NA
	Total		399,998	112,173	112,611

The CICDDoS2019 dataset contains more than seven crore instances with 87 features. Moreover, it covered thirteen variants of modern DDoS attacks (like DrPortMap, DrNetBIOS, DrUDP, DrUDP-Lag, DrSYN, DrNTP, DrDNS, DrLDAP, DrMSSQL, DrSNMP, DrSSDP, DrWebDDoS, and DrTFTP). The authors of [60] explored that it is a reliable IDS dataset for developing ML or DL models to detect modern-day DDoS attacks, so we considered it a benchmark dataset. For the experimentation, we sampled the training, validation, and testing datasets from the 70 milion instances, such as: collected 400,000 instances for training, 100,000 for validation, and testing. Among the three datasets, the training and validation sets contain 12 DDoS attack class labels, and the testing set contains seven attack labels. The detailed information about the sample datasets of CICDDoS2019 is depicted in Table 1.

4.2. Evaluation metrics

The evaluation metrics will explore the model performance in terms of Accuracy (Acc), Precision (Pre), F-score (Fsc), Sensitivity (Sn), Specificity (Sp), and Balanced Accuracy (BA).

Confusion Matrix =

Actual \ Predicted		
	TP	**FN**
	FP	**TN**

First, we generated a confusion matrix for the predicted and actual class labels information, then we calculated all these metrics using the following equations:

$$\text{accuracy (Acc)} = \frac{\text{TP+TN}}{\text{TP+TN+FN+FP}}, \tag{6}$$

$$\text{precision (Pre)} = \frac{\text{TP}}{\text{TP+FP}}, \tag{7}$$

$$\text{sensitivity (Sn)} = \frac{\text{TP}}{\text{TP+FN}}, \tag{8}$$

$$\text{specificity (Sp)} = \frac{\text{TN}}{\text{TN+FP}}, \tag{9}$$

$$\text{F1-score(Fsc)} = 2 \times \frac{\text{Pre} \times \text{Sn}}{\text{Pre} + \text{Sn}}, \tag{10}$$

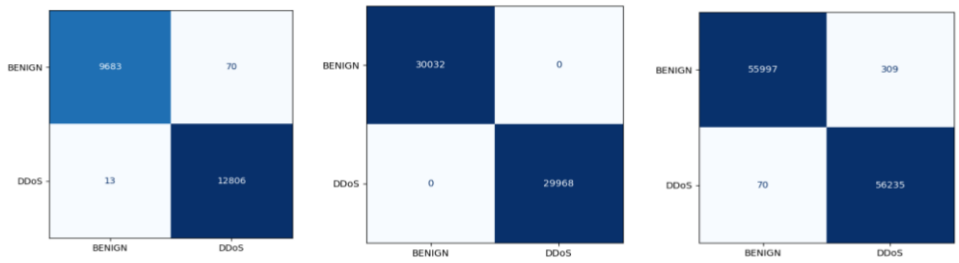
$$\text{Balanced Accuracy (BA)} = \frac{\text{Sn+Sp}}{2}. \tag{11}$$

4.3. Evaluation on CICDDoS2019 dataset

The proposed framework integrates the parts: the WPBS feature selection method and the ML model. The WPBS method was evaluated on the most recent and reliable ID dataset, CICDDoS2019. As shown in Fig. 1, the training dataset was loaded into the framework and pre-processed, while missing value instances, redundant features, and socket features were removed. After preprocessing, the number of features was reduced from 87 to 78. The 78 features were subjected to Welch's t-test. The Welch's t-test eliminated 8 features and yielded 66 significant features with a 95% confidence level. These features were retained from the dataset and given to the point biserial test. The PBS test obtained 39 significant features are Idle Min, Bwd Packet Length Std, Bwd Packets/s, Flow Packets/s, Fwd Packet Length Min, Flow Duration, URG Flag Count, CWE Flag Count, Packet Length

Mean, Bwd IAT Mean, Bwd IAT Max, Min Packet Length, Fwd IAT Total, Fwd Packet Length Std, Flow IAT Mean, Average, Packet Size, Fwd Packet Length Mean, Init_Win_bytes_forward, Fwd IAT Max, Idle Max, Inbound, Idle Std, Total Fwd Packets, Total Length of Fwd Packets, Fwd Packet Length Max, Init_Win_bytes_backward, Fwd IAT Std, Fwd Header Length, ACK Flag Count, act_data_pkt_fwd, min_seg_size_forward, Flow IAT Max, Max Packet Length, Bwd IAT Std, Fwd IAT Mean, Idle Mean, Fwd Packets/s, Flow Bytes/s, and Flow IAT Std. These features were retained from the training, validation, and testing datasets. Next, we normalized the datasets using min-max normalization to ensure uniform data scaling was maintained. After that, we encoded the class labels. All attack classes were labeled as DDoS, and the benign class was labeled as BENIGN.

Binary class classification. An optimized DenseMLP classifier, as discussed above in Section 3, was trained using the training dataset. While training, a validation dataset is given for evaluating at each epoch and improving model performance. At the seventeenth epoch, the model performance converged. To evaluate the performance of the model on the testing dataset. For the test dataset, the model has given the prediction results. From the prediction results, the confusion matrix was generated and depicted in Fig. 2. Furthermore, the evaluation metrics were calculated and recorded as Acc = 99.66%, Sn = 99.87%, Sp = 99.45%, Pre = 99.45%, Fsc = 99.66%, and BA = 99.66% from the confusion matrix. Whereas the baseline 78 features showed the performance metrics results as Acc = 97.32%, Sn = 99.33%, Sp = 94.71%, Pre = 94.97%, Fsc = 97.39%, and BA = 97.32%. It is determined that the proposed WPBS-selected features showed superior performance over the baseline 78 features.



