Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.052796

ARTICLE

Internet of Things Enabled DDoS Attack Detection Using Pigeon Inspired Optimization Algorithm with Deep Learning Approach

Turki Ali Alghamdi and Saud S. Alotaibi*

Department of Computer Science and Artificial Intelligence, College of Computing, Umm Al-Qura University, Makkah, 21955, Saudi Arabia

*Corresponding Author: Saud S. Alotaibi. Email: ssotaibi@uqu.edu.sa

Received: 15 April 2024 Accepted: 11 July 2024 Published: 12 September 2024

ABSTRACT

Internet of Things (IoTs) provides better solutions in various fields, namely healthcare, smart transportation, home, etc. Recognizing Denial of Service (DoS) outbreaks in IoT platforms is significant in certifying the accessibility and integrity of IoT systems. Deep learning (DL) models outperform in detecting complex, non-linear relationships, allowing them to effectually severe slight deviations from normal IoT activities that may designate a DoS outbreak. The uninterrupted observation and real-time detection actions of DL participate in accurate and rapid detection, permitting proactive reduction events to be executed, hence securing the IoT network's safety and functionality. Subsequently, this study presents pigeon-inspired optimization with a DL-based attack detection and classification (PIODL-ADC) approach in an IoT environment. The PIODL-ADC approach implements a hyperparameter-tuned DL method for Distributed Denial-of-Service (DDoS) attack detection in an IoT platform. Initially, the PIODL-ADC model utilizes Z-score normalization to scale input data into a uniform format. For handling the convolutional and adaptive behaviors of IoT, the PIODL-ADC model employs the pigeon-inspired optimization (PIO) method for feature selection to detect the related features, considerably enhancing the recognition's accuracy. Also, the Elman Recurrent Neural Network (ERNN) model is utilized to recognize and classify DDoS attacks. Moreover, reptile search algorithm (RSA) based hyperparameter tuning is employed to improve the precision and robustness of the ERNN method. A series of investigational validations is made to ensure the accomplishment of the PIODL-ADC method. The experimental outcome exhibited that the PIODL-ADC method shows greater accomplishment when related to existing models, with a maximum accuracy of 99.81%.

KEYWORDS

Internet of things; denial of service; deep learning; reptile search algorithm; feature selection

1 Introduction

Numerous IoT devices linked to the system promptly rise, so network attacks like DoS and flooding grow simultaneously [1]. These assaults cause system disruption and DoS to IoT systems. IoT safety is an intriguing and challenging subject requiring advanced measures to prevent numerous attacks [2]. Due to the significant heterogeneity of IoT, preserving even communication values through manifold systems is problematic. Developing many solutions for each device is a complex process. As

Copyright © 2024 The Authors. Published by Tech Science Press.
This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

an outcome, an intelligent system must adjust to numerous gadgets while professionally defending them from safety threats [3]. Distributed DDoS assaults are chief threats to the system, affecting users and gadgets based on them. DDoS assaults contain manifold plans besides one target, preventing genuine consumers from accessing services like websites and email [4]. They signify the most common and dangerous attack beside and from IoT networks, 5th generation (5G) communication systems, and Cloud Computing (CC).

DDoS attacks are classified into dual chief classes such as high- and low-rate attacks which afford to the dimension of traffic they create [5]. The low-rate attack behavior is really modest because they perform likewise to genuine traffic and account for nearly 10–20 percent of total usual network traffic. If regular traffic of low-rate assaults is small, they theoretically decrease the service quality of the target and stop the service completely [6]. However, many heterogeneous devices organized in an IoT environment make it complex to identify IoT attacks by employing customary rule-based safety solutions. It is a highly challenging task to improve optimum safety techniques for every kind of device [7]. Machine learning (ML) is a substitute method that permits one to improve optimum safety techniques depending on experimental data from every device. DL has a lot of achievements in numerous uses, such as face detection, image processing, and natural language translation [8].

DL can able to extract raw features from data without the need for human participation. It attains a higher performance rate by mechanically identifying associations in raw data [9]. As an outcome of DL-based techniques, the accuracy of classifying attacks has enlarged even more [10]. In addition, temporary network traffic connections frequently offer consecutive data and efficiently train DL techniques with successive traffic, leading to data loss [11]. Some methods related to enlarged cybersecurity include integrating ML models to recognize DDoS assaults over IoT gadgets [12]. ML or DL techniques are crucial for analyzing numerous datasets, mainly IoT, to improve the capability to identify cyberattacks [13]. The restricted resources, like the limited computational capability linked to IoT devices, pose many limitations, so other methodologies should be applied to tackle these limits frequently when needed [14].

This manuscript offers the design of pigeon-inspired pigeon-inspired optimization with DL-based attack detection and classification (PIODL-ADC) technique on an IoT platform. The PIODL-ADC system employs a hyperparameter-tuned DL model for DDoS attack recognition in the IoT atmosphere. Primarily, the PIODL-ADC technique employs Z-score normalization to scale input data into a uniform format. For the feature selection process, the PIODL-ADC technique uses the PIO algorithm. Meanwhile, the Elman Recurrent Neural Network (ERNN) model was applied to detect and identify DDoS attacks. Furthermore, Reptile Search Algorithm (RSA) based hyperparameter tuning is exploited for optimal hyperparameter selection of the ERNN model. A series of experimental analyses are made to ensure the performance of the PIODL-ADC technique.

2 Related Works

In [15], the authors developed an exclusive technique for safeguarding IoT systems using an SDN (Software Defined Network)-enabled structure that integrates an active counter-based technique and DL methods. The main goal is to identify and moderate numerous safety vulnerabilities that attackers use to create DDoS attacks in IoT systems. A developed framework was verified by employing the CICDDoS2019 dataset for detecting exploitation and reflection attacks in User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Internet Control Message Protocol (ICMP). In [16], a new attack recognition technique was developed. Initially, input data pre-processed from the most applicable features are removed. The removed raw landscapes openly assumed long short-term memory (LSTM), and mined higher-order arithmetical features exposed to deep reinforcement learning (DRL) to detect. Next, the average of LSTM and DRL offers identified output in an actual way. The load of LSTM is enhanced by the self-improved battle royale optimization (SIBRO) technique.

Ortet Lopes et al. [17] developed CyDDoS, a combined Intrusion Detection Systems (IDS) structure integrating feature engineering techniques with Deep Neural Networks (DNNs). The ensemble Feature Selection (FS) depends on 5 ML classifiers employed to detect and remove the most relevant features utilized by the analytical method. In [18], a Low-Rate Denial of Service (LDDoS) attack recognition technique has been proposed depending on the DL model that contains an initiation purpose of LSTM by analyzing specific values of dissimilar LDDoS assaults and usual traffic. Ahmim et al. [19] developed a new DL-based IDS consisting of two stages. This hybrid technique integrates DL techniques such as Convolutional Neural Networks (CNNs), Deep Autoencoder, LSTM, and DNN. The primary stage has dissimilar parallel sub-neural systems trained by exact methods. The second stage employs the output of the frozen first stage joined by early data as input.

Sagu et al. [20] developed a hybrid technique for recognizing attacks in an IoT atmosphere with three levels. Primarily, higher-order arithmetical features are removed. Then, recognition takes place by employing Bidirectional Long Short-Term Memory (BLSTM) and Gated Recurrent Unit (GRU) to identify the presence of network assaults. To enhance classification accuracy, loads of BLSTM are optimally set over a self-upgraded Cat and Mouse Optimizer (SU-CMO) method. Ragab et al. [21] develop a Piecewise Harris Hawks Optimization (PHHO) with an Optimal DL Classifier (PHHO-ODLC) model. This method has a staged procedure. At an early stage, the PHHO technique is used to pick pertinent features and improve classification performance. Then, an attention-based bidirectional LSTM (ABiLSTM) system is used for the DDoS attack detection procedure. Lastly, the ABiLSTM network's hyperparameter collection is executed using a grey wolf optimizer (GWO).

