mathematics

MDPI

Article

Robust DDoS Attack Detection Using Piecewise Harris Hawks Optimizer with Deep Learning for a Secure Internet of Things Environment

Mahmoud Ragab [1,*], Sultanah M. Alshammari [2,3], Louai A. Maghrabi [4], Dheyaaldin Alsalman [5], Turki Althaqafi [6] and Abdullah AL-Malaise AL-Ghamdi [6,7]

[1] Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[2] Center of Excellence in Smart Environment Research, King Abdulaziz University, Jeddah 21589, Saudi Arabia; sshammari@kau.edu.sa
[3] Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[4] Department of Software Engineering, College of Engineering, University of Business and Technology, Jeddah, Saudi Arabia; l.maghrabi@ubt.edu.sa
[5] Department of Cybersecurity, School of Engineering, Computing and Design, Dar Al-Hekma University, Jeddah 22246, Saudi Arabia; dsalman@dah.edu.sa
[6] Information Systems Department, School of Engineering, Computing and Design, Dar Al-Hekma University, Jeddah 22246, Saudi Arabia; tthaqafi@dah.edu.sa (T.A.); aalmalaise@kau.edu.sa (A.A.-M.A.-G.)
[7] Information Systems Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
* Correspondence: mragab@kau.edu.sa

Abstract: The Internet of Things (IoT) refers to the network of interconnected physical devices that are embedded with software, sensors, etc., allowing them to exchange and collect information. Although IoT devices have several advantages and can improve people's efficacy, they also pose a security risk. The malicious actor frequently attempts to find a new way to utilize and exploit specific resources, and an IoT device is an ideal candidate for such exploitation owing to the massive number of active devices. Especially, Distributed Denial of Service (DDoS) attacks include the exploitation of a considerable number of devices like IoT devices, which act as bots and transfer fraudulent requests to the services, thereby obstructing them. There needs to be a robust system of detection based on satisfactory methods for detecting and identifying whether these attacks have occurred or not in a network. The most widely used technique for these purposes is artificial intelligence (AI), which includes the usage of Deep Learning (DL) and Machine Learning (ML) to find cyberattacks. The study presents a Piecewise Harris Hawks Optimizer with an Optimal Deep Learning Classifier (PHHO-ODLC) for a secure IoT environment. The fundamental goal of the PHHO-ODLC algorithm is to detect the existence of DDoS attacks in the IoT platform. The PHHO-ODLC method follows a three-stage process. At the initial stage, the PHHO algorithm can be employed to choose relevant features and thereby enhance the classification performance. Next, an attention-based bidirectional long short-term memory (ABiLSTM) network can be applied to the DDoS attack classification process. Finally, the hyperparameter selection of the ABiLSTM network is carried out by the use of a grey wolf optimizer (GWO). A widespread simulation analysis was performed to exhibit the improved detection accuracy of the PHHO-ODLC technique. The extensive outcomes demonstrated the significance of the PHHO-ODLC technique regarding the DDoS attack detection technique in the IoT platform.

Keywords: cybersecurity; DDoS attacks; network security; Internet of Things; artificial intelligence; metaheuristics

MSC: 68T35

check for updates

Citation: Ragab, M.; M. Alshammari, S.; Maghrabi, L.A.; Alsalman, D.; Althaqafi, T.; AL-Ghamdi, A.A.-M. Robust DDoS Attack Detection Using Piecewise Harris Hawks Optimizer with Deep Learning for a Secure Internet of Things Environment. *Mathematics* **2023**, *11*, 4448. https://doi.org/10.3390/math11214448

Academic Editor: Faheim Sufi

Received: 24 September 2023
Revised: 21 October 2023
Accepted: 25 October 2023
Published: 27 October 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The Internet of Things (IoT) is an emerging network of physical things which are connected to the internet [1]. With the help of accessible digital data, it assists in the conversion of internet-connected devices from any position and at any time into a connected ecosystem. The physical gadgets which range in size from compact to tremendous equipment interrelate among them without human interference via the internet [2]. Various supporting technologies are available, which include cloud computing, radio frequency identification and wireless sensor networks that have developed as important components of the IoT paradigm's growth [3]. It has been utilized in many applications like healthcare, personal wearable devices and environmental monitoring to improve the variety, veracity, volume and velocity of information. For example, sensitive data like personal information are managed by the connected system and these devices. Therefore, from manufacturing as well as academia, there has been improved attention to increasing security solutions for IoT devices [4]. Distributed Denial of Service (DDoS) threats are mainly developed to prevent genuine clients from accessing a real service or website. The intended website or service is attacked with requests which come from numerous sources and make it inaccessible to legitimate consumers [5].

In numerous ways, the attack can be produced by fake traffic and pingback. These kinds of attacks are more efficient when the server host of the target webpage is insufficient to handle the expected traffic [6]. Owing to the capability of the present servers to control massive amounts of traffic, an attack performed from a single origin is not feasible. So due to evaluation and growth, DDoS attacks have remained a foremost attack throughout the years [7]. To determine DDoS/DoS threats in IoT networks, classical IDS makes use of effective techniques like machine learning (ML), statistical anomaly and signature-based detection [8]. Moreover, the recognition of DDoS or DoS attacks in IoT systems poses a major problem for classical Intrusion-Detection Systems (IDS). These types of networks usually use methods like signature-based, ML-based and statistical anomaly [9]. The unique features of IoT networks include the huge number of interconnected devices, heterogeneous traffic patterns and varied communication protocols which contribute to the difficulty of threading malicious actions.

The traditional IDS techniques are mainly developed for conventional networks and fight to manage the unpredictable as well as dynamic nature of IoT surroundings [10]. The conventional methods are not more efficient in handling the progressive threats [11]. Advanced deep learning (DL) methods have been developed for abnormal behavior identification (ABN) and automatic intrusion detection (AID). Recently, ML and DL methods have been specially designed and applied for ABN and AID in networks and for their prevention [12].

This study presents a Piecewise Harris Hawks Optimizer with an Optimal Deep Learning Classifier (PHHO-ODLC) for a secure IoT environment. The fundamental goal of the PHHO-ODLC technique is to detect the existence of DDoS attacks in the IoT platform. The PHHO-ODLC technique follows a three-stage process. At the initial stage, the PHHO algorithm can be employed to choose relevant features and thereby enhance the classification performance. Next, the attention-based bi-directional long short-term memory (ABiLSTM) model can be applied to the DDoS attack classification process. Finally, the hyperparameter selection of the ABiLSTM network is implemented by the use of a grey wolf optimizer (GWO). A widespread simulation analysis was performed to show the improved detection accuracy of the PHHO-ODLC technique.

2. Literature Survey

Sharifian et al. [13] designed a Binary Improved African Vulture Optimization Algorithm (Sin-Cos BIAVOA) method. This technique utilizes a new Compound Transfer method (Sin-Cos) to improve the exploration. The Gravitational-Fixed Radius NN (GFRNN) is used as a classification algorithm to choose the optimum feature set in this technique. Dora and Laskhmi [14] proposed a DDoS classification technique by incorporating opti-

mized LSTM and CNN, which is referred to as CNN-O-LSTM. The optimal features can be chosen by the Closest Position-Based GWO (CP-GWO) method. The CNN technique is mainly designed to learn features. Lastly, optimized LSTM is utilized for the detection part, and it is investigated on standard datasets. In [15], a new DL technique was introduced. The research presented the CNN technique, which established an effective feature fusion mechanism. Moreover, a symmetric logarithmic loss method is also designed based on the categorical cross-entropy. Additionally, the designed detection structure has been implemented in the GPU-enabled TensorFlow and estimated by utilizing the NSL-KDD datasets.

Matsa et al. [16] developed a Forward Feature Selection (FFS) technique, which is applied in selecting the optimal features for DDoS attacks. The DL and highly advanced ML method was utilized to execute a hybrid technique for combining DM algorithms of deep neural networks and CNNs. Implementation was employed on FS given the need to detect DDoS on the software-defined networks by utilizing the FFS procedure. Rihan et al. [17] projected a method for identifying threats in IoT networks by employing ensemble FS and DL techniques. Ensemble FS integrates filter methods, namely, L1based, Chi-square, mutual information, variance threshold and ANOVA techniques. The wrapper process is named Recursive Feature Elimination (RFE), which is useful in improving the FS. In [18], a Hybrid Sample Selected RNN-ELM (hybrid SSRNN-ELM) method was provided. From the original dataset, the selected features are removed by utilizing a Sequence Forward Selector (SFS) and LR—Recursive Feature Extraction (LR-RFE). Next, RNN is utilized for learning the features. Next, at the end layer, the ELM algorithm is applied. By using the NSL-KDD dataset, this method is verified.