(a) (b) (c)

Fig 2. Confusion matrices: CICIDS2017 (a); CICIDS2018 (b); CICDDoS2019 datasets (c)

The DenseMLP model ROC curves represent the balanced performance of DDoS and BENIGN predictions, which was depicted (see Fig. 3a). The effectiveness of the proposed WPBS method is also evaluated using eleven other machine learning models. Except for the QDA model, the remaining models also showed accuracy in the range of 92% to 99%. As depicted in Table 2, the Dense MLP model's performance compared with existing ML models, such as Decision Tree (DT), Adaboost (ADB), KNN, Naïve Bayes (NB), Linear Discriminant Analysis (LDA), Ridge, Quadratic Discriminant Analysis (QDA), Random Forest (RF), and XGBoost (XGB), showed better performance.

Table 2. Results on CICDDoS2019 dataset

SN	Classifier	With the WPBS approach						Without the WPBS approach					
		Sn	Sf	Pre	Acc	Fsc	BA	Sn	Sf	Pre	Acc	Fsc	BA
1	ADB	99.93	88.01	89.29	93.97	94.31	93.97	99.90	91.31	92.00	95.61	95.79	95.61
2	DT	85.65	86.69	86.55	86.17	86.10	86.17	83.71	94.23	93.55	88.97	88.36	88.97
3	EXT	99.99	96.30	96.43	98.14	98.18	98.14	99.99	94.99	95.23	97.49	97.55	97.49
4	KNN	99.99	96.40	96.52	98.19	98.23	98.19	99.92	96.71	96.82	98.32	98.35	98.32
5	LDA	98.73	94.21	94.46	96.47	96.55	96.47	99.86	86.65	88.20	93.25	93.67	93.25
6	LR	99.86	97.32	97.39	98.59	98.61	98.59	99.79	95.36	95.56	97.58	97.63	97.58
7	NB	90.13	99.31	99.24	94.72	94.47	94.72	92.01	97.18	97.02	94.59	94.45	94.59
8	QDA	100.00	0.11	50.03	50.06	66.69	50.06	100	0.11	50.03	50.05	66.69	50.06
9	RF	99.91	97.17	97.24	98.54	98.56	98.54	99.79	97.66	97.71	98.73	98.74	98.73
10	Ridge	98.82	87.17	88.51	92.99	93.38	92.99	99.82	89.33	90.34	94.58	94.85	94.58
11	XGB	99.99	97.11	97.19	98.55	98.57	98.55	99.99	96.63	96.74	98.31	98.33	98.31
12	DenseMLP	**99.66**	**99.87**	**99.45**	**99.45**	**99.66**	**99.66**	**99.93**	**94.71**	**94.97**	**97.32**	**97.39**	**97.32**

4.4. Evaluation on CICIDS2017 and CICIDS2018

The significant features identified in the CICDDoS2019 dataset using the WPBS method were projected on the CICIDS2017 and CICIDS2018 datasets. Among these 39 features, the inbound feature is not available in both datasets. Due to this, experiments were conducted on both datasets using 38 features. These features were retained from the datasets. Thereafter, the MLP classifier was trained using the training dataset, while the validation dataset was used to validate the model. The trained MLP model was tested using the testing datasets. Likewise, other ML classifiers are trained and tested with these datasets. The evaluation metrics for all models over the CICIDS2017 and CICIDS2018 datasets are calculated from the confusion matrices, which are depicted in Fig. 2a and Fig. 2b. These metric results of the ML classifier over the CICIDS2017 and CICIDS2018 datasets are depicted in Tables 3 and 4. As represented in Fig. 3a and Fig. 3b, ROC curves were generated to determine the AUC score and balanced performance of the model. The AUC score was calculated on both datasets as 1.0; it indicates that the model showed better balanced accuracy.