In [22], an SDN-enabled DL-driven structure has been developed for threat recognition in an IoT atmosphere. The advanced Cuda-DNN, GRU (Cu-DNNGRU), and Cuda-BLSTM (Cu-BLSTM) classification algorithms are approved for actual threat recognition. The offered model also executed ten-fold cross-validation to display the unbiasedness of outcomes. Aljebreen et al. [23] presented DDoS attack detection using a snake optimizer with ensemble learning (DDAD-SOEL) model. This approach incorporated a snake optimizer for the feature subset section and integration of LSTM, ABiLSTM, and deep belief network (DBN) methods. Also, an Adadelta optimizer is employed for the hyperparameter tuning process. Bella et al. [24] introduced a hybrid correlation-based feature selection-bat optimization algorithm (HCFS-BOA) technique and present a CNN method. This model utilized min-max normalization and CNN classification.

In the field of DDoS recognition in IoT platforms, present models mostly need help with the high heterogeneity and dimensionality of data, paving the way to inefficiency in detecting relevant factors that crucially affect the accuracy of the recognition. Conventional feature selection models may need to sufficiently address IoT data streams' dynamic and convolutional behavior, so further advanced models are required. Metaheuristic techniques are prevalent because of their capacity to navigate substantial search spaces and maximize convolutional issues, improving feature selection outcomes in this background. Moreover, a research gap exists in effectually incorporating these models with hyper-parameter tuning procedures to improve the precision and robustness of recognition methods. Present research considers feature selection and hyperparameter tuning separately, leaving out potential effects that may be attained by mutually maximizing both features. Addressing this gap via an overall model that utilizes metaheuristic techniques for feature selection and concurrent hyperparameter tuning may improve DDoS recognition, safeguarding more productive and dependable safety for IoT platforms. Therefore, the PIODL-ADC technique involves the development of PIO-based feature selection and Resident Space Object (RSO)-based hyperparameter tuning.

3 The Proposed Method

This manuscript proposes the design of the PIODL-ADC technique in an IoT environment. The technique employs a hyperparameter-tuned DL model for DDoS attack recognition in IoT platforms. Fig. 1 represents the entire flow of the PIODL-ADC methodology.

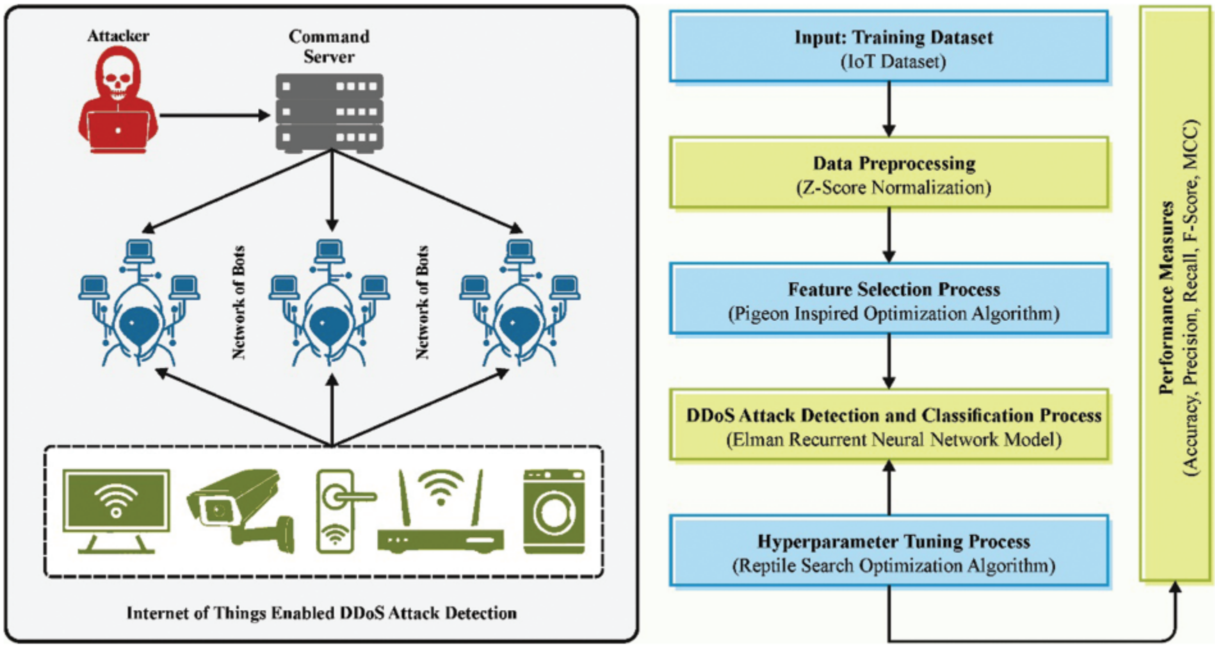

Attacker
Command Server
Network of Bots
Network of Bots
Internet of Things Enabled DDoS Attack Detection
Input: Training Dataset (IoT Dataset)
Data Preprocessing (Z-Score Normalization)
Feature Selection Process (Pigeon Inspired Optimization Algorithm)
DDoS Attack Detection and Classification Process (Elman Recurrent Neural Network Model)
Hyperparameter Tuning Process (Reptile Search Optimization Algorithm)
Performance Measures (Accuracy, Precision, Recall, F-Score, MCC)

Figure 1: Overall flow of PIODL-ADC technique

3.1 Z-Score Normalization

Primarily, the PIODL-ADC technique employs a Z-score normalized to scale the input data into a uniform format. Z-score normalized is a serious pre-processing method in DDoS recognition in IoT environments, allowing standardized representation of different sensor data [25]. This model converts raw sensor values by deducting the mean and dividing by the standard deviation resulting in a distribution with a standard deviation of 1 and a mean of 0. Using Z-score normalization, differences in sensor readings are efficiently normalized, permitting reliable comparison and recognition of unusual patterns indicative of DDoS attacks. In IoT settings, where various devices with dissimilar sensing abilities donate to the data stream, Z-score normalization is essential in safeguarding the features employed for DDoS detection are reliably signified, allowing ML techniques to distinguish abnormal network behavior linked with potential attacks efficiently.

3.2 Feature Selection Process

For the feature selection process, the PIODL-ADC technique uses the Pigeon-Inspired Optimization (PIO) algorithm. The PIO is a biologically inspired Swarm Intelligence (SI) optimization algorithm based on the behaviors of pigeons' flocks [26]. Various amendments are introduced to improve the convergence rate by changing the implementation procedure or the tuning parameters. The study presents a predator-prey PIO (PPPIO) for combined controller design and mission planning. Moreover, Bloch quantum-behaved PIO (BQPIO) is a hybrid model that integrates PIO with a quantum model. Also, PIO is employed to find air robot path planning optimization problems and is adapted by incorporating control parameterization and time discretization (CPTD) methods to deal with the issue of Unmanned Aerial Vehicle (UAV) formation.

PIO is prolonged in its applicability to other uses such as control of landing systems, gliding trajectory, and Direct Current (DC) motors control spacecraft. The map and compass operator method entirely depends on the earth's and sun's magnetic field, whereby pigeons are used to discover a flock in long travel. For pigeon *i* with speed vector V_i and location vector X_i, its velocity and position in *the* D-dimensional searching range upgraded in all iterations are evaluated as follows:

$$V_i(t) = V_i(t-1) \cdot e^{-Rt} + rand \cdot \left(X_g(t) - X_i(t-1)\right) \tag{1}$$

$$X_i(t) = X_i(t-1) + V_i(t) \tag{2}$$

In Eq. (1), the map and compass factor is R, *rand* denotes a random integer, X_g indicates the existing global optimum location, and X_g is evaluated by comparing locations amongst each pigeon.

The landmark operator model is based on landmarks whereby pigeons use learned landmarks to discover their trajectory and fly toward their nest. This operator signifies that the pigeon is still far from its destination and assumes they are unaware of the landmark. This decreases the pigeon number in every new population by half. Consider $X_c(t)$ as the middle of half of the pigeon's location at *the* r^{th} iteration. Afterwards, each pigeon can fly directly towards *the* X_c's destination.