Setitra et al. [19] developed an improved DL technique with the combination of the Extreme Gradient Boosting (XGBoost) and Autoencoder (AE) methods. Initially, the Shapley Additive exPlanations (SHAP) FS procedure is implemented. On the preceding subsets, the AE is trained. The latent symbol is employed as the input which is produced by the AE. Similarly, Grid Search cross-validation (GSCV) is utilized to find out the hyperparameters. Yousuf and Mir [20] projected a Detecting Attack by employing a Live Capture Neural Network (DALCNN) with the model of RNN as well as executing a Software Defined Network (SDN) by utilizing the OpenDayLight stage. Additionally, the three-tier architecture is mainly designed to categorize and identify DDoS threats. This method organizes the type of attack through ML/DL concepts and novel activation functions.

Padmashree and Krishnamoorthi [21] introduced an effective feature selection with the feature fusion method for the recognition of intruders in IoT. From the preprocessed data, the high-order statistical features are chosen according to the presented Decision tree-based Pearson Correlation Recursive Feature Elimination (DT-PCRFE) method. Alzaqebah et al. [22] present a modified bio-inspired algorithm, the Grey Wolf Optimization algorithm (GWO), which improves the efficiency of the IDS in identifying normal and anomalous traffic in the network. The major improvement covers the smart initialization stage, which fuses the filter and wrapper techniques to ensure that the informative features will be included in an early iteration. Toldinas et al. [23] present a new technique for network intrusion detection using multi-stage DL image recognition. The network feature is converted into four-channel (Red, Green, Blue and Alpha) images. Then, the image is used for classification for training and testing the pre-trained DL model ResNet-50.

3. The Proposed Model

In this study, we have designed an automatic PHHO-ODLC algorithm for a secure IoT environment. The fundamental goal of the PHHO-ODLC technique is to detect the existence of DDoS attacks in the IoT platform. The PHHO-ODLC technique follows three-stage processes such as PHHO PHHO-based FS, ABiLSTM-based DDoS attack detection and GWO-based hyperparameter tuning. Figure 1 depicts the entire flow of the PHHO-ODLC algorithm.

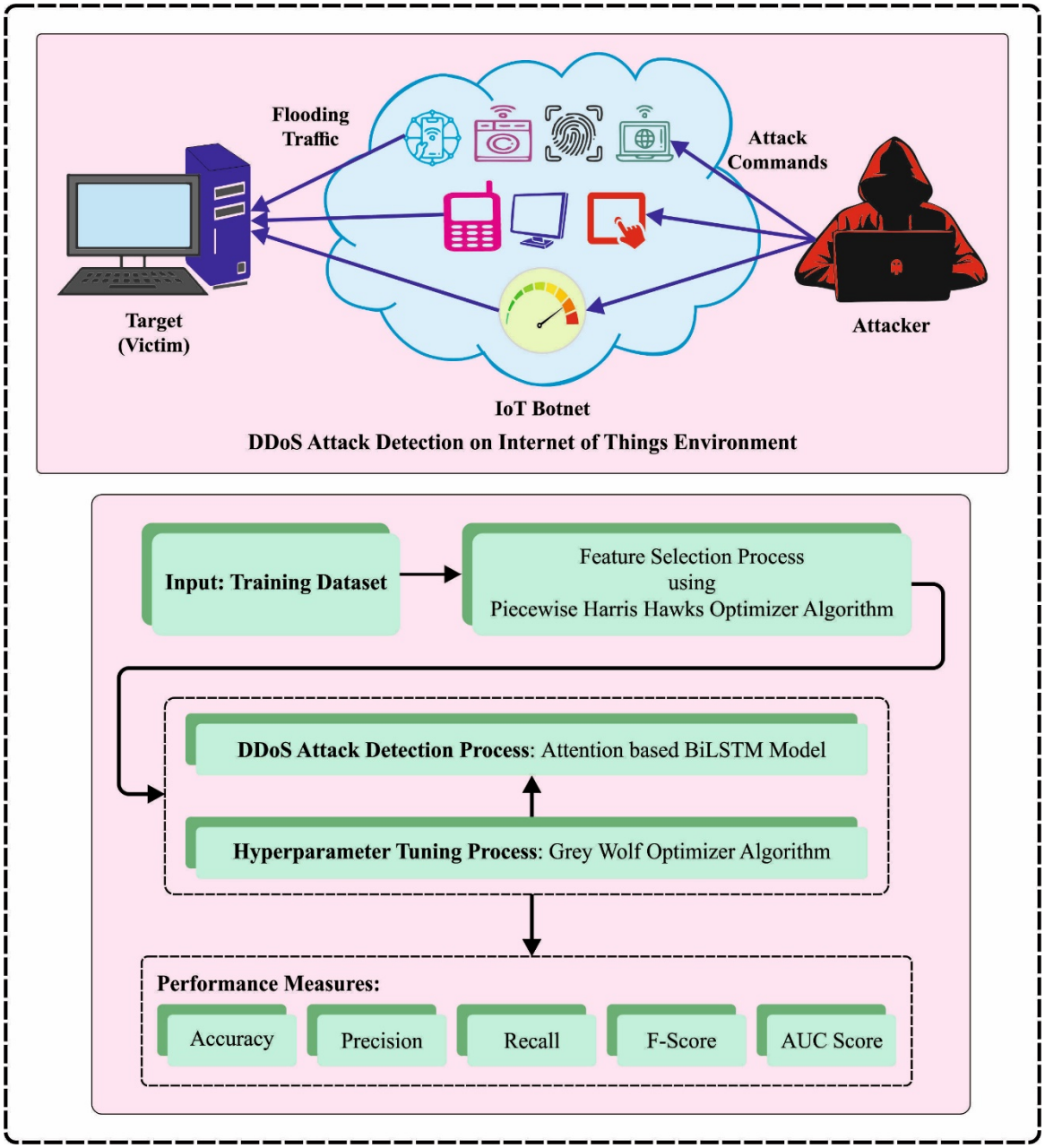

Figure 1. Overall flow of the PHHO-ODLC algorithm.

3.1. Design of the PHHO Algorithm

Primarily, the PHHO algorithm can be employed to choose relevant features and thereby enhance the classification performance. Heidari et al., in 2019, introduced a gradient-free metaheuristic and population-based algorithm to HHO, which emulates the pursuing behaviors of the hawk group to find an optimum solution [24]. The HHO comprises three stages: the local development, global search and transition stages.

Global search stage

The Hawk individuals split up to enlarge the search space and improve the chances of finding the target. Individuals in the population will perch on any place, and the two selection tactics for the perch location are as follows:

$$X(t+1) = \begin{cases} X_{rand}(t) - r_1|X_{rand}(t) - 2r_2X(t)|, \; q \geq 0.5 \\ (X_{rabbit}(t) - X_m(t)) - r_3(LB + r_4(UB - LB)), \; q < 0.5 \end{cases} \quad (1)$$

In Equation (1), r_1, r_2, r_3, r_4 and q are the random number ranges within [0, 1], X_{rabbit} represents the prey location, X_{and} shows an individual random location in the present hawk group, UB and LB denote the upper and lower limitations of the search area, N indicates the population number, X_m refers to the average location of the individual in the existing hawk group and $X(t)$ shows the individual location as follows:

$$X_m(t) = \frac{1}{N}\sum_{i=1}^{N} X_i(t) \tag{2}$$

Transition stage

The individual hawk chooses the hunting strategy based on the changes in the escaping energy of the prey. Now, the HHO technique transits from the search to exploitation phases using the subsequent escaping energy equation.

$$E = 2E_0\left(1 - \frac{t}{T}\right) \tag{3}$$

In Equation (3), the escaping energy at the initial state is E_0 and is a randomly generated value within $[-1, 1]$, T represents the overall iteration counter and t shows the existing iteration counter.

Local development phase

Based on the escaping route of the prey, the hawk adopts a pursuit strategy. The HHO technique exploits the subsequent four social behaviors for stimulating the roundup behaviors of hawks. The escaping possibility of prey is represented as r, where $r \geq 0.5$ implies failure and $r < 0.5$ implies success.

Soft roundup: if $r \geq 0.5$ and $|E| \geq 0.5$, then the prey has sufficient escaping energy and the prey is energetic; hence, the hawk uses a soft strategy, as follows:

$$X(t+1) = \Delta X(t) - E|JX_{rabbit}(t) - X(t)| \tag{4}$$

$$X(t) = X_{rabbit}(t) - X(t) \tag{5}$$

From the expression, the difference between the prey and the existing location of individuals at iteration t is $\Delta X(t)$, and the random escaping strength of the prey is J, which is a randomly generated value within [0, 2].