Table 3. Binary classification results obtained on the CICIDS2017 dataset

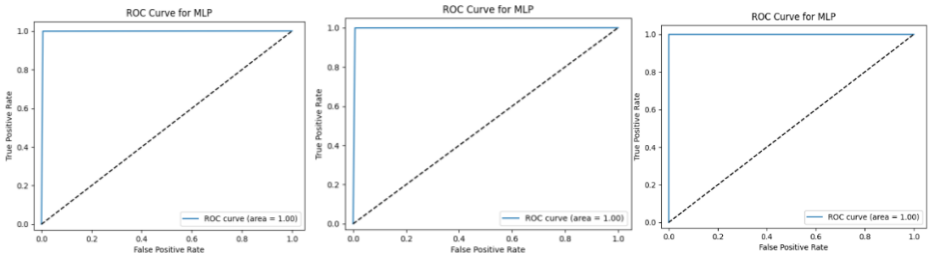
SN	Classifier	With the WPBS approach						Without the WPBS approach					
		Sn	Sf	Pre	Acc	Fsc	BA	Sn	Sf	Pre	Acc	Fsc	BA
1	ADB	99.90	93.77	95.47	97.25	97.63	96.83	100	99.94	99.95	99.97	99.99	99.99
2	DT	99.95	99.00	99.24	99.53	99.59	99.47	99.97	99.85	99.88	99.92	99.92	99.91
3	EXT	99.97	99.87	99.90	99.92	99.93	99.92	99.93	99.98	99.98	99.95	99.95	99.95
4	KNN	99.98	99.69	99.77	99.86	99.88	99.84	99.97	99.97	99.98	99.97	99.98	99.98
5	LDA	99.89	93.48	95.27	97.12	97.52	96.68	91.89	50.00	70.88	73.87	80.02	70.94
6	LR	99.87	96.42	97.35	98.38	98.59	98.14	99.87	97.60	98.21	98.89	99.09	98.81
7	NB	0.00	100.00	0.00	43.21	0.00	50.00	0.00	100	0.00	43.02	0.00	50.00
8	QDA	0.00	100.00	0.00	43.21	0.00	50.00	0.00	100	0.00	43.02	0.00	50.00
9	RF	99.50	99.83	99.87	99.64	99.68	99.66	67.44	99.99	99.99	81.44	80.55	83.71
10	Ridge	99.89	92.99	94.93	96.91	97.35	96.44	82.90	95.79	96.31	88.44	89.10	89.34
11	XGB	83.13	99.89	99.90	90.37	90.74	91.51	98.73	99.97	99.98	99.26	99.85	99.35
12	DenseMLP	99.89	99.28	99.46	99.63	99.68	99.59	99.93	99.98	99.98	99.95	99.98	99.98

The DenseMLP model achieved Acc = 99.63%, Sn = 99.89%, Sp = 99.28%, Pre = 99.46%, Fsc = 99.68%, and BA = 99.59% using proposed features on the CICIDS2017 dataset. Whereas, the baseline 78 features achieved the following metric results: Acc = 99.95%, Sn = 99.93%, Sp = 99.98%, Pre = 99.98%,

Fsc = 99.98%, and BA = 99.98%. Here, the WPBS-selected features showed 0.32% lower in terms of accuracy.

Table 4. Binary classification results obtained on the CICIDS2018 dataset

SN	Classifier	With the WPBS approach						Without the WPBS approach					
		Sn	Sf	Pre	Acc	Fsc	BA	Sn	Sf	Pre	Acc	Fsc	BA
1	ADB	100	100	100	100	100	100	100	99.99	99.99	100	100	100
2	DT	49.72	100	99.99	74.89	66.42	74.86	100	100	100	100	100	100
3	EXT	77.86	100	100	88.94	87.55	88.93	100	100	100	100	100	100
4	KNN	100	100	100	100	100	100	100	100	100	100	100	100
5	LDA	100	99.97	99.97	99.99	99.99	99.99	49.59	99.98	99.95	74.81	66.29	74.78
6	LR	99.48	99.97	99.97	99.73	99.72	99.72	100	99.98	99.98	99.99	99.99	99.99
7	NB	97.93	69.37	76.13	83.64	85.67	83.65	99.98	99.97	99.97	99.98	99.98	99.98
8	QDA	0.00	100	0.00	50.05	0.00	50.00	0.00	100	0.00	50.05	0.00	50.00
9	RF	92.92	100	100	96.46	96.33	96.46	100	100	100	100	100	100
10	Ridge	100	99.99	99.99	99.99	99.99	99.99	49.59	99.99	99.99	74.82	66.30	74.79
11	XGB	47.92	100	100	73.99	64.80	73.96	90.31	100.00	100.00	95.16	94.91	95.15
12	DenseMLP	100	100	100	100	100	100	100	100	100	100	100	100



(a) (b) (c)

Fig. 3. ROC curves of (a) CICIDS2017, (b) CICIDS2018 and (c) CICDDoS2019 datasets

On the CICIDS2018 dataset, the DenseMLP model achieved Acc = 100%, Sn = 100%, Sp = 100%, Pre = 100%, Fsc = 100%, and BA = 100% using WPBS-selected features. Whereas, the baseline 78 features achieved the following metrics results: Acc = 100%, Sn = 100%, Sp = 100%, Pre = 100%, Fsc = 100%, and BA = 100%. The proposed WPBS-selected features have given equal performance to the baseline features by reducing the feature space from 78 to 39.

Table 5. Wilcoxon signed rank test results

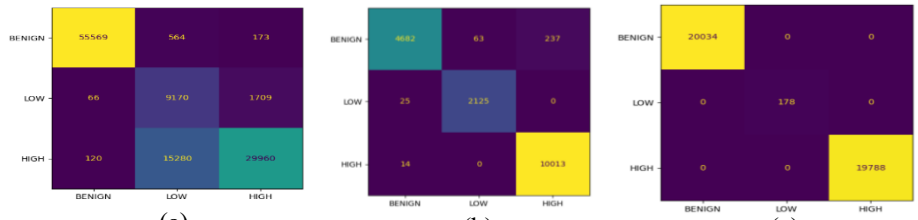
VS	R^+	R^-	Exact p-value	Asymptotic p-value
ADB	145.5	25.5	0.0071330000000000005	0.008419
Decision tree	151.0	2.0	4.578×10^{-5}	0.000385
EXT	127.5	43.5	0.07011	0.062741
KNN	90.5	80.5	≥0.2	0.810697
LDA	169.5	1.5	1.9069×10^{-5}	0.000155
Logistic regression	167.0	4.0	5.34×10^{-5}	0.000306
Naïve bayes	168.0	3.0	3.814×10^{-5}	0.000301
QDA	150.0	3.0	7.63×10^{-5}	0.000333
Random forest	124.5	28.5	0.02169	0.020912
Ridge	169.5	1.5	1.9069×10^{-5}	0.000036
XGB	157.5	13.5	7.553×10^{-4}	0.001592

All the classifiers showed more than 90% balanced accuracies on the CICIDS2017, except QDA and NB. These two classifiers showed a higher performance in terms of specificity, whereas the rest of the metrics showed very low performance. Among all the models, DT, EXT, KNN, RF, and MLP showed excellent performance compared to other models on the CICIDS2017 dataset. Except for the DT, QDA, EXT, and XGB models, the rest of the models showed better performance on CICIDS2018. Among those, the ADB, KNN, and MLP models achieved 100% detection performance.