The location upgrading rule for pigeon *i* at t^{th} iteration is represented below:

$$N_{pl}(t) = \frac{N_p(t-1)}{2} \tag{3}$$

$$x_c = \frac{\sum_{N_{pl}} X_i(t)\, fitness\,(X_i(t))}{\sum_{N_{pl}} fitness\,(X_i(t))} \tag{4}$$

$$X_i(t) = X_i(t-1) + rand.\,(X_c(t) - X_i(t-1)) \tag{5}$$

Fitness $(X_i(t))$ denotes the quality of individual pigeon:

$$fitness\,(X_i(t)) = \begin{cases} \dfrac{1}{f_{\min}(X_i(t)) + \varepsilon} & \textit{for minimization problems} \\ f_{\max}(X_i(t)) & \textit{for maximization problems} \end{cases} \tag{6}$$

For every individual, the optimum location of Nc^{th} iteration is represented by X_p, and $X_p = \min(X_{i1}, X_{i2}, \ldots, X_{iNc})$. The aim of the PIO algorithm must be recognized. These two controllers control the vehicle by multiplying the feedback signal through certain gains. These gains change with time since the missile technique is a time-variant. The PIO is to calculate the optimal value for gains to control missile movement. Fig. 2 exhibits the flowchart of PIO.

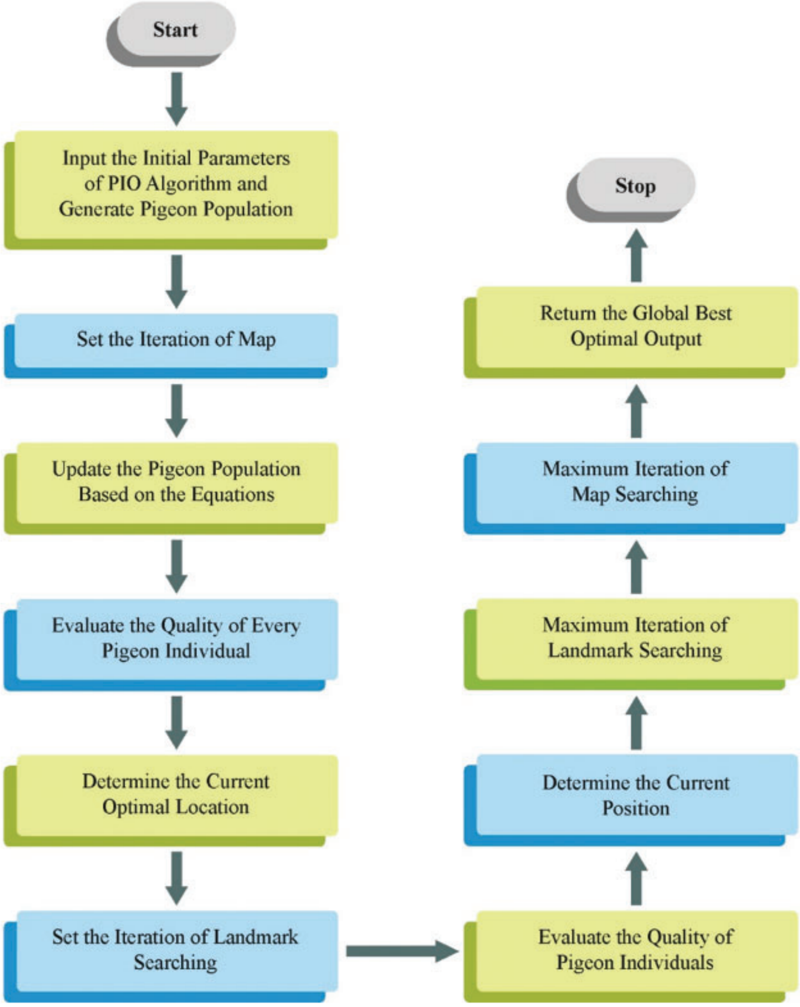

Start
Input the Initial Parameters of PIO Algorithm and Generate Pigeon Population
Set the Iteration of Map
Update the Pigeon Population Based on the Equations
Evaluate the Quality of Every Pigeon Individual
Determine the Current Optimal Location
Set the Iteration of Landmark Searching
Evaluate the Quality of Pigeon Individuals
Determine the Current Position
Maximum Iteration of Landmark Searching
Maximum Iteration of Map Searching
Return the Global Best Optimal Output
Stop

Figure 2: Flowchart of PIO technique

The fitness function (FF) employed in the developed technique is specially designed to balance the number of designated features in every solution (minimum) and classification accuracy (maximum) achieved by utilizing these particular features. Eq. (7) signifies FF to assess solutions.

$$Fitness = \alpha\gamma_R(D) + \beta\frac{|R|}{|C|} \tag{7}$$

whereas $\gamma_R(D)$ denotes the classification error rate of a given classifier. $|R|$ refers to the cardinality of the nominated subset, and $|C|$ indicates the total extent of features in the dataset; α and β mean two parameters corresponding to the impact of classification excellence and subset length, $\in [1,0]$ and $\beta = 1 - \alpha$.

3.3 DDoS Attack Detection Model

At this stage, the ERNN model is applied to recognize and identify to recognize and identify DDoS attacks. ERNNs networks with hidden layer (HL) without innovative devices. ERNN is formally described below:

$$h_t = f\left(W_i x_t + W h_{t-1} + b_h\right) \tag{8}$$

$$y_t = g\left(U h_t + b_o\right) \tag{9}$$

whereas W_i signifies input to HL weights, W denotes the recurrent weight matrix of HL, b_h means hidden bias, U represents HL to outcome weighted matrix and b_o refers to the bias vector for the resultant layer. f and g are corresponding nonlinear functions at HL and output layers. h_t, x_t, y_t relates to state, input and output at time t, individually and h_{t-1} is a state at preceding time instant $t-1$. In this case, it was a regression challenge that the output layer preserved linear (i.e., g means identity function) and rectified linear units (ReLU) utilized in HL.

The parameters of networks enhanced with esteem to mean squared error loss function are mentioned as follows:

$$E = \frac{1}{T}\sum_{t=1}^{T}\left(d_t - y_t\right)^2 \tag{10}$$

T denotes sequence length, and d_t signifies the preferred signal at time t. The limits of the output layer (in Eq. (9)) were learned by employing conventional back-propagation. Other limits of the model (in Eq. (8)) were learned by utilizing back-propagation over time (BPTT). The recursion for calculating the error signal at HL via BPTT is given as follows:

$$e_t = y_t - d_t \tag{11}$$

$$\delta_t = f' * \left(W^T \delta_{t+1} + U^T e_t\right) \tag{12}$$

e_t, δ_t symbolize error signal at time t at the resultant layer and HL, correspondingly. f' means a derivative of the activation function in HL. However, naive execution of BPTT causes a vanishing phenomenon or gradient explosion.

3.4 RSA-Based Hyperparameter Tuning

Eventually, the RSA-based hyperparameter tuning is exploited for optimal hyperparameter selection of the ERNN model. Abualigah et al. first developed RSA in 2021, a special kind of natural-inspired optimization technique. It is a gradient-free technique that can cope with complicated challenges subjected to certain constraints.

The initial phase of the algorithm involves selecting a potential solution randomly using Eq. (13):

$$x_{i,j} = rand \cdot \left(U_b - L_b\right) + L_b;\, i \in (1, \ldots, N) \;\; and\, j \in (1, \ldots, q) \tag{13}$$

Now, the overall population with q features is N. The solution of the i^{th} population having $the\, j^{th}$ feature denotes $x_{i,j}$. The upper and lower boundaries for $the\, j^{th}$ feature are U_b and L_b and "*rand*" is an arbitrarily created value within $[0, 1]$. Based on iteration count, RSA shifts between exploitation (hunting) and exploration (encircling) strategies that correspondingly characterize local and global search techniques.