Hard round-up: if $r \geq 0.5$ but $|E| < 0.5$, then the prey has low energy to escape and is exhausted; hence, the individual hawk adopts a hard strategy as:

$$X(t+1) = X_{rabbit}(t) - E|\Delta X(t)| \tag{6}$$

Soft round-up with progressive quick dive: if $r < 0.5$ and $|E| \geq 0.5$, then the target has the possibility of effective escape and the prey is energetic, so the hawk individuals adopt a gentle encirclement to perform the surprise attacks. The study introduced a Levy flight (LF) to emulate the behaviors and escaping route of the target, and the updating location strategy is given below:

$$Y = X_{rabbit}(t) - E|JX_{rabbit}(t) - X(t)| \tag{7}$$

$$Z = Y + S \times LF(D) \tag{8}$$

$$X(t+1) = \begin{cases} Y, F(Y) < F(X(t)) \\ Z, F(Z) < F(X(t)) \end{cases} \tag{9}$$

where the random vector of size $1 \times D$ dimension is S, D shows the problem dimension, the Levy flight function is $LP()$ and the fitness function is $F()$. Hard round-up with progressive

quick dive: if $r < 0.5$ and $|E| < 0.5$, then the prey does not have sufficient energy to escape; hence, a progressive quick-dive tough roundup approach is applied.

$$Y = X_{rabbit}(t) - E|JX_{rabbit}(t) - X_m(t)| \tag{10}$$

$$Z = Y + S \times LF(D) \tag{11}$$

$$X(t+1) = \begin{cases} Y, F(Y) < F(X(t)) \\ Z, F(Z) < F(X(t)) \end{cases} \tag{12}$$

3.2. Piecewise Chaotic Map

A standard representative of a chaotic map is a piecewise chaotic map, which is randomized and more ergodic. The piecewise chaotic map is introduced to increase the initial population for increasing the probability of escaping from local optima and also enhancing the population diversity of HHO. The mathematical equation is given below:

$$x(t+1) = \begin{cases} \dfrac{x(t)}{p}, & 0 \le x(t) < p \\ \dfrac{x(t)-p}{0.5-p}, & p \le x(t) < 0.5 \\ \dfrac{1-p-x(t)}{0.5-p}, & 0.5 \le x(t) < 1-p \\ \dfrac{1-x(t)}{p}, & 1-p \le x(t) < 1 \end{cases} \tag{13}$$

In the PHHO technique, the FF is used to balance between the number of features selected in the solution (minimum) and the classification outcome (maximum) attained by the selected features. Equation (10) shows the FF for calculating the solution.

$$Fitness = \alpha\gamma_R(D) + \beta\frac{|R|}{|C|} \tag{14}$$

In Equation (14), the parameters α and β correspond to the significance of the classification quality and subset length. $\in [1, 0]$ and $\beta = 1 - \alpha.\gamma_R(D)$ shows the classifier error rate. $|R|$ shows the cardinality of the selected subset, and the total number of features in the dataset is represented as $|C|$.

3.3. Structure of the ABiLSTM Model

The ABiLSTM model can be used for attack detection. The classical LSTM is only capable of using prior context [25]. The Bi-LSTM is used to access long-range data to better grab two-direction context dependency. At the same time, Bi-directional architecture extracts the context data from both directions with forward and backward layers.

The hidden sequence and output of the forward layer are computed repeatedly by the input in a sequential order from step 1 to step t, and the hidden sequence and output of the backward layer are repeated from step t to 1. $\overrightarrow{h_t}$ and $\overleftarrow{h_t}$ indicate the output of the forward and backward layers computed by the typical LSTM, correspondingly. The Bi-LSTM layer produces an output vector, Y, where every component is evaluated by the following equation:

$$\mathrm{y_t} = \sigma\left(\overrightarrow{h_t}, \overleftarrow{h_t}\right) \tag{15}$$

where function σ is used for coupling the two $\overrightarrow{h_t}$ and $\overleftarrow{h_t}$ series. The last output of the Bi-LSTM layer is formulated as $Y = [y_1, y_2, \ldots, y_t]$, where the final component, y_t, refers to

the predicted well-log values for the next depth once the Bi-LSTM implements well-logging prediction. Figure 2 represents the structure of ABiLSTM.

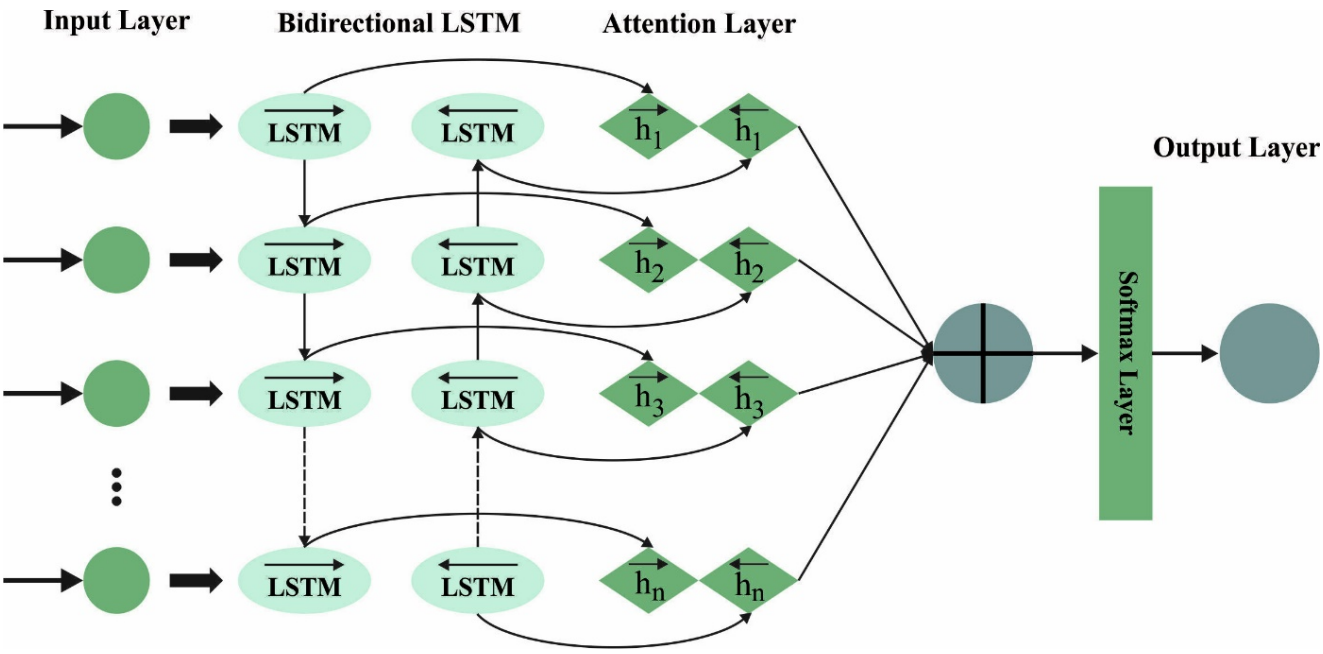

Figure 2. Architecture of ABiLSTM.

In recent times, the attention model-based NN has illustrated success in a large number of tasks. In Bi-LSTM with an attention model, the attention mechanism aligns with the input cell state at the existing step through the implicit state of Bi-LSTM or to exploit the final cell state of the Bi-LSTM, Next, the relationship between the outputs and the candidate intermediate states is evaluated. The relevant data are highlighted, and the unrelated data are suppressed to optimize the efficiency and accuracy of prediction in the learning method:

$$M = \tanh(Y) \tag{16}$$

$$\alpha = softmax\left(w_a^T M\right) \tag{17}$$

$$A = Y\alpha^T \tag{18}$$

where Y refers to a matrix and shows the features taken by the Bi-LSTM networks in the above-mentioned matrix $Y = [y_1, y_2, \ldots, y_t]$. T indicates the transpose function. The weight coefficient matrix of the attention layer can be represented as w_a. α signifies the attention weight for features Y.

3.4. Process Involved in GWO-Based Parameter Selection

The GWO approach is employed to tune the hyperparameter values of the ABiLSTM model. GWO is a global random search approach presented by inspiring searching and hunting behaviors of grey wolves [26]. There are four levels of GW population from low to high: α, β, δ and ω wolves. Target hunting is performed strictly based on the order of the wolf pack. The hunting procedure of GW can be separated into three parts, namely, searching and attacking prey, encircling prey and hunting. GWs move closer and encircle prey once they start searching for prey, and the performance is represented in Equations (19) and (20) as:

$$D = \left|M \cdot X_p(t) - X(t)\right| \tag{19}$$

$$X(t+1) = X_p(t) - A \cdot D \tag{20}$$

whereas t denotes the count of existing iterations, $X(t)$ and $X(t)$ imply the location vectors of prey and GW x, $(t+1)$ is the novel place of GW and D denotes the distance between GW and targets. M and A are co-ordination coefficient vectors which are determined by Equations (21) and (22):

$$A = 2a \cdot r_1 - a \tag{21}$$

$$M = 2 \cdot r_2 \tag{22}$$

where a represents the convergence factor to be linearly reduced from two to zero in the iteration method, and r_1 and r_2 denote the random numbers between zero and one.