From the above discussions on the models' performances over the three datasets, we observed that some of the models showed better performance on some of the datasets. For instance, the DenseMLP model has given better performance on the CICIDS2018 and CICDDoS2019 datasets compared to the rest of the models, whereas it was shown to be lower than other models on the CICIDS2017 dataset.

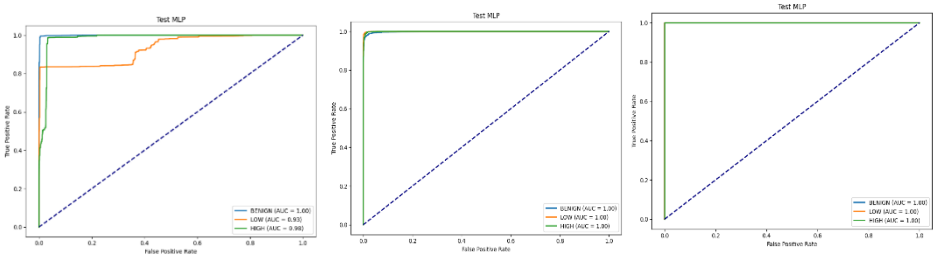
We conducted the Wilcoxon signed-rank validation test to understand the generalizable performance of the model over the three IDS datasets. This non-parametric test decides which model showed consistent performance across the three datasets. The Wilcoxon test results are depicted in Table 5. It indicates that the MLP model has higher R+ values than the rest of the models, such that the MLP model performed well across the three datasets, irrespective of the data sizes.

Ternary class classification. The existing research work was limited to detecting the DDoS attacks, but the low-rate attacks show more impact on network infrastructure by slowly entering the network, which can lead to significant degradation of service over time and make them harder to identify compared to high-rate attacks. To address this issue, the dataset class labels are converted into low-rate, high-rate, and benign classes (ternary classes) using Andrew curves [61]. The optimized DenseMLP model was trained using the ternary class dataset with 39 significant features. On the trained model, we applied a test dataset to evaluate the model's performance. Fig. 4 and Fig. 5 depict the confusion matrices and ROC curves of the predictions over the three test datasets. The accuracy, precision, and f-score values of the proposed model are 84.09%, 91.30%, and 85.81%, respectively, obtained on the CICDDoS2019 dataset. On the other two datasets (CICIDS2018 and CICIDS2017), the proposed model achieved accuracy, precision, and F-score values ranging from 98% to 100%. These results show that the proposed model achieved good performance over the three IDS cross-datasets. These ternary results are depicted in Table 6.



(a) (b) (c)

Fig. 4. Ternary class confusion matrices of: CICIDS2017 (a); CICIDS2018 (b); CICDDoS2019 datasets (c)



(a) (b) (c)

Fig. 5. Ternary class ROC curves of: CICIDS2017 (a); CICIDS2018 (b), CICDDoS2019 datasets (c)

Table 6. Ternary class classification results

SN	Dataset	Acc	Pre	Fsc
1	CICIDS2017	98.02	98.04	98.00
2	CICIDS2018	100	100	100
3	CICDDoS2019	84.09	91.30	85.81

State-of-the-art comparison with existing studies. As we discussed above, the DenseMLP model showed better performance integrating with the WPBS feature selection method. The WPBS-MLP framework performance was compared with the existing DDoS detection studies. For the comparison, the feature subsets reported in the respective studies were first mapped to our sampled CICDDoS2019 and CICIDS2017 datasets, retaining only the corresponding features available in our dataset. These retained feature subsets were then used as inputs to the same DenseMLP architecture. The performance results of existing studies using feature subsets on the CICIDS2017 dataset were depicted in Table 7, and the results of existing studies on the CICDDoS2019 dataset were depicted in Table 8.

Table 7 presents the proposed model performance comparison with existing IDS works using different feature subsets on the CICIDS2017 dataset. The existing works [20, 40, 26] showed less than 98% accuracy on CICIDS2017 for DDoS detection, whereas the proposed work showed higher accuracy at 99.63%. Compared to the existing works, it shows superior performance for detecting low-rate and high-rate attacks with 98.02%, 98.04%, and 98% in terms of accuracy, precision, and F-score.

Furthermore, the proposed WPBS method selected 39 features, and its performance was compared with the existing works' suggested feature subsets on the CICDDoS2019 dataset. As presented in Table 8, the WPBS-MLP model on the CICDDoS2019 dataset showed 99.66%, 99.87%, 99.45%, 99.66%, and 99.66% results in terms of sensitivity, specificity, precision, F-score, and balanced accuracy for detecting DDoS attacks. We observed that the existing work [47] used 80 features, and its accuracy is 0.10% higher than our model's, whereas our model got higher performance on the rest of the metrics with a lower feature space. Our model achieved higher balanced accuracy, which was not mentioned in the existing works. The BA shows that both DDoS and BENIGN instances are how accurately they are detected. Nevertheless, our proposed model has superior performance to the [28, 30-32, 47, 48, 52] existing works in terms of Acc, Pre, Rec, F-score, and BA. Our model showed superior performance to the existing works for detecting

low-rate and high-rate DDoS attacks in terms of accuracy (84.09%), precision (91.30%), and F-score (85.81%), whereas it was 0.15% lower compared to the work [47].