3.5 Exploration Stage

Crocodile moves within search space via two different strategies: high walking and belly walking. When $t \le \frac{T}{4}$, a high walking search plan is employed and when $t \le \frac{T}{2}$ and $\tau \le \frac{T}{4}$, the belly walking search strategy is utilized, in which t represents constant iteration. The mathematical model of exploration behavior is given in the following:

$$x_{i,j}\left(t+1\right)=\begin{cases}\left[-n_{i,j}\left(t\right)\cdot Best\left(t\right)\cdot\gamma\right]-\left[rand\cdot R_{i,j}\left(t\right)\right], & t\leq\dfrac{T}{4}\\ Es\left(t\right)\cdot x_{\left(i\in[1,N],j\right)}\cdot Best\left(t\right)\cdot rand, & t\leq\dfrac{2T}{4}\ and\ t\geq\dfrac{T}{4}\end{cases}\tag{14}$$

where the hunting operator is $n_{i,j}$, the best solution refers to $Best\left(t\right)$, $\gamma=0.1$, a constant that governs exploration accuracy during iteration. The $\eta_{i,j}(t)$ hunting parameter shown in Eq. (15) is used to retain continuity of exploration and prevent getting trapped in local optima.

The reduced function is $R_{i,j}$(t) shown in Eq. (16), used to restrict the search range. "*rand*" is a randomly generated value, and the evolutionary sense $Es(t)$, shown in Eq. (17), representing the likelihood proportion dropped from 1 to −1 during iteration.

$$\eta_{i,j}\left(t\right)=Best\left(t\right)\times P_{i,j}\tag{15}$$

$$R_{i,j}=\frac{Best(t)-x_{(rand,j)}}{Best(t)+\in}\tag{16}$$

$$Es\left(t\right)=2\times rand_{\in[-1,1]}\times\left(1-\frac{1}{T}\right)\tag{17}$$

where $\in$ denotes a smaller value. $P(i,j)$ difference parameter is given by:

$$P_{i,j}=\sigma+\frac{x_{i,j}-M(x_i)}{Best(t)(U_b-L_b)+\in}\tag{18}$$

In Eq. (19), σ is the sensitivity parameter set as 0.1 and M indicates the mean location:

$$M=\frac{1}{n}\sum_{j-1}^{m}x_{i,j}\tag{19}$$

3.6 Exploitation Stage

The hunting or exploitation stage specifies that crocodiles apply cooperative and coordinated hunting strategies during prey attacks. In the optimization algorithm, this strategy is used to perform a local search and find the potential solution. The coordination hunting is performed according to $t\leq\frac{3T}{4}$ and $t>\frac{2T}{4}$, while the cooperative hunting is performed if $t\leq T$ and $t>\frac{3T}{4}$. The location-updating formula can be represented as follows:

$$x_{i,j}\left(t+1\right)=\begin{cases}Best\left(t\right)\cdot rand_{\in[-1,1]}, P_{i,j}, & t\leq\dfrac{3T}{4}\ and\ t\geq\dfrac{2T}{4}\\ \left[n_{i,j}\left(t\right)\cdot\varepsilon\cdot Best\left(t\right)\right]-\left[R_{i,j}\left(t\right)\cdot rand_{\in[-1,1]}\right], & t\leq T\ and\ t\geq\dfrac{3T}{4}\end{cases}\tag{20}$$

The termination condition is met once t hits the predefined maximum T. The quickness, efficiency, and speed of the local search optimization technique named interior-point procedure was employed to further the performance of RSA's global search.

The RSA model originates an FF to reach an upgraded classifier solution. It defines a positive integer to signify a better solution for candidate outcomes. In this research, the minimization of the classifier error rate is measured as FF, as assumed in Eq. (21).

$$fitness\left(x_i\right) = ClassifierErrorRate\left(x_i\right) = \frac{number\ of\ misclassified\ samples}{Total\ number\ of\ samples} * 100 \tag{21}$$

4 Experimental Validation

This The experimental outcome of the PIODL-ADC technique has been tested using the attack database [27], which comprises 2056 instances and five class labels, as represented in Table 1.

Table 1: Details on database

Classes	No. of instances
DDoS	500
DoS	500
Recon	500
Theft	79
Normal	477
Total instances	**2056**

Fig. 3 illustrates the confusion matrices attained by the PIODL-ADC technique under 80:20 and 70:30 of TRPH/TSPH. The results indicate the effectual detection and classification of all four classes.

The DDoS attack recognition results of the PIODL-ADC approach are reported on 80:20 of TRPH/TSPH, presented in Table 2 and Fig. 4. The attained performances demonstrate that the PIODL-ADC system offers effectual recognition outcomes. On 80% of TRPH, the PIODL-ADC technique offers an average $accu_y$ of 99.39%, $prec_n$ of 97.51%, $reca_l$ of 97.81%, F_{score} of 97.65%, and MCC of 97.27%. Meanwhile, on 20% of TSPH, the PIODL-ADC system gains an average $accu_y$ of 99.81%, $prec_n$ of 99.61%, $reca_l$ of 99.60%, F_{score} of 99.61%, and MCC of 99.48%.

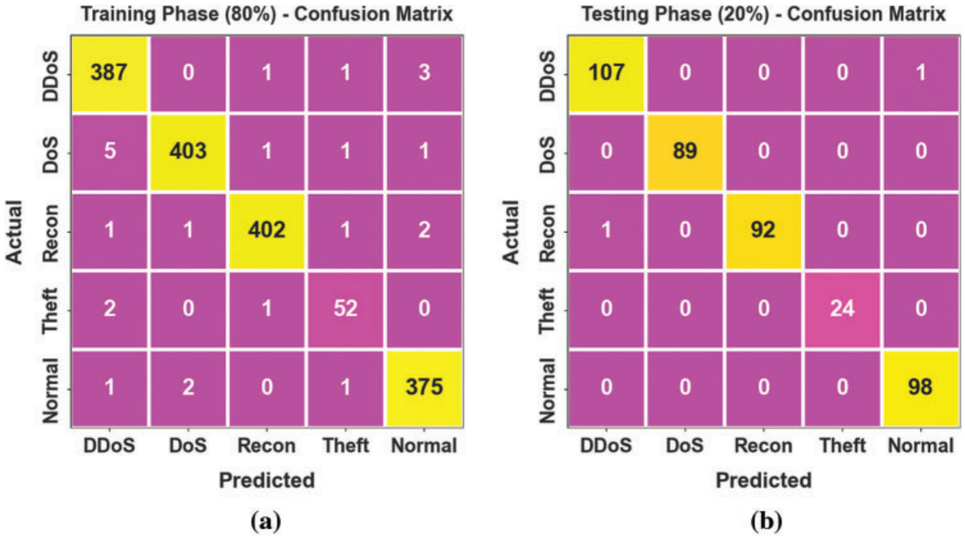
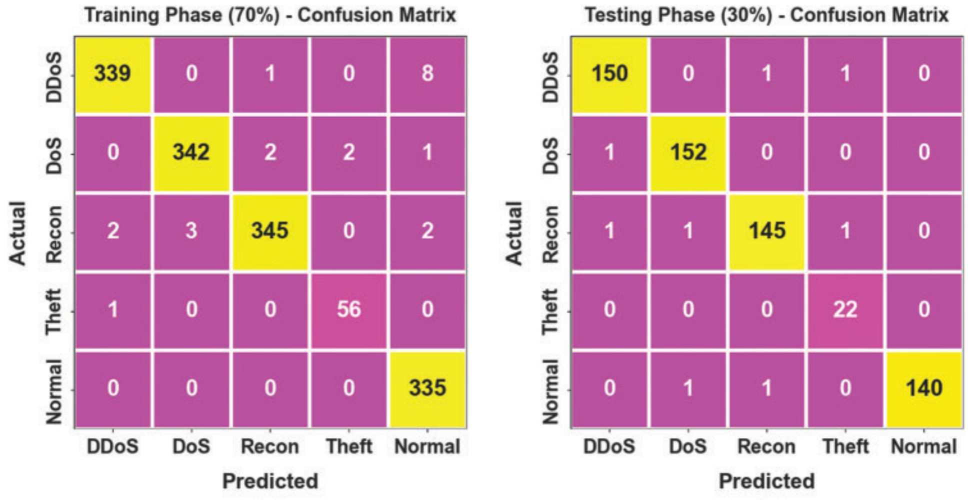