In the control of optimum wolves, wolves recognize the place of prey and get closer towards it. This performance is represented by Equations (23)–(26):

$$D_\alpha = |M_1 \cdot X_\alpha - X(t)|, X_1 = X_\alpha - A_1 \cdot D_\alpha \tag{23}$$

$$D_\beta = \left|M_2 \cdot X_\beta - X(t)\right|, X_2 = X_\beta - A_2 \cdot D_\beta \tag{24}$$

$$D_\delta = |M_3 \cdot X_\delta - X(t)|, X_3 = X_\delta - A_3 \cdot D_\delta \tag{25}$$

$$X(t+1) = \frac{X_1 + X_2 + X_3}{3} \tag{26}$$

whereas α stands for the neighboring wolf to prey, β denotes the second nearby wolf towards the target and δ implies the third adjoining wolf towards the target. The upgraded average of α, β and δ wolves provides the novel GW place.

GW groups mostly hunt based on the information of α, β and δ wolves. During the mathematical process, the values of the co-ordination coefficient vector can be deployed for controlling if the GW is exploring for an attacking target. If $|A| > 1$, then GW in the prey increases their searching possibility to place the prey efficiently. If $|A| < 1$, then GW restricts the searching region to attack the target. The fitness selection is a primary factor in the GWO technique. An encoded solution is employed to evaluate the outcome of the solution candidate. At this point, the accuracy values are the major condition exploited to design a FF.

$$Fitness = \max(P) \tag{27}$$

$$P = \frac{TP}{TP + FP} \tag{28}$$

where TP and FP represent the true- and false-positive values.

4. Performance Evaluation

The DDoS attack detection results of the PHHO-ODLC technique are tested by applying the BoT-IoT dataset [27] in terms of two aspects: the binary dataset and multi-class dataset. Table 1 shows the details of the binary database.

Table 1. Details on the binary database.

Binary Database	
Classes	**No. of Samples**
Attack	1579
Normal	477
Total No. of Instances	2056

Figure 3 illustrates the classifier analysis of the PHHO-ODLC algorithm on the binary database. Figure 3a,b show the confusion matrices provided with the PHHO-ODLC system at 80:20 of the TR Phase/TS Phase. The figure signified that the PHHO-ODLC algorithm has recognized and classified two class labels. Also, Figure 3c exhibits the PR curve of the

PHHO-ODLC algorithm. The outcome illustrated that the PHHO-ODLC methodology has attained improved PR performance in two classes. However, Figure 3d shows the ROC analysis of the PHHO-ODLC method. The outcome described that the PHHO-ODLC algorithm resulted in an efficient outcome with high ROC values in different class labels.

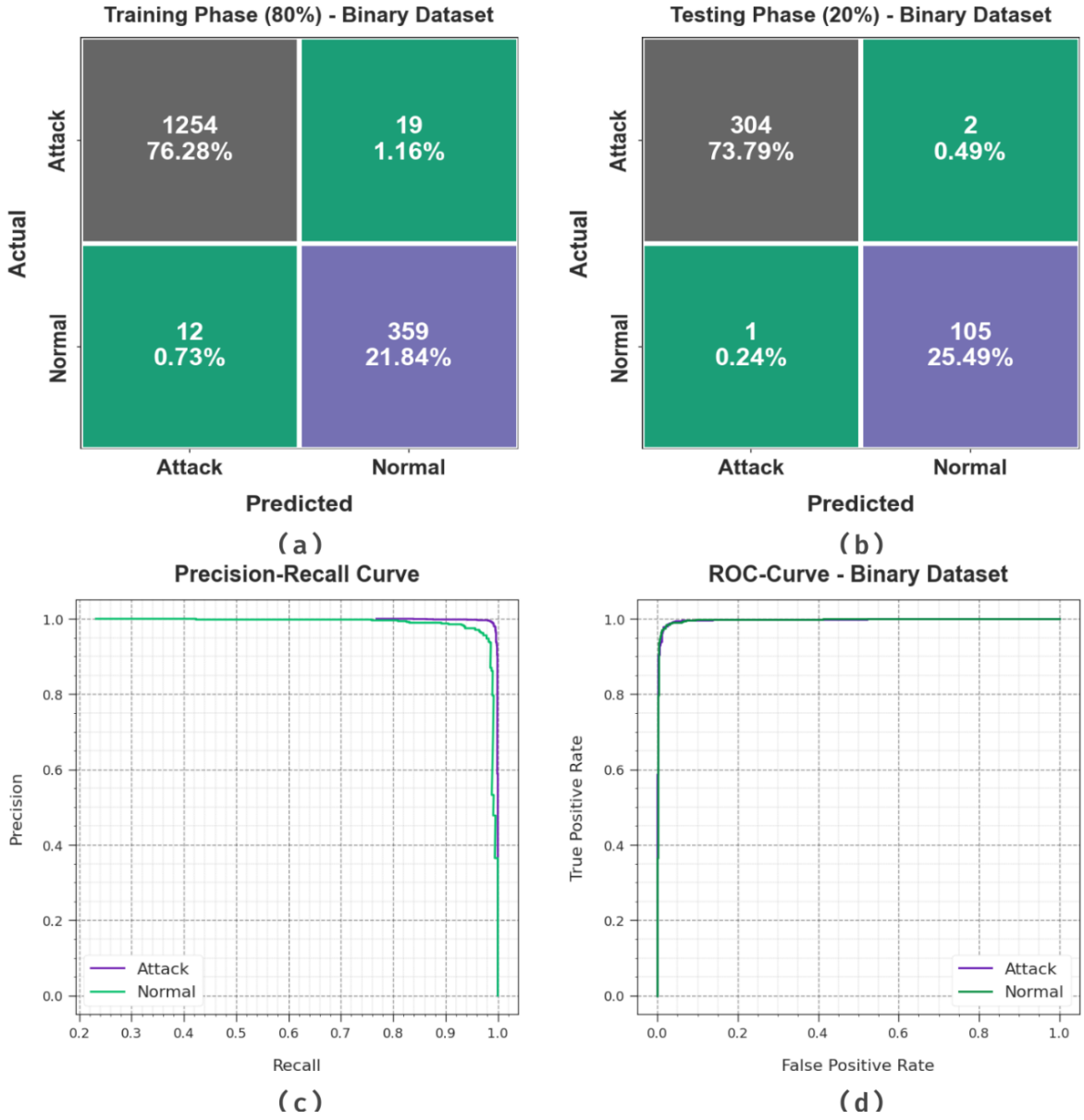

Figure 3. Binary database. (**a**,**b**) Confusion matrices, (**c**) PR_curve and (**d**) ROC.

The attack detection outcomes of the PHHO-ODLC method are tested on the binary dataset in Table 2 and Figure 4. The simulation value indicated that the PHHO-ODLC algorithm appropriately recognizes the attacks and normal samples. On 80% of the TR Phase, the PHHO-ODLC system provides an average $accu_y$ of 97.64%, $prec_n$ of 97.01%, $reca_l$ of 97.64%, F_{score} of 97.32% and AUC_{score} of 97.64%. Additionally, with 20% of the TS Phase, the PHHO-ODLC approach offers an average $accu_y$ of 99.20%, $prec_n$ of 98.90%, $reca_l$ of 99.20%, F_{score} of 99.05% and AUC_{score} of 99.20%, correspondingly.

Table 2. Attack detection outcome of the PHHO-ODLC algorithm on a binary database.

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
			TR Phase (80%)		
Attack	98.51	99.05	98.51	98.78	97.64
Normal	96.77	94.97	96.77	95.86	97.64
Average	97.64	97.01	97.64	97.32	97.64
			TS Phase (20%)		
Attack	99.35	99.67	99.35	99.51	99.20
Normal	99.06	98.13	99.06	98.59	99.20
Average	99.20	98.90	99.20	99.05	99.20