Table 7. Performance comparison with existing studies on the CICIDS2017 dataset

SN	Reference	Feature selection method	No of features	Binary classification						Ternary classification		
				Sn	Sf	Pre	Acc	Fsc	BA	Acc	Pre	Fsc
1	[46]	Ensemble	9	98.01	98.05	99.19	98.02	98.60	98.03	95.93	96.00	95.93
2	[40]	RF	4	97.05	92.17	96.82	95.64	96.94	94.61	95.25	95.22	95.25
3	[20]	Filter and wrapper	10 (RF)	97.70	91.57	96.60	95.93	97.15	94.64	97.06	97.06	97.06
4			10 (IG)	91.02	92.80	96.87	91.53	93.85	91.91	93.72	93.73	93.72
5	**Proposed**	**WPBS**	**39**	**99.89**	**99.28**	**99.46**	**99.63**	**99.68**	**99.59**	**98.02**	**98.04**	**98.00**

Table 8. Performance comparison with existing studies on the CICDDoS2019 dataset

SN	Reference	Feature selection method	No of features	Binary classification						Ternary classification		
				Sn	Sf	Pre	Acc	Fsc	BA	Acc	Pre	Fsc
1	[52]	t-Test	59	99.52	98.09	98.11	98.80	98.81	98.80	82.56	89.11	84.19
2	[27]	SFFS	10	65.59	58.68	61.35	62.13	63.40	62.13	71.22	81.69	74.51
3	[28]	Time based	25	98.51	82.89	85.20	90.70	91.38	90.70	66.06	90.50	70.68
4	[47]	SAE	80	99.67	99.49	99.49	99.58	99.58	99.58	84.24	91.48	86.13
5	[48]	EFS	10	99.02	99.34	99.34	99.18	99.18	99.18	58.08	89.05	66.24
6	[30]	ANOVA	15	59.37	95.20	92.52	77.29	72.33	77.29	62.99	74.11	62.47
7	[32]	RF	7	99.41	56.32	69.48	79.48	81.79	77.87	83.33	87.42	83.34
8	**Proposed**	**WPBS**	**39**	**99.66**	**99.87**	**99.45**	**99.45**	**99.66**	**99.66**	**84.09**	**91.30**	**85.81**

5. Conclusion

In this study, we presented an integrated framework that combines statistical hypothesis test-based WPBS feature selection with a DenseMLP model to detect DDoS attacks effectively. It addressed the computational overhead issue of IDS systems by selecting the significant features. The proposed method selects an optimal subset that minimizes the dimensionality and enhances the detection accuracy. It was evaluated on the three IDS datasets and reduced more than 50% of the feature space from the datasets. The DenseMLP model showed better performance in terms of accuracy when integrating with the WPBS method compared to other machine learning models, and it was statistically validated by the Wilcoxon signed-rank test. Moreover, the DenseMLP model also showed superior performance to the existing IDS works across the CICIDS2017 and CICDDoS2019 datasets. From these, we are concluding that the WPBS method selected features that can make a generalizable ML model. In addition to this, our model achieved a range of 84% to 100% accuracy for detecting the low-rate and high-rate attacks, whereas it showed a lower accuracy on the CICDDoS2019 dataset. The future work will focus on improving the detection rate of low-rate and high-rate DDoS attacks.

References

1. Ravi, N., S. M. Shalinie, C. Lal, M. Conti. AEGIS: Detection and Mitigation of TCP SYN Flood on SDN Controller. – IEEE Trans Netw Serv Manage, Vol. **18**, 2021, No 1, pp. 745-759, DOI: 10.1109/TNSM.2020.3037124.

