SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V10I4P108

Volume 10 Issue 4, 77-90, April 2023

Original Article

Moth Search Optimizer with Deep Learning Enabled Intrusion Detection System in Wireless Sensor Networks

C. Murugesh[1], S. Murugan[2]

[1]*Department of Computer and Information Science, Annamalai University, Annamalai Nagar*
[2]*Dr. M.G.R. Government Arts and Science College for Women, Villupuram.*

[1]*Corresponding Author : 78murugesh@gmail.com*

Received: 28 February 2023 Revised: 29 March 2023 Accepted: 13 April 2023 Published: 27 April 2023

Abstract – *The latest wireless sensor network (WSN) developments in critical applications have introduced security risks, like jamming. Intrusion Detection System (IDS) in WSN is the method of recognizing malevolent or unauthorized activities in the network. The intruder's presence to launch different attacks within the network cannot be disregarded. Despite a great deal of effort by the researcher workers, IDS still experienced difficulties enhancing recognition performance while minimizing the false alarm rate and identifying novel intrusions. Recently, Deep Learning (DL) and Machine Learning (ML) based IDS system has been deployed as promising solution to effectively identify intrusion across the network. Therefore, the study presents a Moth Search Optimization with DL-based Intrusion Detection (MSODL-ID) method in the WSN. The MSODL-ID technique aims to effectually identify the occurrence of malicious activities or intrusions in the network. To accomplish this, the MSODL-ID technique undergoes two stages of preprocessing: data conversion and data scaling. In addition, the MSODL-ID technique employs Convolutional Recurrent Neural Network (CRNN) model with a Hopfield layer for intrusion detection purposes. For optimal hyperparameter selection of the CRNN model, the MSO algorithm is used and thereby enhances the classification performance of the CRNN model. The stimulation analysis of the MSODL-ID system is tested by means of Kaggle datasets, and the outcomes exhibit the promising performance of the MSODL-ID system over other current DL approaches.*

Keywords - *Intrusion Detection System, Wireless Sensor Networks, Deep Learning, Security, Moth Search Optimizer.*

1. Introduction

Wireless Sensor Network (WSN) presents a wide range of applications over their reasonably massive number of wireless sensor nodes (SNs) [1]. The nodes in WSN were resource limited in terms of computational capabilities, storage, and communication. Though it has limitations, because of cost and extended coverage WSNs are generally preferred for applications like traffic control, habitat monitoring, home automation, and environment monitoring. Like other networks [2], WSNs are exposed to security menaces because of their dispersed and wireless characteristics [4].

The limited battery power needs less computation to increase the network lifetime, which avoids the disposition of standard security techniques and makes the network susceptible. Invaders can easily use these vulnerable networks and obtain access to the network, which was a main security problem in WSN [5]. Network intrusion detection systems utilized in the WSNs identify intrusions or security attacks and secure the network. IDS were indispensable for authorization, user authentication, and dealing with doubtful actions [6]. In general, intrusions refer to malicious actions to perform unauthorized tasks and obtain network access. IDS secures the network by identifying those malicious unauthorized actions.

To solve these issues, researchers have started to concentrate on framing IDS utilizing ML approaches [7]. ML is a type of Artificial Intelligence (AI) approach that can automatically find valuable data from massive datasets. ML-related IDS can achieve satisfactory detection levels if sufficient training data is accessible [9] and ML methods have sufficient generalizability to find new attacks and attack variants. Also, ML-related IDS do not hinge on field knowledge; thus, it is easy to build and design [10]. Deep learning (DL) refers to a subdivision of ML that could reach outstanding performances. Compared with classical ML approaches [11], DL techniques are better at handling big data. Likewise, DL methods can learn feature representations automatically from raw information and output outcomes; they work in an end-to-end manner and are practical [12]. One notable feature of DL is the deep structure, which has many hidden layers [13, 14, 16].

The study presents a Moth Search Optimization with the DL-based Intrusion Detection (MSODL-ID) method in the WSN. The MSODL-ID technique aims to effectually identify the occurrence of malicious activities or intrusions in the network. To accomplish this, the MSODL-ID technique undergoes two stages of preprocessing: data conversion and data scaling. In addition, the MSODL-ID technique employs Convolutional Recurrent Neural Network (CRNN) model with a Hopfield layer for intrusion detection purposes. For optimal hyperparameter selection of the CRNN model, the MSO algorithm is used, enhancing the classification performance of the CRNN model. The stimulation analysis of the MSODL-ID system is tested by means of the Kaggle dataset.