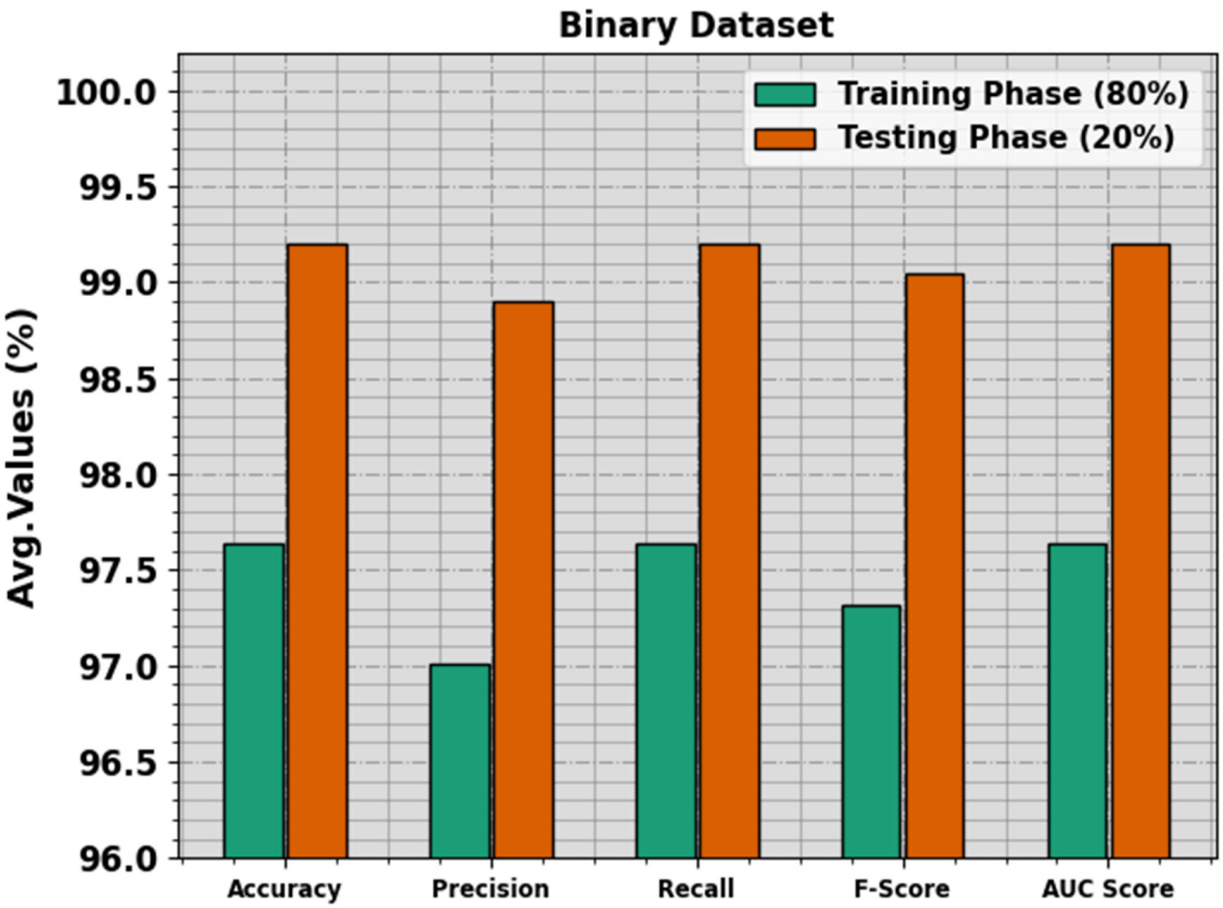

Figure 4. Average of the PHHO-ODLC algorithm on a binary database.

To calculate the performance of the PHHO-ODLC approach on the binary dataset, TR and TS $accu_y$ curves are described, as demonstrated in Figure 5. The TR and TS $accu_y$ curves exhibit the performance of the PHHO-ODLC method over numerous epochs. The figure provided meaningful details about the learning task and generalization capabilities of the PHHO-ODLC model. With a rise in the epoch count, it is observed that the TR and TS $accu_y$ curves are enhanced. It is noted that the PHHO-ODLC system achieves enriched testing accuracy that has the potential to recognize the patterns in the TR and TS data.

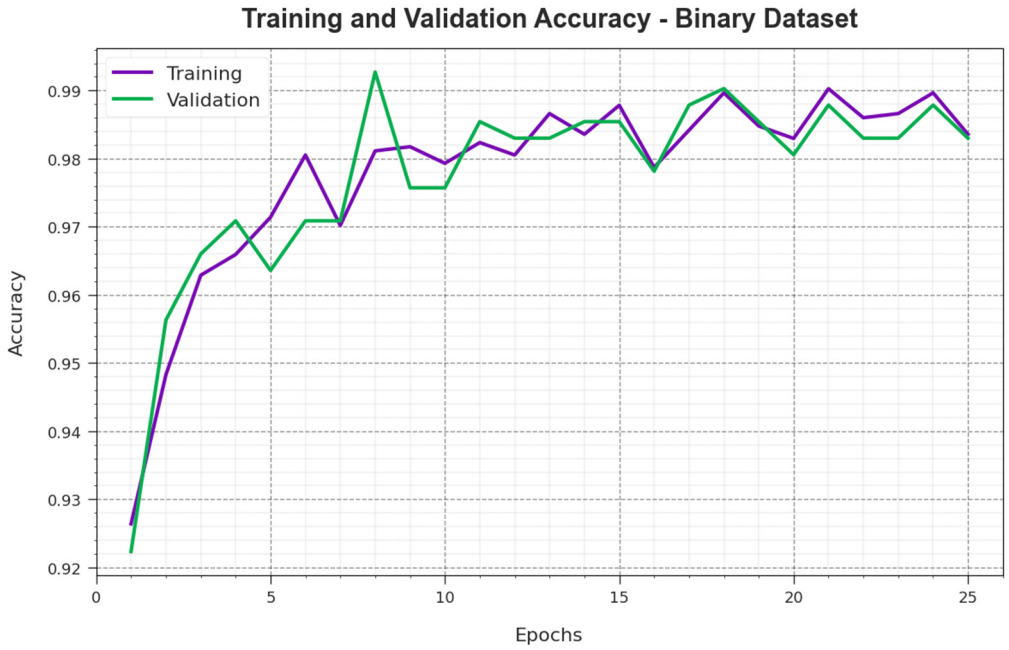

Figure 5. $Accu_y$ curve of the PHHO-ODLC algorithm on a binary database.

Figure 6 shows the overall TR and TS loss values of the PHHO-ODLC system on a binary dataset over epochs. The TR loss indicates the model loss is minimized over epochs. Mainly, the loss values obtained decreased as the model adapted the weight for diminishing the predicted error on the TR and TS data. The loss curves exhibit the extent to which the model fits the training data. It is noted that the TR and TS loss is progressively minimized and represents that the PHHO-ODLC system efficiently learns the patterns demonstrated in the TR and TS data. It is also evidenced that the PHHO-ODLC methodology modifies the parameters for decreasing the difference between the actual and predicted training labels.

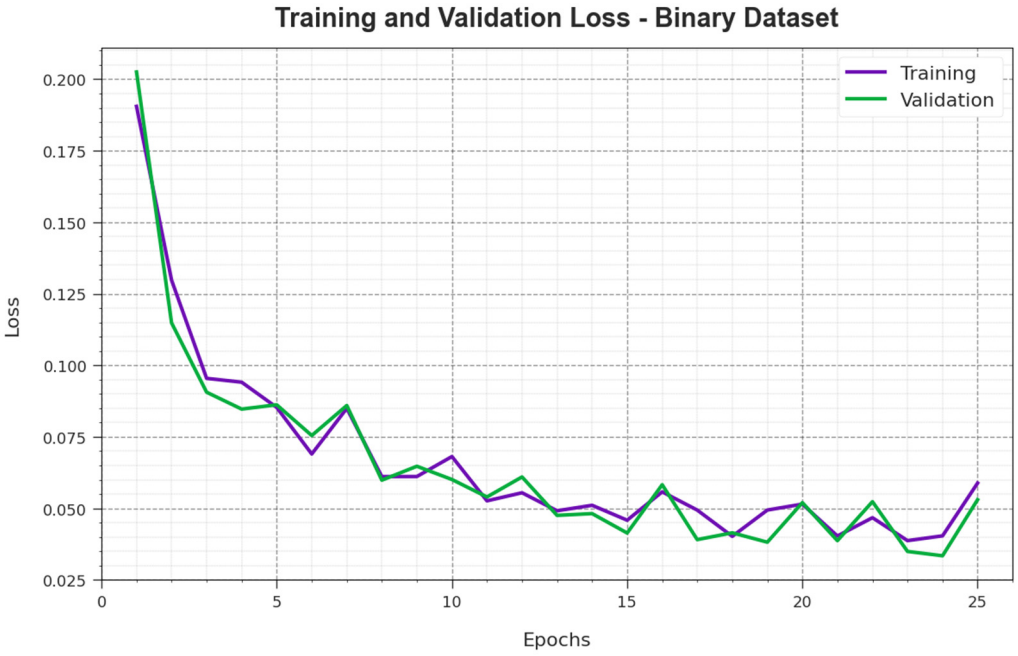

Figure 6. Loss curve of the PHHO-ODLC algorithm on a binary database.

Table 3 demonstrates the details of the multiclass dataset.

Table 3. Details on the multiclass database.

Multiclass Database	
Class	**No. of Instances**
DDoS	500
DoS	500
Recon	500
Theft	79
Normal	477
Total No. of Samples	2056

Figure 7 demonstrates the classifier analysis of the PHHO-ODLC algorithm on the multiclass database. Figure 7a,b represent the confusion matrix provided with the PHHO-ODLC technique at 80:20 of the TR Phase/TS Phase. The outcome demonstrated that the PHHO-ODLC algorithm has detection and is categorized on five class labels. Figure 7c defines the PR curve of the PHHO-ODLC model. The figure indicates that the PHHO-ODLC method has attained improved PR outcomes in five classes. Figure 7d reveals the ROC analysis of the PHHO-ODLC system. The experimental outcome indicated that the PHHO-ODLC method resulted in an effectual solution with improved ROC outcomes in various class labels.