Figure 3: (Continued)



Training Phase (70%) - Confusion Matrix

Actual \ Predicted	DDoS	DoS	Recon	Theft	Normal
DDoS	339	0	1	0	8
DoS	0	342	2	2	1
Recon	2	3	345	0	2
Theft	1	0	0	56	0
Normal	0	0	0	0	335

(c)

Testing Phase (30%) - Confusion Matrix

Actual \ Predicted	DDoS	DoS	Recon	Theft	Normal
DDoS	150	0	1	1	0
DoS	1	152	0	0	0
Recon	1	1	145	1	0
Theft	0	0	0	22	0
Normal	0	1	1	0	140

(d)

Figure 3: Confusion matrices of (a–c) TRPH of 80% and 70% and (b–d) TSPH of 20% and 30%

Table 2: DDoS attack recognition of PIODL-ADC technique on 80:20 of TRPH/TSPH

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	MCC
TRPH (80%)					
DDoS	99.15	97.73	98.72	98.22	97.67
DoS	99.33	99.26	98.05	98.65	98.21
Recon	99.51	99.26	98.77	99.01	98.69
Theft	99.57	92.86	94.55	93.69	93.48
Normal	99.39	98.43	98.94	98.68	98.29
Average	**99.39**	**97.51**	**97.81**	**97.65**	**97.27**
TSPH (20%)					
DDoS	99.51	99.07	99.07	99.07	98.75
DoS	100.00	100.00	100.00	100.00	100.00
Recon	99.76	100.00	98.92	99.46	99.31
Theft	100.00	100.00	100.00	100.00	100.00
Normal	99.76	98.99	100.00	99.49	99.34
Average	**99.81**	**99.61**	**99.60**	**99.61**	**99.48**

The DDoS attack recognition outcome of the PIODL-ADC methodology is defined on 70:30 of TRPH/TSPH and is presented in Table 3 and Fig. 5. The archived outcomes demonstrate that the PIODL-ADC method offers an effectual recognition solution.

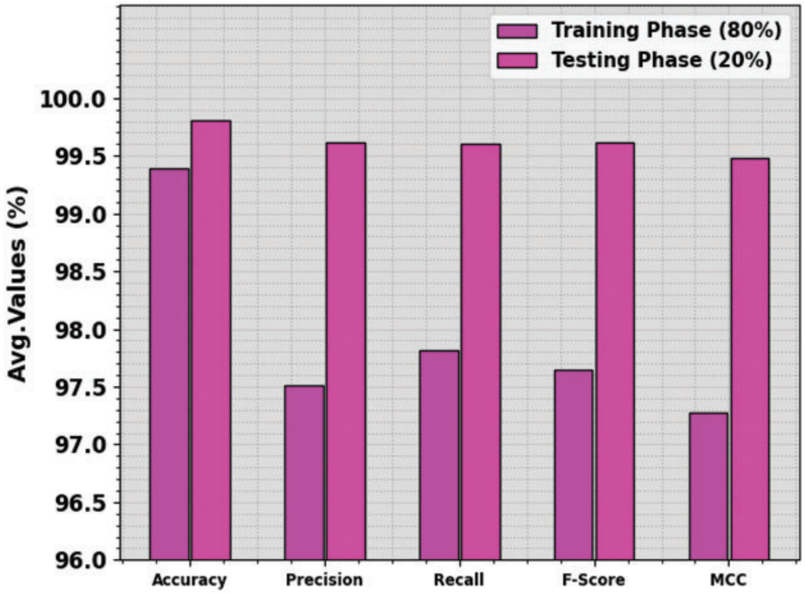


Figure 4: Average of PIODL-ADC technique on 80:20 of TRPH/TSPH

Table 3: DDoS attack recognition outcome of PIODL-ADC technique at 70:30 of TRPH/TSPH

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	MCC
TRPH (70%)					
DDoS	99.17	99.12	97.41	98.26	97.72
DoS	99.44	99.13	98.56	98.84	98.48
Recon	99.31	99.14	98.01	98.57	98.12
Theft	99.79	96.55	98.25	97.39	97.29
Normal	99.24	96.82	100.00	98.38	97.91
Average	**99.39**	**98.15**	**98.45**	**98.29**	**97.90**
TSPH (30%)					
DDoS	99.35	98.68	98.68	98.68	98.25
DoS	99.51	98.70	99.35	99.02	98.70
Recon	99.19	98.64	97.97	98.31	97.77
Theft	99.68	91.67	100.00	95.65	95.58
Normal	99.68	100.00	98.59	99.29	99.08
Average	**99.48**	**97.54**	**98.92**	**98.19**	**97.88**

On 70% of TRPH, the PIODL-ADC approach gains an average $accu_y$ of 99.39%, $prec_n$ of 98.15%, $reca_l$ of 98.45%, F_{score} of 98.29%, and MCC of 97.90%. In the meantime, on 30% of TSPH, the PIODL-ADC method reaches an average $accu_y$ of 99.48%, $prec_n$ of 97.54%, $reca_l$ of 98.92%, F_{score} of 98.19%, and MCC of 97.88%.

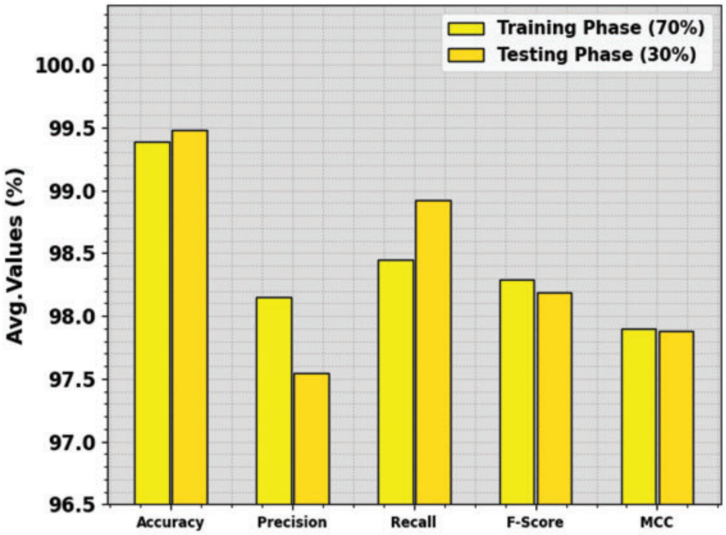


Figure 5: Average of PIODL-ADC technique on 70:30 of TRPH/TSPH

The $accu_y$ curves for training (TR) and validation (VL) exposed in Fig. 6 for the PIODL- Analog-to-Digital Converter (ADC) system on 80:20 of TRPH/TSPH offer valuable insights into its solution under distinct epochs. Primarily, there is a consistent improvement in both TR and TS $accu_y$ with increasing epochs, indicating the model's proficiency in learning and distinguishing designs from TR and TS data. The upward trend in TS $accu_y$ underscores the model's adaptability to the TR dataset and its ability to make correct forecasts on unobserved data, emphasizing robust generalized skills.

Fig. 7 provides a widespread overview of the TR and TS loss outcomes for the PIODL-ADC approach on 80:20 of TRPH/TSPH under distinct epochs. The TR loss consistently decreases as the model refines its weight to minimize classifier errors on both data. The loss curves exemplify the model's arrangement with the TR data, emphasizing its ability to capture patterns effectively in both datasets. Noteworthy is the continuous refinement of parameters in the PIODL-ADC algorithm, aimed at decreasing differences between forecasts and actual TR labels.

Regarding the precision-recall (PR) curve obtainable in Fig. 8, the findings unequivocally support that the PIODL-ADC system on 80:20 of TRPH/TSPH consistently accomplishes improved PR values across all the classes. These outcomes underscore the model's effectual capacity for discriminating among different classes, underscoring its efficacy in accurately identifying class labels.