2. P a t i l, N. V., C. R. K r i s h n a, K. K u m a r. SSK-DDoS: Distributed Stream Processing Framework Based Classification System for DDoS Attacks. – Cluster Computing, Vol. **25**, 2022, pp. 1355-1372.
3. B o u y e d d o u, B., F. H a r r o u, B. K a d r i, Y. S u n. Detecting Network Cyber-Attacks Using an Integrated Statistical Approach. – Cluster Comput, Vol. **24**, 2021, pp. 1435-1453. DOI: 10.1007/s10586-020-03203-1.
4. A l m e i d a, V., D. D o n e d a, J. A b r e u. Cyberwarfare and Digital Governance. – IEEE Internet Computer Security, Vol. **21**, 2017, No 2, pp. 68-71.
5. B a t c h u, R. K., H. S e e t h a. A Generalized Machine Learning Model for DDoS Attacks Detection Using Hybrid Feature Selection and Hyperparameter Tuning. – Computer Networks, Vol. **200**, 2021, pp. 1-13, 108498. DOI: 10.1016/j.comnet.2021.108498.
6. N a i e m, S., A. E. K h e d r, A. M. I d r e e s, M. I. M a r i e. Enhancing the Efficiency of Gaussian Naïve Bayes Machine Learning Classifier in the Detection of DDOS in Cloud Computing. – In: IEEE Access, Vol. **11**, 2023, pp. 124597-124608. DOI: 10.1109/ACCESS.2023.3328951.
7. M o u s t a f a, N., J. S l a y. UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set). – In: Proc. of Mil. Commun. Inf. Syst. Conf. (MilCIS'15), November 2015, pp. 1-6.
8. F l a d e n m u l l e r, H. A., M. P a r i e n t e, G. P u j o l l e. Intrusion Detection in 5G and Wi-Fi Networks: A Survey of Current Methods, Challenges, and Perspectives. – IEEE Access, Vol. **13**, 2025, pp. 40950-40976. DOI: 10.1109/ACCESS.2025.3546338.
9. L a n s k y, J., S. A l i, M. M o h a m m a d i, M. K. M a j e e d, S. H. T. K a r i m, S. R a s h i d i, M. H o s s e i n z a d e h, A. M. R a h m a n i. Deep Learning-Based Intrusion Detection Systems: A Systematic Review. – In: IEEE Access, Vol. **9**, 2021, pp. 101574-101599. DOI: 10.1109/ACCESS.2021.3097247.
10. K i m, G., S. L e e, S. K i m. A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection. – Expert Systems with Applications, Vol. **41**, 2014, No 4, pp. 1690-1700. DOI: 10.1016/j.eswa.2013.08.066.
11. M o h i u d d i n, A., A. N. M a h m o o d, J. H u. A Survey of Network Anomaly Detection Techniques. – Journal of Network and Computer Applications, Vol. **60**, 2016, pp. 19-31, DOI: 10.1016/j.jnca.2015.11.016.
12. S h o n e, N., T. N. N g o c, V. D. P h a i, Q. S h i. A Deep Learning Approach to Network Intrusion Detection. – In: IEEE Transactions on Emerging Topics in Computational Intelligence,
Vol. **2**, February 2018, No 1, pp. 41-50. DOI: 10.1109/TETCI.2017.2772792.
13. J a v a i d, A., Q. N i y a z, W. S u n, M. A l a m. A Deep Learning Approach for Network Intrusion Detection System. – In: Proc. of EAI International Conference on Bio-Inspired Information and Communications Technologies (BICT'16), 2016.
14. Z a r p e l ã o, B. B., R. S. M i a n i, C. T. K a w a k a n i, S. C. de A l v a r e n g a. A Survey of Intrusion Detection in Internet of Things. – J. Netw. Comput. Appl., Vol. **84**, 2017, pp. 25-37.
15. Y i n, C., Y. Z h u, J. F e i, X. H e. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. – In: IEEE Access, Vol. **5**, 2017, pp. 21954-21961. DOI: 10.1109/ACCESS.2017.2762418.
16. Z h a n g, J., M. Z u l k e r n i n e. A Deep Neural Network-Based Intrusion Detection System for Internet of Things. – IEEE Trans Ind Inform, Vol. **14**, 2018, No 7, pp. 3189-3198.
17. L i, Y., Z. T i a n. Lightweight Anomaly Detection for Industrial Control Systems Based on Deep Learning. – IEEE Trans Ind Inform, Vol. **16**, 2020, No 10, pp. 6692-6701.
18. K h a m m a s s i, C., S. K r i c h e n. A ga-lr Wrapper Approach for Feature Selection in Network Intrusion Detection. – Computer Security, Vol. **70**, 2017, pp. 255-277. DOI: 10.1016/j.cose.2017.06.005.
19. S a l o, F., A. B. N a s s i f, A. E s s e x. Dimensionality Reduction with IG-PCA and Ensemble Classifier for Network Intrusion Detection. – Computer Networks, Vol. **148**, 2019, pp. 164-175.