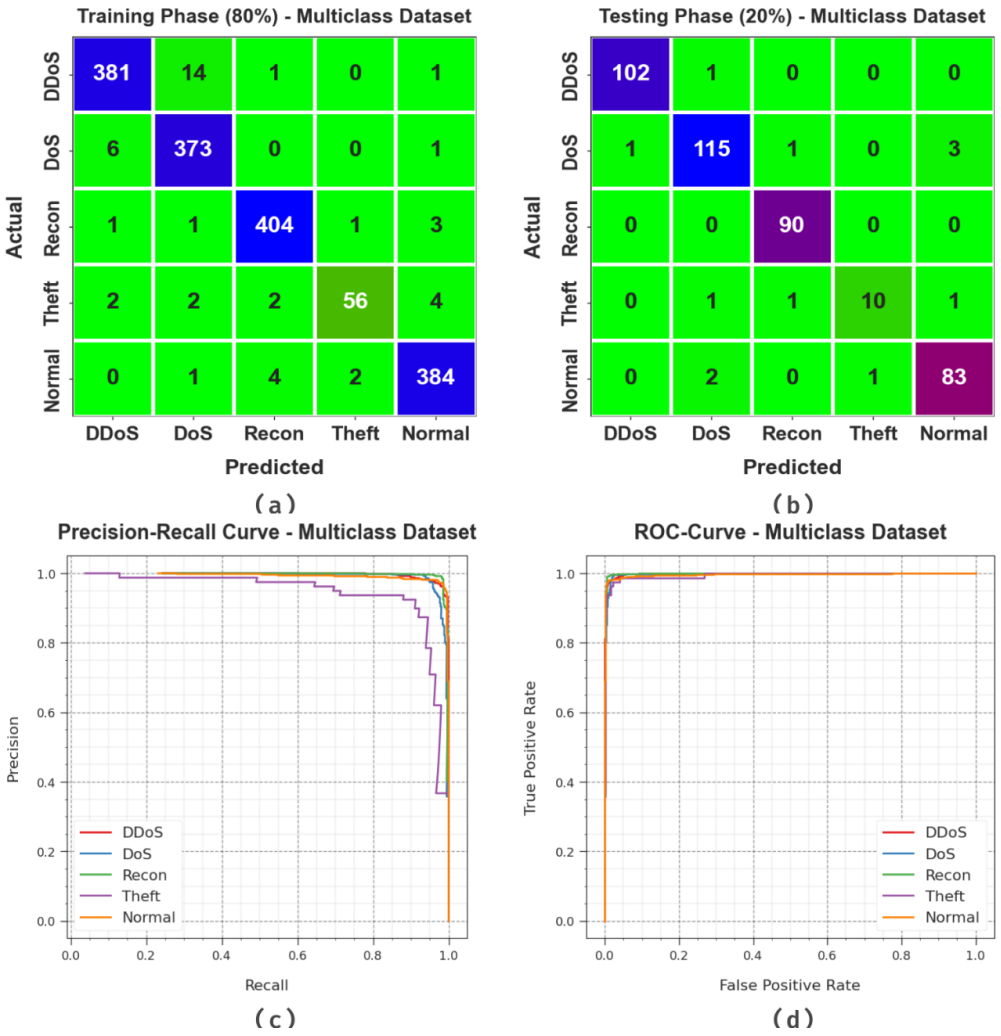

Figure 7. Multiclass database. (**a**,**b**) Confusion matrices, (**c**) PR_curve and (**d**) ROC.

The attack detection analysis of the PHHO-ODLC approach is tested on the multiclass database in Table 4 and Figure 8. The observation data indicate that the PHHO-ODLC method properly recognizes all five classes. On 80% of the TR Phase, the PHHO-ODLC method provides an average $accu_y$ of 98.88%, $prec_n$ of 96.80%, $reca_l$ of 95.14%, F_{score} of 95.91% and AUC_{score} of 97.21%. Additionally, with 20% of the TS Phase, the PHHO-ODLC technique offers an average $accu_y$ of 98.83%, $prec_n$ of 95.96%, $reca_l$ of 93.66%, F_{score} of 94.69% and AUC_{score} of 96.45%, correspondingly.

Table 4. Attack detection outcome of the PHHO-ODLC algorithm on a multiclass database.

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
			TR Phase (80%)		
DDoS	98.48	97.69	95.97	96.82	97.62
DoS	98.48	95.40	98.16	96.76	98.37
Recon	99.21	98.30	98.54	98.42	98.98
Theft	99.21	94.92	84.85	89.60	92.33
Normal	99.03	97.71	98.21	97.96	98.75
Average	98.88	96.80	95.14	95.91	97.21
			TS Phase (20%)		
DDoS	99.51	99.03	99.03	99.03	99.35
DoS	97.82	96.64	95.83	96.23	97.23
Recon	99.51	97.83	100.00	98.90	99.69
Theft	99.03	90.91	76.92	83.33	88.34
Normal	98.30	95.40	96.51	95.95	97.64
Average	98.83	95.96	93.66	94.69	96.45

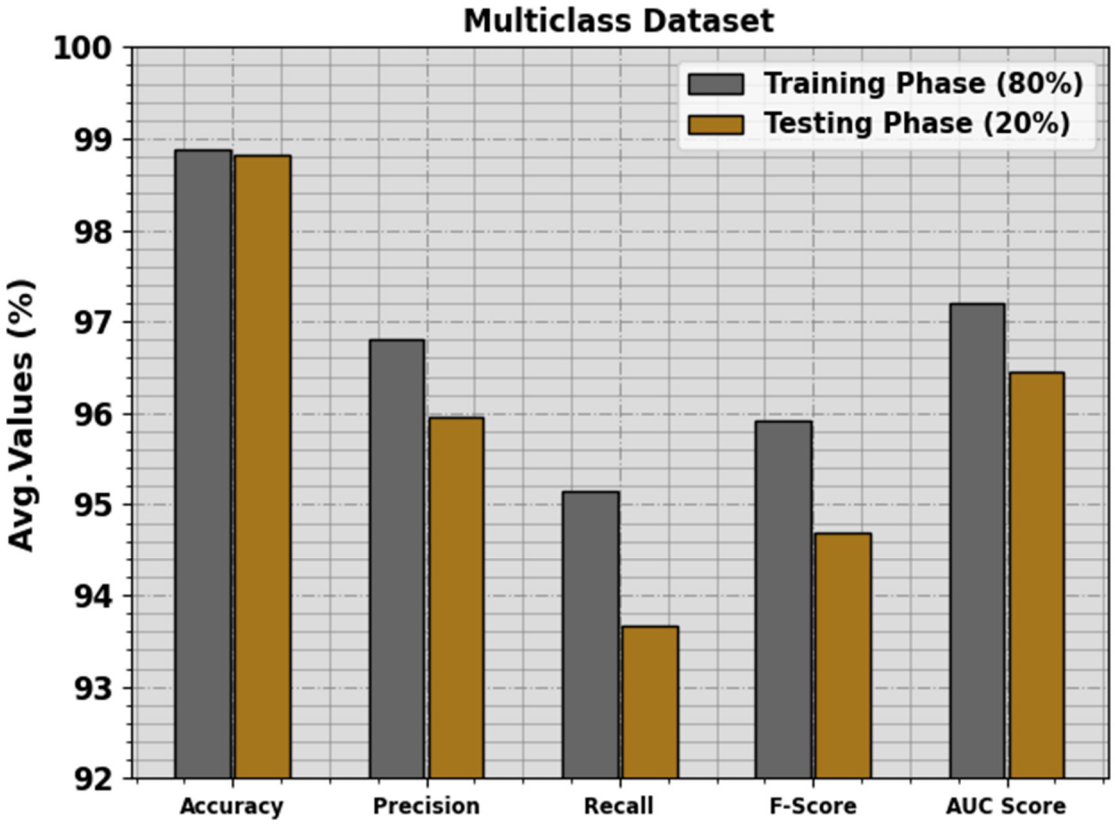

Figure 8. Average of the PHHO-ODLC algorithm on a multiclass database.

To determine the performance of the PHHO-ODLC system on the multiclass dataset, TR and TS $accu_y$ curves are defined, as shown in Figure 9. The TR and TS $accu_y$ curves indicate the performance of the PHHO-ODLC approach over several epochs. The figure offered meaningful details about the learning tasks and generalization capacity of the PHHO-ODLC technique. With an improvement in the epoch count, it is noted that the TR and TS $accu_y$ curves get enriched. It is evident that the PHHO-ODLC method attains better testing accuracy and can recognize the patterns in the TR and TS data.