Furthermore, in Fig. 9, the PIODL-ADC algorithm creates Receiver Operating Characteristic (ROC) outcomes on 80:20 of TRPH/TSPH, demonstrating its proficiency in distinguishing among classes. These curves provide appreciated insights into how the trade-off between True Negative Rate (TPR) and False Positive Rate (FPR) varies under various classifier epochs and thresholds. The results underscore the model's correct classifier performance under various class labels, emphasizing its effectiveness in addressing diverse classification challenges.

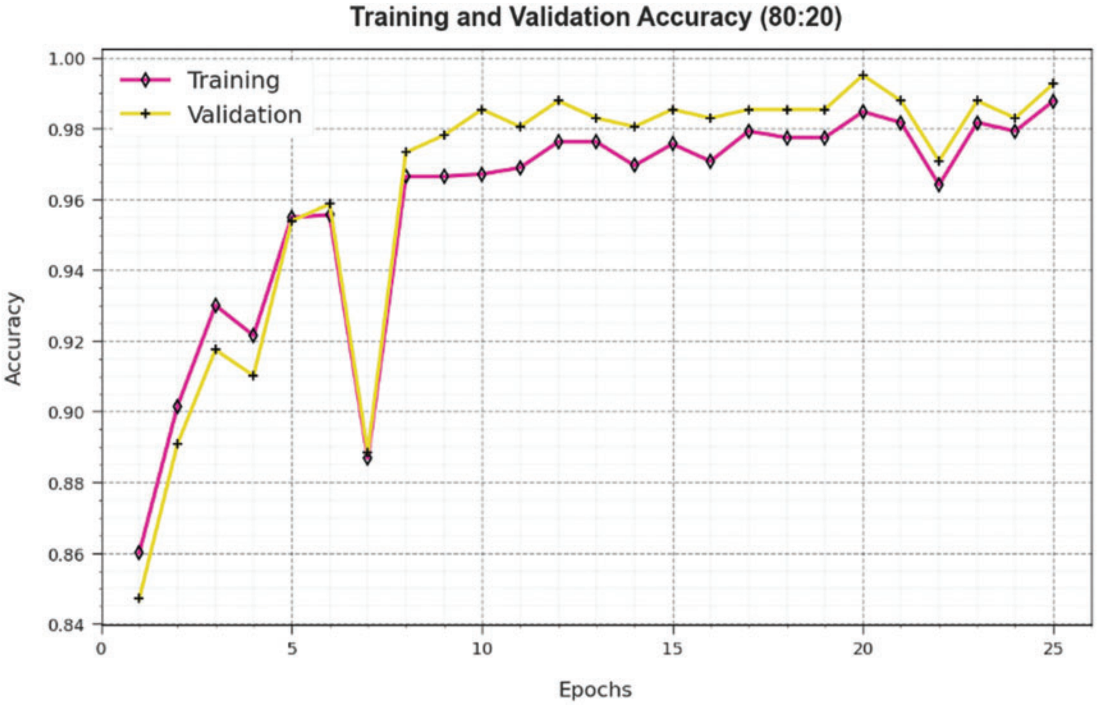


Figure 6: $Accu_y$ curve of PIODL-ADC technique on 80:20 of TRPH/TSPH

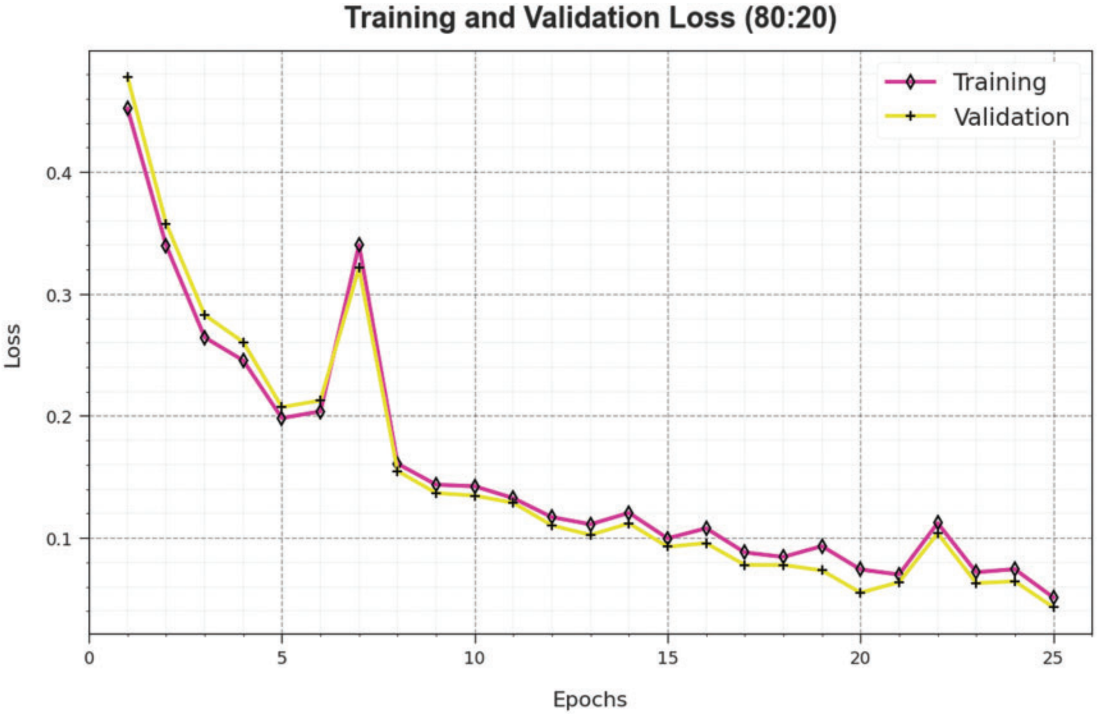


Figure 7: Loss curve of PIODL-ADC system at 80:20 of TRPH/TSPH

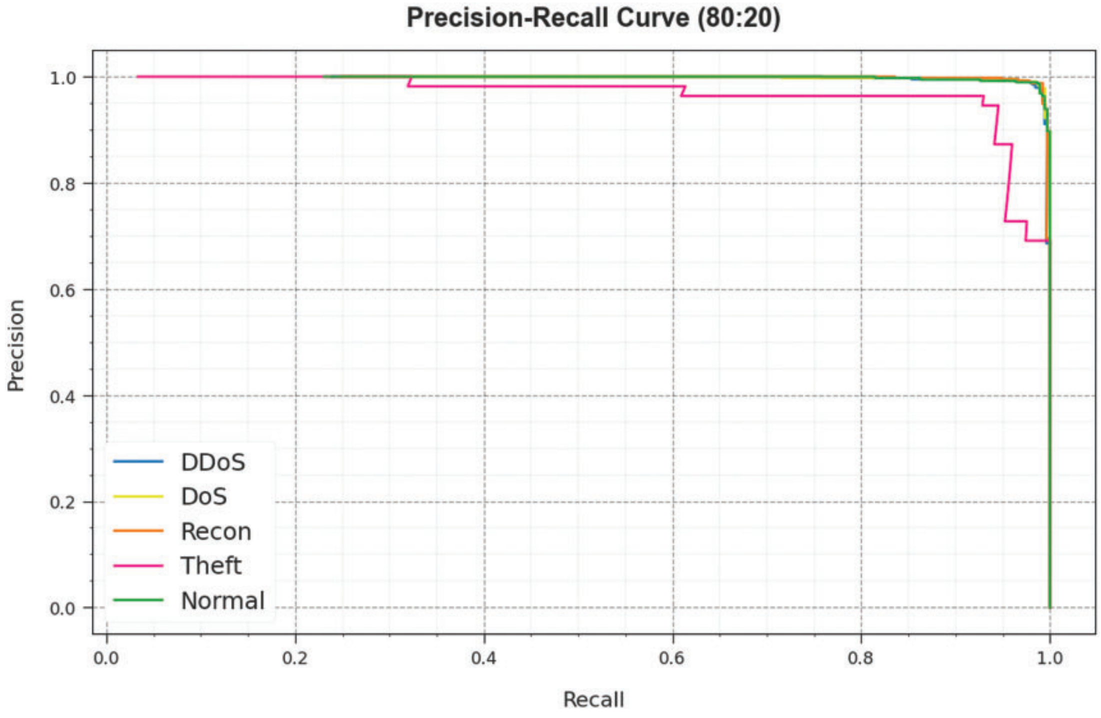


Figure 8: PR curve of PIODL-ADC system at 80:20 of TRPH/TSPH

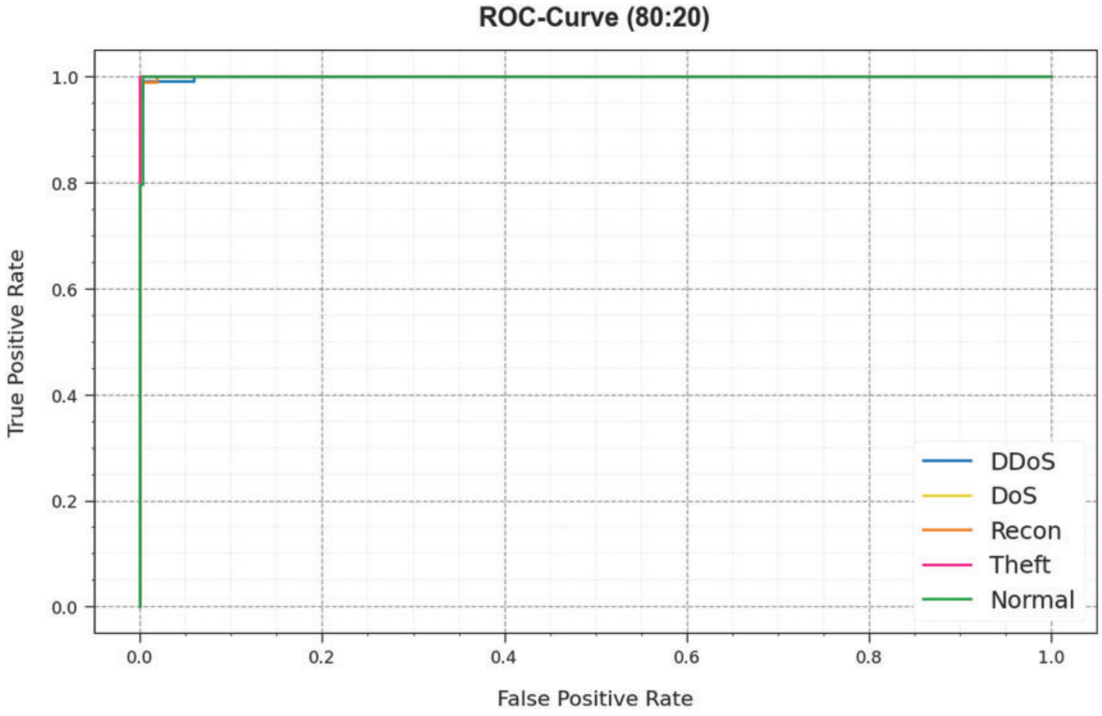


Figure 9: ROC curve of PIODL-ADC technique on 80:20 of TRPH/TSPH

Finally, a detailed comparative analysis of the PIODL-ADC approach with recent systems is provided in Table 4 and Fig. 10 [23]. The results implied a higher solution for the PIODL-ADC method regarding different metrics. Based on $accu_y$, the PIODL-ADC technique reported an improved $accu_y$ of 99.81% whereas the DDAD-SOEL, H3SC-DLIDS, AE-ML, IDS-IOT, XGBoost, and RF approaches reach lesser $accu_y$ values of 99.61%, 98.70%, 97.48%, 96.83%, 96.77%, and 96.12%, respectively. Also, based on $prec_n$, the PIODL-ADC algorithm reported a higher $prec_n$ of 99.61% although the DDAD-SOEL, H3SC-DLIDS, AE-ML, IDS-IOT, XGBoost, and RF system attain lower $prec_n$ values of 99.27%, 96.45%, 95.31%, 95.47%, 993.68%, and 94.40%, correspondingly. At last, based on F_{score}, the PIODL-ADC system reported higher F_{score} of 99.61% but the DDAD-SOEL, H3SC-DLIDS, AE-ML, IDS-IOT, XGBoost, and RF methodologies gain minimal F_{score} values of 99.28%, 95.70%, 94.82%, 95.21%, 94.91%, and 94.16%, correspondingly.