2. Related Works

Kagade and Jayagopalan [17] intend to set up a new IDS using a DL method. First of all, optimum cluster heads (CHs) have opted amongst the SNs, where the SNs that have maximum energy act as CH. In the presented technique, the selection of CH was assessed effectively through consideration of the energy parameter under the limitations like distance and delay. An innovative technique called Self Improved Sea Lion Optimization (SI-SLnO) method was presented for optimal selection. Muruganandam et al. [19] developed a DL-related feed-forward ANN technique that enables accurate predictions of the k-barrier counting for potential ID and lessening. The four potential characteristics of sensing transmission area, the area of the ROI, many sensors, and sensor sensing areas are utilized to assess and learn the feed-forward ANN method. Otair et al. [20] devised a method to detect intrusions and address feature selection problems utilizing the Grey Wolf Optimization (GWO) combined with PSO to use the optimal values for updating the data of all greys wolf locations. This method preserved the individual's optimum location data by the PSO method that prevented the GWO method from getting trapped in local optima.

Amaran and Mohan [22] presented an innovative optimum SVM (OSVM) related IDS in WSN. The proposed technique contains the fruitful selection of the best kernels in the SVM method using WOA for ID. The usage of OSVM approach is employed for identifying intrusion with potential outputs since the SVM kernel gets converted through WOA, in [25], proposed an optimized collaborative IDS (OCIDS) for WSN. It utilizes an improved ABC optimization method for optimizing the hierarchical IDS employed to WSN by means of the consumption of limited resources and the precision of ID. Also, this presented system optimized the weighted SVM technique for enhancing detection accuracy and reducing false alarm rates.

In [26], the authors presented an innovative, robust network intrusion classifier structure that depends on the improvised Visual Geometry Group (VGG-19) pretrained method for extending the WSN performance. Principally, for training the parameters of VGG-19, the pretrained weights from the ImageNet dataset were used.

Then, a method called a Hybrid DNN related to CNN and LSTM will be used to extract the features from the network traffic dataset and increase the ID accuracy. This VGG19 with the Hybrid CNN-LSTM method uses multi-classification and binary classification to classify assaults as either attacked or normal. Jianjian et al. [27] offer an ID technique modelled as an IDS for WSNs-DoS attacks related to the improved AdaBoost-RBFSVM technique. The effect of training was attained for making the RBF-SVM method the AdaBoost weak classification. Conversely, the eigenspace for the attack is devised afterwards investigating the DoS attack, and the respective IDS was modelled.

3. The Proposed Model

In this research, we have designed an automated IDS using the MSODL-ID model for WSN. The MSODL-ID technique aims to effectually identify the occurrence of malicious activities or intrusions in the network. It follows a three-stage process: preprocessing, CRNN with Hopfield-based intrusion detection, and MSO-based hyperparameter tuning. Figure 1 represents the working process of the MSODL-ID system.

3.1. Data Preprocessing

Initially, the MSODL-ID technique undergoes two stages of preprocessing: data conversion and data scaling. At the time of the data conversion procedure, categorical information can be transformed into numerical values. Next, min-max normalizing is employed to scale the input data. It is widely applied for calculating the similarity degree amongst the points. Consider A as data which is mapped from the data ranges from Amin to Amax, as follows:

$$A_{normalized} = \frac{A-A_{min}}{A_{max}-A_{min}} \quad (1)$$

The employment of min-max normalization guarantees that the feature was extracted at a similar scale.

3.2. Intrusion Detection using CRNN with Hopfield Network

In this work, the MSODL-ID technique exploited the CRNN model with the Hopfield layer for intrusion detection purposes. CNN includes multiple fully connected and convolutional layers [29]. One or more neurons encompass every layer. Every neuron evaluates the weight afterwards, getting the value from the feature vectors and later transferring the weight to the following layer. Since language and audio are transferred through waveforms, an RNN transforms information into a pattern defined by human semantics.