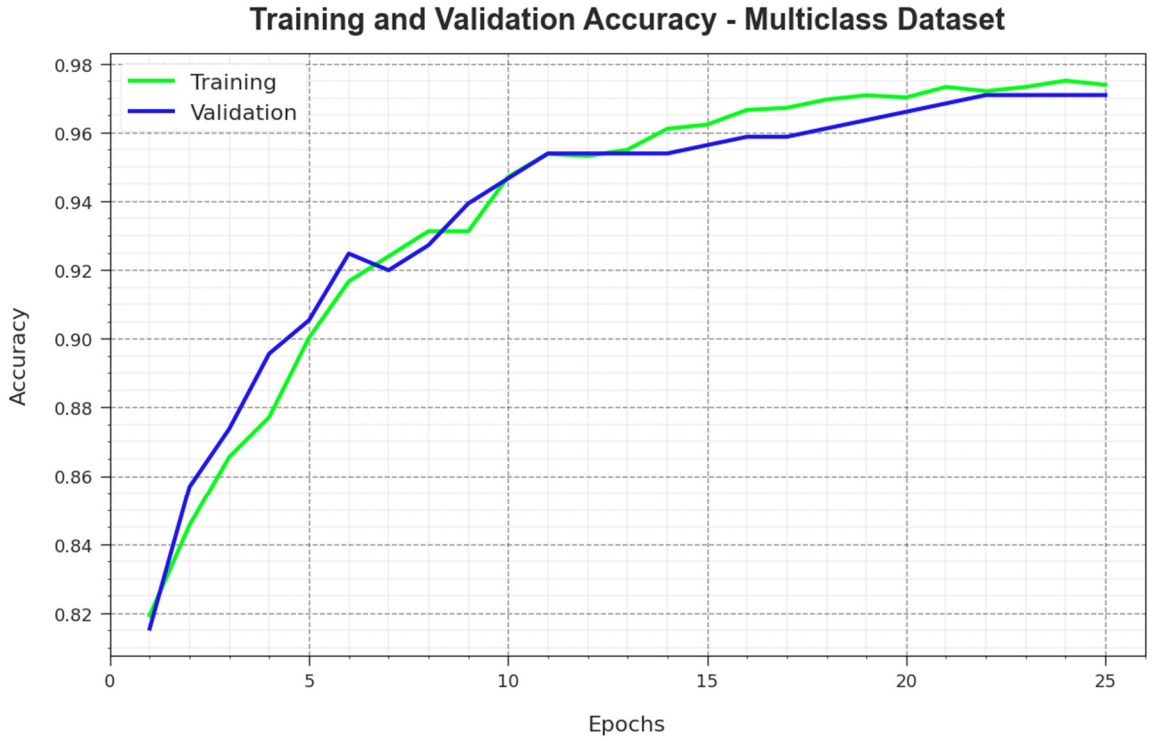

Figure 9. $Accu_y$ curve of the PHHO-ODLC algorithm on a multiclass database.

Figure 10 illustrates the overall TR and TS loss values of the PHHO-ODLC method on a multiclass dataset over epochs. The TR loss specifies the model loss decreases over epochs. Generally, the loss values get reduced as the model adjusts the weight to reduce the predictable error on the TR and TS data. The loss curves show the extent to which the model fits the training data. It is observed that the TR and TS loss is gradually diminishing, signifying that the PHHO-ODLC algorithm efficiently learns the patterns demonstrated in the TR and TS data. It is also evidenced that the PHHO-ODLC technique adapts the parameters to lessen the dissimilarity between the predicted and actual training labels.

Finally, a comprehensive outcome of the PHHO-ODLC system with other methods is represented in Table 5 and Figure 11 [28]. The outcomes highlight the enhanced results of the PHHO-ODLC technique. Based on $accu_y$, the PHHO-ODLC technique gains an increased $accu_y$ of 99.20%, while the H3SC-DLIDS, AE-MLP, IDS-IoT, XGBoost, RF and DT models obtain decreased $accu_y$ values of 99.05%, 98.19%, 97.40%, 97.09%, 97.00% and 95.21%, respectively. Also, based on $prec_n$, the PHHO-ODLC method achieves an improved $prec_n$ of 98.90%, whereas the H3SC-DLIDS, AE-MLP, IDS-IoT, XGBoost, RF and DT methodologies obtain reduced $prec_n$ values of 96.65%, 95.91%, 95.80%, 94.28%, 94.98% and 92.43%, individually. Finally, based on $reca_l$, the PHHO-ODLC approach gains a raised $reca_l$ of 99.20%, but the H3SC-DLIDS, AE-MLP, IDS-IoT, XGBoost, RF and DT systems acquire minimized $reca_l$ values of 95.67%, 93.31%, 94.90%, 92.13%, 93.69% and 92.51%, correspondingly.

These outcomes confirmed the better solution of the PHHO-ODLC technique on the DDoS attack detection algorithm. The PHHO-ODLC method's superiority in performance

over other techniques can be justified through its novel approach to DDoS attack recognition in IoT environments. In the initial stage, the usage of the PHHO enables highly effective feature selection, ensuring that only the most relevant data attributes are used for classification. This tailored feature set minimizes noise and augments the model's precision, a crucial benefit in distinguishing genuine threats from noise in IoT data. In the second stage, the incorporation of the ABiLSTM network equips the PHHO-ODLC technique with deep learning abilities, facilitating the analysis of sequential data patterns. This enables the effective detection of complex attack patterns and further increases accuracy in DDoS attack classification. Furthermore, the third stage, using the GWO for hyperparameter tuning, ensures that the model is fine-tuned to its highest performance, improving its capability to adapt to various IoT environments and attack scenarios. In summary, the PHHO-ODLC technique excels due to its holistic method, including deep learning, feature selection and hyperparameter optimization, which collectively improve its accuracy and resilience in DDoS attack detection, setting it apart as a robust solution in the IoT security landscape.

Figure 10. Loss curve of the PHHO-ODLC algorithm on a multiclass database.

Table 5. Comparative outcome of the PHHO-ODLC system with other approaches.

Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
PHHO-ODLC	99.20	98.90	99.20	99.05
H3SC-DLIDS	99.05	96.65	95.67	96.14
AE-MLP	98.19	95.91	93.31	95.13
IDS-IoT	97.40	95.80	94.90	95.53
XGBoost	97.09	94.28	92.13	95.05
RF	97.00	94.98	93.69	94.57
DT	95.21	92.43	92.51	93.26

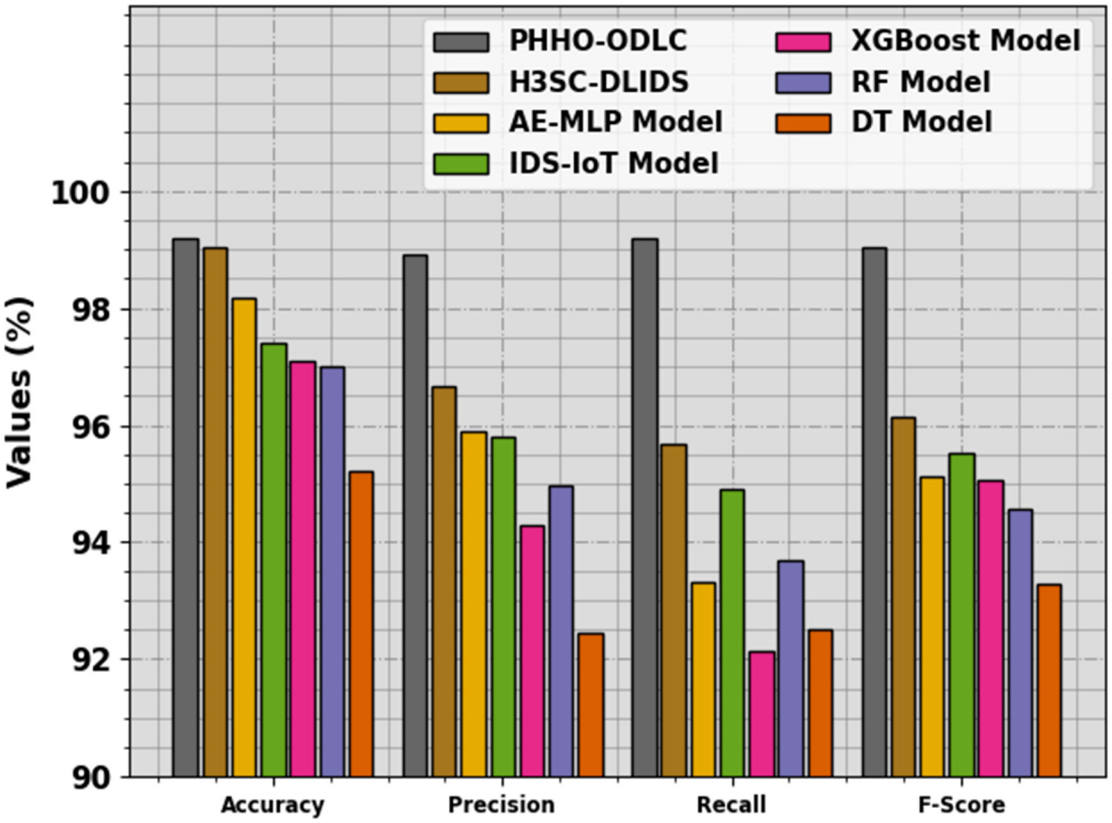

Figure 11. Comparative outcome of the PHHO-ODLC methodology with other approaches.