Table 4: Comparative outcome of PIODL-ADC technique with other models

Method	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
PIODL-ADC	99.81	99.61	99.6	99.61
DDAD-SOEL	99.61	99.27	99.27	99.28
H3SC-DLIDS	98.70	96.45	95.23	95.70
AE-ML	97.48	95.31	93.11	94.82
IDS-IOT	96.83	95.47	94.26	95.21
XGBoost	96.77	93.68	91.25	94.91
RF Model	96.12	94.40	93.29	94.16

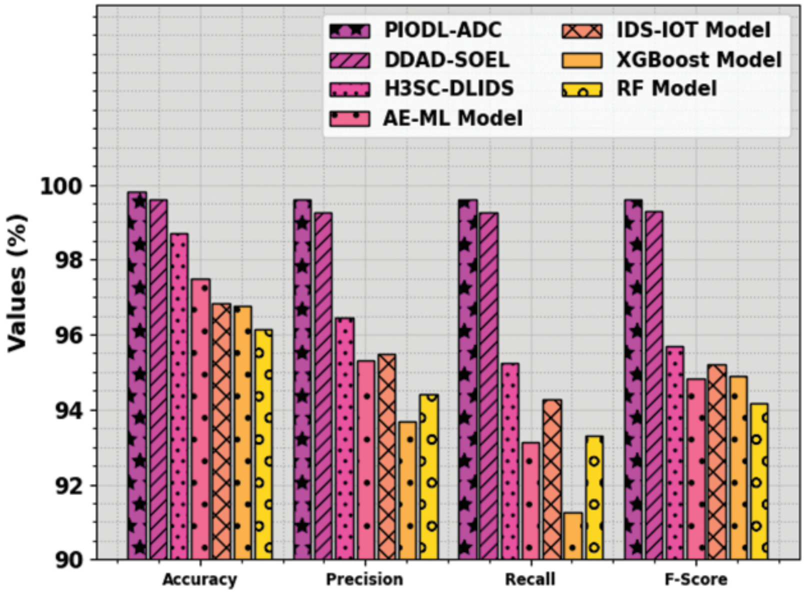


Figure 10: Comparative outcome of PIODL-ADC technique with other approaches

These results guaranteed the superior performance of the PIODL-ADC technique on the DDoS attack recognition process.

5 Conclusion

In this manuscript, the PIODL-ADC technique is proposed in an IoT environment. The PIODL-ADC technique employs a hyperparameter-tuned DL model for DDoS attack recognition in an IoT environment. Primarily, the PIODL-ADC technique employs Z-score normalization to scale the input data into a uniform format. For the feature selection process, the PIODL-ADC technique uses the PIO algorithm. Meanwhile, the ERNN model is applied to identify and detect DDoS attacks. Furthermore, RSA-based hyperparameter tuning is exploited to optimize the hyperparameter selection of the ERNN model. A series of experimental analyses are made to ensure the performance of the PIODL-ADC model. The experimental values stated that PIODL-ADC methodology exhibits better performance when compared to other techniques in different measures.

Acknowledgement: None.

Funding Statement: None.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Turki Ali Alghamdi, Saud S. Alotaibi; data collection: Turki Ali Alghamdi, Saud S. Alotaibi; analysis and interpretation of results: Turki Ali Alghamdi, Saud S. Alotaibi, draft manuscript preparation: Turki Ali Alghamdi, Saud S. Alotaibi. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data sharing does not apply to this article as no datasets were generated during the current study.