20. S a y e d, M. S. E., N. -A. L e-K h a c, M. A. A z e r, A. D. J u r c u t. A Flow-Based Anomaly Detection Approach with Feature Selection Method Against DDoS Attacks in SDNs. – In: IEEE Transactions on Cognitive Communications and Networking, Vol. **8**, December 2022, No 4, pp. 1862-1880. DOI: 10.1109/TCCN.2022.3186331.
21. B h u y a n, M. H., A. K a l w a r, A. G o s w a m i, D. K. B h a t t a c h a r y y a, J. K. K a l i t a. Low-Rate and High-Rate Distributed DoS Attack Detection Using Partial Rank Correlation. – In: Proc. of 5th International Conference on Communication Systems and Network Technologies, Gwalior, India, 2015, pp. 706-710. DOI: 10.1109/CSNT.2015.24.
22. P é r e z-D í a z, J. A., I. A. V a l d o v i n o s, K.-K. R. C h o o, D. Z h u. A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning. – IEEE Access Vol. **8**, 2020, pp. 155859-155872. DOI: 10.1109/ACCESS.2020.3019330.
23. F a t a n i, A., A. D a h o u, M. A. A. A l-Q a n e s s, S. L u, M. A b d E l a z i z. Advanced Feature Extraction and Selection Approach Using Deep Learning and Aquila Optimizer for IoT Intrusion Detection System. – Sensors, Vol. **22**, 2022, 140. DOI: 10.3390/s22010140.
24. T a v a l l a e e, M., E. B a g h e r i, W. L u, A. A. G h o r b a n i. A Detailed Analysis of the KDD CUP 99 Data Set. – In: Proc. of IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA'09), 2009, pp. 1-6.
25. M o u s t a f a, N., B. T u r n b u l l, K. -K. R. C h o o. An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things. – IEEE Internet of Things Journal, Vol. **6**, June 2019, No 3, pp. 4815-4830. DOI: 10.1109/JIOT.2018.2871719.
26. A y a d, A. G., A. S. N e h a l, N. A. H i k a l. Hybrid Approach for Efficient Feature Selection in Anomaly Intrusion Detection for IoT Networks. – The Journal of Supercomputing, Vol. **80**, 2024, pp. 6942-26984. DOI: 10.1007/s11227-024-06409-x.
27. Z a i n u d i n, A., L. A. C. A h a k o n y e, R. A k t e r, D. S. K i m, J. M. L e e. An Efficient Hybrid-DNN for DDoS Detection and Classification in Software-Defined IIoT Networks. – IEEE Internet of Things Journal, Vol. **10**, 2023, No 10, pp. 8491-8504.
28. H a l l a d a y, J., D. C u l l e n, N. B r i n e r, J. W a r r e n, K. F y e, R. B a s n e t, J. B e r g e n, T. D o l e c k. Detection and Characterization of DDoS Attacks Using Time-Based Features. – IEEE Access, Vol. **10**, 2022, pp. 49794-49807. DOI: 10.1109/ACCESS.2022.3173319.
29. D o n g, S., M. S a r e m. DDoS Attack Detection Method Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks. – IEEE Access, Vol. **8**, 2020, pp. 5039-5048. DOI: 10.1109/ACCESS.2019.2963077.
30. G a u r, V., R. K u m a r. Analysis of Machine Learning Classifiers for Early Detection of DDoS Attacks on IoT Devices. – Arabian Journal for Science and Engineering, Vol. **47**, 2022, No 2, pp. 1353-1374.
31. H i r s i, A., L. A u d a h, A. S a l h, M. A. A l h a r t o m i, S. A h m e d. Detecting DDoS Threats Using Supervised Machine Learning for Traffic Classification in Software Defined Networking. – In: IEEE Access, Vol. **12**, 2024, pp. 166675-166702. DOI: 10.1109/ACCESS.2024.3486034.
32. J a n s i R a n i, S. V., et al. Detection of DDoS Attacks in D2D Communications Using Machine Learning Approach. – Computer Communications, Vol. **198**, 2023, pp. 32-51. DOI: 10.1016/j.comcom.2022.11.013.
33. K u m a r i, P., A. K u m a r J a i n. Timely Detection of DDoS Attacks in IoT with Dimensionality Reduction. – Cluster Computing, Vol. **27**, 2024, pp. 7869-7887. DOI: 10.1007/s10586-024-04392-9.
34. A s h i k u l, L., C. D a g l i. Network Intrusion Detection System Using Deep Learning. – In: Procedia Computer Science, Vol. **185**, 2021, pp. 239-247.
35. D h a n a b a l, L., S. K. S h a n t h a r a j a h. A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms. – International Journal of Advanced Research Comput. Sci. Software Eng., Vol. **5**, 2015, No 1, pp. 801-805.
36. L o p e z-M a r t i n, M., B. C a r r o, A. S a n c h e z-E s g u e v i l l a s, J. L l o r e t. Network Intrusion Detection System Using Recurrent Neural Networks. – IEEE Access, Vol. **5**, 2017, pp. 18042-18050.