5. Conclusions

In this manuscript, we have developed an automatic PHHO-ODLC technique for a secure IoT environment. The fundamental goal of the PHHO-ODLC method is to detect the presence of DDoS attacks in the IoT platform. The PHHO-ODLC algorithm follows three-stage processes such as PHHO-based FS, ABiLSTM-based DDoS attack detection and GWO-based hyperparameter tuning. A detailed comparative result analysis indicated that the proposed model achieves a better performance over other models, with a maximum accuracy of 99.20%. The PHHO-ODLC technique provides a robust solution for detecting DDoS attacks in the IoT environment, ensuring the security and integrity of interconnected devices. Its real-world applications extend to safeguarding critical IoT systems, such as smart cities, healthcare and industrial automation, from disruptive cyber threats. Future research will explore the scalability of the PHHO-ODLC technique in dealing with large IoT networks and a wide range of attack types. Moreover, the development of adaptive mechanisms to respond to evolving DDoS attack strategies and the integration of anomaly detection methods will be integral to further improving IoT security.

Author Contributions: Conceptualization, M.R. and A.A.-M.A.-G.; Methodology, M.R. and S.M.A.; Software, L.A.M. and D.A.; Validation, L.A.M. and T.A.; Formal analysis, S.M.A. and T.A.; Investigation, T.A. and A.A.-M.A.-G.; Resources, S.M.A. and D.A.; Data curation, L.A.M., D.A., T.A. and A.A.-M.A.-G.; Writing—original draft, M.R. and S.M.A.; Writing—review & editing, L.A.M.; Visualization, D.A.; Supervision, A.A.-M.A.-G.; Project administration, M.R.; Funding acquisition, S.M.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research work was funded by Institutional Fund Projects under grant no. (IFPDP-260-22). Therefore, the authors gratefully acknowledge the technical and financial support from the Ministry of Education and Deanship of Scientific Research (DSR), King Abdulaziz University (KAU), Jeddah, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Emil Selvan, G.S.R.; Ganeshan, R.; Jingle, I.D.J.; Ananth, J.P. FACVO-DNFN: Deep learning-based feature fusion and Distributed Denial of Service attack detection in cloud computing. *Knowl.-Based Syst.* **2023**, *261*, 110132.
2. Hong, L.; Wehbi, K.; Alsalah, T.H. Hybrid feature selection for efficient detection of DDoS attacks in IoT. In Proceedings of the 2022 6th International Conference on Deep Learning Technologies, Xi'an, China, 26–28 July 2022; pp. 120–127.
3. Sanchez, O.R.; Repetto, M.; Carrega, A.; Bolla, R.; Pajo, J.F. Feature selection evaluation towards a lightweight deep learning DDoS detector. In Proceedings of the ICC 2021-IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
4. Wang, C.; Zhu, T. DDoS attack detection methods based on deep learning in healthcare. *J. Mech. Med. Biol.* **2023**, *23*, 2340008. [CrossRef]
5. Akgun, D.; Hizal, S.; Cavusoglu, U. A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. *Comput. Secur.* **2022**, *118*, 102748. [CrossRef]
6. Malliga, S.; Nandhini, P.S.; Kogilavani, S.V. A comprehensive review of deep learning techniques for the detection of (distributed) denial of service attacks. *Inf. Technol. Control* **2022**, *51*, 180–215. [CrossRef]
7. Savanović, N.; Toskovic, A.; Petrovic, A.; Zivkovic, M.; Damaševičius, R.; Jovanovic, L.; Bacanin, N.; Nikolic, B. Intrusion Detection in Healthcare 4.0 Internet of Things Systems via Metaheuristics Optimized Machine Learning. *Sustainability* **2023**, *15*, 12563. [CrossRef]
8. Khempetch, T.; Wuttidittachotti, P. DDoS attack detection using deep learning. *IAES Int. J. Artif. Intell.* **2021**, *10*, 382. [CrossRef]
9. Alaca, Y.; Çelik, Y. Cyber attack detection with QR code images using lightweight deep learning models. *Comput. Secur.* **2023**, *126*, 103065. [CrossRef]
10. Saurabh, K.; Kumar, T.; Singh, U.; Vyas, O.P.; Khondoker, R. NFDLM: A Lightweight Network Flow-based Deep Learning Model for DDoS Attack Detection in IoT Domains. In Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 6–9 June 2022; pp. 736–742.
11. Farukee, M.B.; Shabit, M.Z.; Haque, M.R.; Sattar, A.S. DDoS attack detection in IoT networks using deep learning models combined with the random forest as a feature selector. In *Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8–9, 2020, Revised Selected Papers*; Springer: Singapore, 2021; pp. 118–134.
12. Cherian, M.; Varma, S.L. Secure SDN–IoT Framework for DDoS Attack Detection Using Deep Learning and Counter-Based Approach. *J. Netw. Syst. Manag.* **2023**, *31*, 54. [CrossRef]
13. Sharifian, Z.; Barekatain, B.; Quintana, A.A.; Beheshti, Z.; Safi-Esfahani, F. Sin-Cos-bIAVOA: A new feature selection method based on an improved African vulture optimization algorithm and a novel transfer function to DDoS attack detection. *Expert Syst. Appl.* **2023**, *228*, 120404. [CrossRef]
14. Dora, V.R.S.; Lakshmi, V.N. Optimal feature selection with CNN-feature learning for DDoS attack detection using meta-heuristic-based LSTM. *Int. J. Intell. Robot. Appl.* **2022**, *6*, 323–349. [CrossRef]
15. Ma, L.; Chai, Y.; Cui, L.; Ma, D.; Fu, Y.; Xiao, A. A deep learning-based DDoS detection framework for the Internet of Things. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
16. Matsa, L.S.; Zodi-Lusilao, G.-A.; Bhunu-Shava, F. Forward feature selection for DDoS detection on cross-plane of software-defined network using hybrid deep learning. In Proceedings of the 2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), Windhoek, Namibia, 23–25 November 2021; pp. 1–7.
17. Rihan, S.D.A.; Anbar, M.; Alabsi, B.A. Approach for Detecting Attacks on IoT Networks Based on Ensemble Feature Selection and Deep Learning Models. *Sensors* **2023**, *23*, 7342. [CrossRef] [PubMed]
18. Hariprasad, S.; Deepa, T.; Bharathiraja, N. Detection of DDoS Attack in IoT Networks Using Sample Selected RNN-ELM. *Intell. Autom. Soft Comput.* **2022**, *34*, 1425–1440. [CrossRef]
19. Setitra, M.A.; Fan, M.; Bensalem, Z.E.A. An efficient approach to detect distributed denial of service attacks for software-defined internet of things combining autoencoder and extreme gradient boosting with feature selection and hyperparameter tuning optimization. *Trans. Emerg. Telecommun. Technol.* **2023**, *34*, e4827. [CrossRef]
20. Yousuf, O.; Mir, R.N. DDoS attack detection in the Internet of Things using recurrent neural network. *Comput. Electr. Eng.* **2022**, *101*, 108034. [CrossRef]
21. Padmashree, A.; Krishnamoorthi, M. Decision Tree with Pearson Correlation-based Recursive Feature Elimination Model for Attack Detection in IoT Environment. *Inf. Technol. Control* **2022**, *51*, 771–785. [CrossRef]
22. Alzaqebah, A.; Aljarah, I.; Al-Kadi, O.; Damaševičius, R. A modified grey wolf optimization algorithm for an intrusion detection system. *Mathematics* **2022**, *10*, 999. [CrossRef]

23. Toldinas, J.; Venčkauskas, A.; Damaševičius, R.; Grigaliūnas, Š.; Morkevičius, N.; Baranauskas, E. A novel approach for network intrusion detection using multistage deep learning image recognition. *Electronics* **2021**, *10*, 1854. [CrossRef]
24. Shao, L.; Chen, W. Coal and Gas Outburst Prediction Model Based on Miceforest Filling and PHHO–KELM. *Processes* **2023**, *11*, 2722. [CrossRef]
25. Shan, L.; Liu, Y.; Tang, M.; Yang, M.; Bai, X. CNN-BiLSTM hybrid neural networks with attention mechanism for well log prediction. *J. Pet. Sci. Eng.* **2021**, *205*, 108838. [CrossRef]
26. Deng, S.; Pan, H.-Y.; Wang, H.-G.; Xu, S.-K.; Yan, X.-P.; Li, C.-W.; Peng, M.-G.; Peng, H.-P.; Shi, L.; Cui, M.; et al. A hybrid machine learning optimization algorithm for multivariable pore pressure prediction. *Pet. Sci.* **2023**. [CrossRef]
27. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Gener. Comput. Syst.* **2019**, *100*, 779–796. [CrossRef]
28. Katib, I.; Ragab, M. Blockchain-Assisted Hybrid Harris Hawks Optimization Based Deep DDoS Attack Detection in the IoT Environment. *Mathematics* **2023**, *11*, 1887. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.