Ethics Approval: This study not included human or animal subjects.

Conflict of Interest: The authors declare that they have no conflict of interest to report regarding the present study.

References

[1] A. Alomiri, S. Mishra, and M. AlShehri, "Machine learningbased security mechanism to detect and prevent cyber-attacks in IoT networks," *Int. J. Comput. Digit. Syst.*, vol. 14, no. 1, pp. 645–659, 2023.

[2] K. Sritharan, R. Elagumeeharan, S. Nakkeeran, A. Mohamed, B. Ganegoda and K. Yapa, "Machine learning based distributed denial-of-services attacks detection and mitigation testbed for SDN-enabled IoT devices," in *2022 13th Int. Conf. on Comput. Commun. and Netw. Technol. (ICCCNT)*, Kharagpur, India, IEEE, 2022, pp. 1–6.

[3] R. Zagrouba and R. Alhajri, "Machine learning-based attacks detection and countermeasures in IoT," *Int. J. Commun. Netw. Inform. Secur.*, vol. 13, no. 2, pp. 158– 167, 2021.

[4] A. Seifousadati, S. Ghasemshirazi, and M. Fathian, "A Machine Learning approach for DDoS detection on IoT devices," arXiv preprint arXiv:2110.14911, 2021.

[5] H. Chen, C. Meng, and J. Chen, "DDoS attack simulation and machine learning-based detection approach in the Internet of Things experimental environment," *Int. J. Inf. Secur. Priv.*, vol. 15, no. 3, pp. 1–18, 2021. doi: 10.4018/IJISP.2021070101.

[6] H. Cheng, J. Liu, T. Xu, B. Ren, J. Mao and W. Zhang, "Machine learning-based low-rate DDoS attack detection for SDNenabled IoT networks," *Int. J. Sens. Netw.*, vol. 34, no. 1, pp. 56–69, 2020. doi: 10.1504/IJSNET.2020.109720.

[7] J. G. Almaraz-Rivera, J. A. Perez-Diaz, and J. A. Cantoral-Ceballos, "Transport and application layer DDoS attack detection to IoT devices by using machine learning and deep learning models," *Sensors*, vol. 22, no. 9, pp. 3367, 2022. doi: 10.3390/s22093367.

[8] M. ElKashlan, H. Aslan, and M. A. Azer, "DDoS attack detection in iot using machine learning based intrusion detection system (IDS)," in *2022 18th Int. Comput. Eng. Conf. (ICENCO)*, IEEE, 2022, vol. 1, pp. 19–24. doi: 10.1109/ICENCO55801.2022.10032515.

[9] M. Anwer, S. M. Khan, and M. U. Farooq, "Attack detection in IoT using machine learning," *Eng. Technol. Appl. Sci. Res.*, vol. 11, no. 3, pp. 7273–7278, 2021. doi: 10.48084/etasr.4202.

[10] K. Wehbi, "Machine learning based practical and efficient DDoS attacks detection system for IoT," Doctoral dissertation, Tennessee State Univ., USA, 2022.

[11] A. Prashanthi and R. R. Reddy, "Enhancing cyber security frameworks: Integrating pigeon-inspired optimization and dense neural networks for advanced intrusion detection using the CIC-IDS-2017 dataset," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 11, pp. 220–233, 2024.

[12] M. Abd Elaziz, M. A. Al-qaness, A. Dahou, R. A. Ibrahim, and A. A. Abd El-Latif, "Intrusion detection approach for cloud and IoT environments using deep learning and Capuchin Search Algorithm," *Adv. Eng. Softw.*, vol. 176, no. 5, pp. 103402, 2023. doi: 10.1016/j.advengsoft.2022.103402.

[13] C. Kumar and M. S. A. Ansari, "An explainable nature-inspired cyber attack detection system in Software-Defined IoT applications," *Expert. Syst. Appl.*, vol. 250, no. 4, pp. 123853, 2024. doi: 10.1016/j.eswa.2024.123853.

[14] H. Asgharzadeh, A. Ghaffari, M. Masdari, and F. S. Gharehchopogh, "Anomaly-based intrusion detection system in the Internet of Things using a convolutional neural network and multi-objective enhanced Capuchin Search Algorithm," *J. Parallel Distr. Comput.*, vol. 175, no. 5, pp. 1–21, 2023. doi: 10.1016/j.jpdc.2022.12.009.

[15] M. Cherian and S. L. Varma, "Secure SDN-IoT framework for DDoS attack detection using deep learning and counter based approach," *J. Netw. Syst. Manage.*, vol. 31, no. 3, pp. 54, 2023. doi: 10.1007/s10922-023-09749-w.

[16] H. Rekha and M. Siddappa, "Hybrid deep learning model for attack detection in internet of things," *Serv. Oriented Comput. Appl.*, vol. 16, no. 4, pp. 293–312, 2022. doi: 10.1007/s11761-022-00342-8.

[17] L. Ortet Lopes, D. Zou, F. A. Ruambo, S. Akbar, and B. Yuan, "Towards effective detection of recent DDoS attacks: A deep learning approach," *Secur. Commun. Netw.*, vol. 2021, pp. 1–14, 2021.

[18] A. A. Alashhab, M. S. M. Zahid, A. Muneer, and M. Abdullahi, "Low-rate DDoS attack detection using deep learning for SDN-enabled IoT Networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 11, pp. 371–377, 2022. doi: 10.14569/issn.2156-5570.

[19] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. B. Dhaou, "Distributed denial of service attack detection for the Internet of Things using hybrid deep learning model," *IEEE Access*, vol. 11, pp. 119862–119875, 2023. doi: 10.1109/ACCESS.2023.3327620.

[20] A. Sagu, N. S. Gill, P. Gulia, J. M. Chatterjee, and I. Priyadarshini, "A hybrid deep learning model with self-improved optimization algorithm for detection of security attacks in IoT environment," *Future Internet*, vol. 14, no. 10, pp. 301, 2022. doi: 10.3390/fi14100301.

[21] M. Ragab, S. Alshammari, L. A. Maghrabi, D. Alsalman, T. Althaqafi and A. A. M. AL-Ghamdi, "Robust DDoS attack detection using piecewise Harris Hawks optimizer with deep learning for a secure internet of things environment," *Mathematics*, vol. 11, no. 21, pp. 4448, 2023. doi: 10.3390/math11214448.

[22] D. Javeed, T. Gao, M. T. Khan, and I. Ahmad, "A hybrid deep learning-driven SDN enabled mechanism for secure communication in Internet of Things (IoT)," *Sensors*, vol. 21, no. 14, pp. 4884, 2021. doi: 10.3390/s21144884.

[23] M. Aljebreen, H. A. Mengash, M. A. Arasi, S. S. Aljameel, A. Salama and M. A. Hamza, "Enhancing DDoS attack detection using snake optimizer with ensemble learning on internet of things environment," *IEEE Access*, vol. 11, pp. 104745, 2023. doi: 10.1109/ACCESS.2023.3318316.

[24] H. K. Bella and S. Vasundra, "Healthcare intrusion detection using hybrid correlation-based feature selection-bat optimization algorithm with convolutional neural network: A hybrid correlation-based feature selection for intrusion detection systems," *Int. J. Adv. Comput. Sci. & Appl.*, vol. 15, no. 1, pp. 671–697, 2024.

[25] T. Rathod *et al.*, "AI and blockchain-based secure data dissemination architecture for iot-enabled critical infrastructure," *Sensors*, vol. 23, no. 21, pp. 8928, 2023. doi: 10.3390/s23218928.

[26] M. Saad and M. A. H. Abozied, "Nonlinear system control analysis and optimization using advanced Pigeon-Inspired optimization algorithm," *J. King Saud Univ.-Eng. Sci.*, vol. 36, no. 1, pp. 45–56, 2022. doi: 10.1016/j.jksues.2022.11.001.

[27] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset," *Future Gener. Comput. Syst.*, vol. 100, no. 7, pp. 779–796, 2019. doi: 10.1016/j.future.2019.05.041.