37. Lansky, J., S. Ali, M. Mohammadi, M. K. Majeed, S. H.T. Karim, S. Rashidi, M. Hosseinzadeh, A. M. Rahmani. Deep Learning-Based Intrusion Detection Systems: A Systematic Review. – IEEE Access, Vol. **9**, 2021, pp. 101574-101599. DOI: 10.1109/ACCESS.2021.3097247.
38. Javaid, A., W. Sun, Q. Niyaz, M. Alam, J. Qadir. Deep Learning-Based Network Intrusion Detection System for CICDDoS2019 Dataset. – IEEE Access, Vol. **8**, 2020, pp. 174198-174209.
39. Alghoson, E. S., O. Abbass. Detecting Distributed Denial of Service Attacks Using Machine Learning Models. – International Journal of Advanced Computer Science and Applications, Vol. **12**, 2021, pp. 616-622.
40. Haider, S., A. Akhunzada, I. Mustafa, T. B. Patel, A. Fernandez, K. K. R. Choo, J. Iqbal. A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks. – IEEE Access, Vol. **8**, 2020, pp. 53972-53983. DOI: 10.1109/ACCESS.2020.2976908.
41. Elubeyd, H., D. Yiltas-Kaplan. Hybrid Deep Learning Approach for Automatic DoS/DDoS Attacks Detection in Software-Defined Networks. – Applied Sciences, Vol. **13**, 2023, No 6, 3828. DOI: 10.3390/app13063828.
42. Elsayed, M. S., N. -A. Le-Khac, S. Dev, A. D. Jurcut. DDoSNet: A Deep-Learning Model for Detecting Network Attacks. – In: Proc. of 21st IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'20), Cork, Ireland, 2020, pp. 391-396, DOI: 10.1109/WoWMoM49955.2020.00072.
43. Sharafaldin, I., A. H. Lashkari, S. Hakak, A. A. Ghorbani. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. – In: Proc. of International Carnahan Conference on Security Technology (ICCST'19), Chennai, India, 2019, pp. 1-8. DOI: 10.1109/CCST.2019.8888419.
44. Bakro, M., R. R. Kumar, M. Husain, Z. Ashraf, A. Ali, S. I. Yaqoob, M. N. Ahmed, N. Parveen. Building a Cloud-IDS by Hybrid Bio-Inspired Feature Selection Algorithms Along with Random Forest Model. – IEEE Access, Vol. **12**, 2024, pp. 8846-8874. DOI: 10.1109/ACCESS.2024.3353055.
45. Aktar, S., A. Y. Nur. Towards DDoS Attack Detection Using Deep Learning Approach. – Computers and Security, Vol. **129**, 2023, 103251.
46. Chanu, U. S., K. J. Singh, Y. J. Chanu. A Dynamic Feature Selection Technique to Detect DDoS Attack. – Journal of Information Security and Applications, Vol. **74**, 2023, pp. 1-10, 103445. DOI: 10.1016/j.jisa.2023.103445.
47. Sindian, S., S. Samer. An Enhanced Deep Autoencoder-Based Approach for DDoS Attack Detection. – Wseas Transactions on Systems Control, Vol. **15**, 2020, pp. 716-725.
48. Lopes, I. O., D. Zou, F. A. Ruambo, S. Akbar, B. Yuan. Towards Effective Detection of Recent DDoS Attacks: A Deep Learning Approach. – Security and Communication Networks, Vol. **2021**, 2021, pp. 1-14. DOI: 10.1155/2021/5710028.
49. Thakkar, A., R. Lohiya. Fusion of Statistical Importance for Feature Selection in Deep Neural Network-Based Intrusion Detection System. – Inf. Fusion, Vol. **90**, 2023, pp. 353-363. DOI: 10.1016/j.inffus.2022.09.026.
50. Pandey, N., P. K. Mishra. Devising a Hybrid Approach for Near Real-Time DDoS Detection in IoT. – Journal of Computers and Electrical Engineering, Vol. **118**, 2024, pp. 1-20, 109448.
51. Hnamte, V., J. Hussain. Dependable Intrusion Detection System Using Deep Convolutional Neural Network: A Novel Framework and Performance Evaluation Approach. – Telematics and Informatics Reports, Vol. **11**, 2023, 100077. DOI: 10.1016/j.teler.2023.100077.
52. Manthena, Raghupathi, Radhakrishna, Vangipuram. Integrating Machine Learning and T-Tests to Optimize Distributed Denial of Service Attacks Detection. – International Journal of Intelligent Engineering and Systems, Vol. **17**, 2024, No 6, pp. 1023-1043. DOI: 10.22266/ijies2024.1231.76.
53. Hussain, S., et al. An Adaptive Intrusion Detection System for WSN Using Reinforcement Learning and Deep Classification. – Arabian Journal for Science and Engineering, Vol. **50**, 2025, pp. 12463-12477.

54. C u r t i s, D. Welch's t-Test is More Sensitive to Real-World Violations of Distributional Assumptions than Student's t-Test, but Logistic Regression is More Robust than Either. – Stat Papers, Vol. **65**, 2024, pp. 3981-3989. DOI: 10.1007/s00362-024-01531-7.
55. A r c h i b a l d, R., D. G h o s a l. A Comparative Analysis of Detection Metrics for Covert Timing Channels. – Computers & Security, Vol. **45**, 2014, pp. 284-292. DOI: 10.1016/j.cose.2014.03.007Y.
56. A g a l g a o n k a r, P., D. J. H a m m e r s t r o m. Evaluation of Smart Grid Technologies Employed for System Reliability Improvement: Pacific Northwest Smart Grid Demonstration Experience. – In: IEEE Power and Energy Technology Systems Journal, Vol. **4**, June 2017, No 2, pp. 24-31. DOI: 10.1109/JPETS.2017.2683502.
57. G i b o n e y, J. S., J. G. P r o u d f o o t, S. G o e l, J. S. V a l a c i c h. The Security Expertise Assessment Measure (SEAM): Developing a Scale for Hacker Expertise. – Computers & Security, Vol. **60**, 2016, pp. 37-51. DOI: 10.1016/j.cose.2016.04.001.
58. T a t e, R. F. Correlation between a Discrete and a Continuous Variable. Point-Biserial Correlation. – In: Ann. Math. Statist., Vol. **25**, September 1954, pp. 603-607.
59. C h e n, Y., A. D. A t n a f u, I. S c h l a t t n e r, W. T. W e l d t s a d i k, M.-C. R o h, H. J. K i m, S.-W. L e e, B. B l a n k e r t z, S. F a z l i. A High-Security EEG-Based Login System with RSVP Stimuli and Dry Electrodes. – In: IEEE Transactions on Information Forensics and Security, Vol. **11**, December 2016, No 12, pp. 2635-2647. DOI: 10.1109/TIFS.2016.2577551.
60. M a n t h e n a, R a g h u p a t h i, R a d h a k r i s h n a, V a n g i p u r a m. A Research toward Building Reliable and Explainable Machine-Learning Systems for DDoS Attacks Detection. – In: Advances in VLSI, Signal Processing and Wireless Communication, Vol. **1323**, Springer, IEdTC 2023. 2025, pp. 679-695. DOI: 10.1007/978-981-96-1587-2_51.
61. M a n t h e n a, R., R. V a n g i p u r a m. Optimized t-Test Feature Selection for Real-Time Detection of Low and High-Rate DDoS Attacks. – International Journal of Electrical and Computer Engineering Systems, Vol. **16**, 2025, No 7, pp. 517-529.

Received: 02.12.2025, First revision: 09.03.2026, Second revision: 19.03.2026, Accepted: 28.03.2026