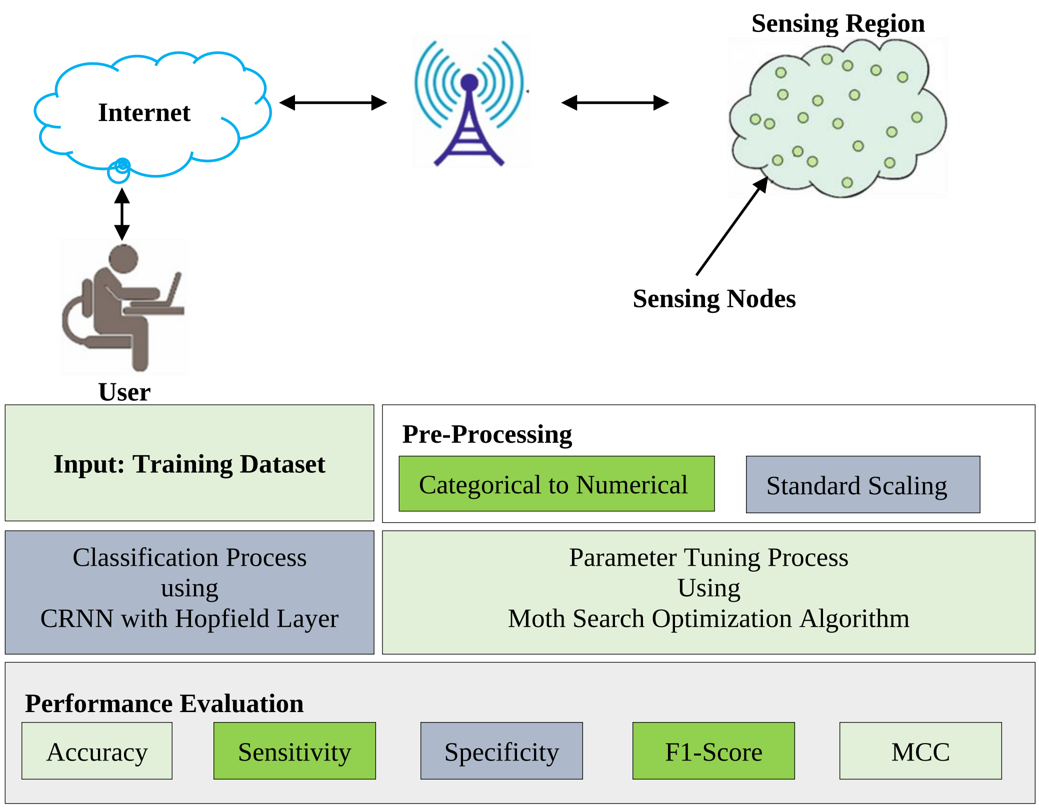

Fig. 1 Working process of MSODL-ID system

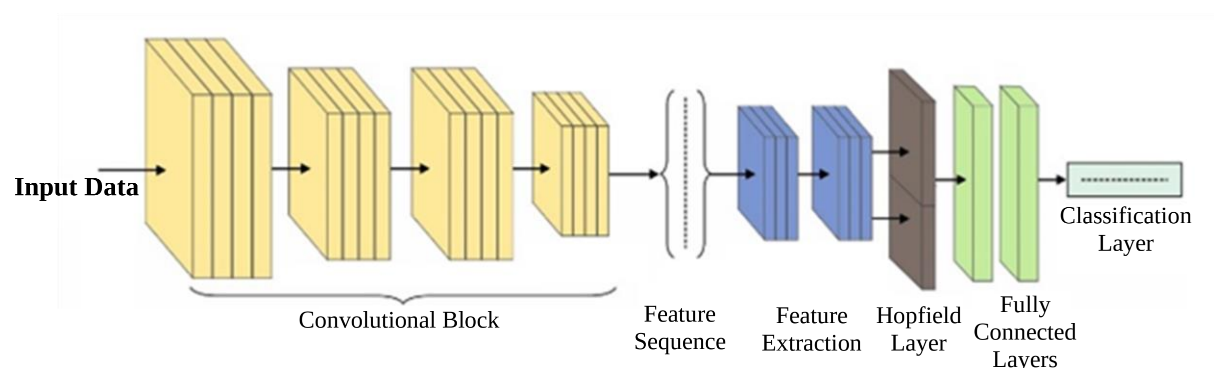

Fig. 2 Architecture of CRNN with hopfield layer

The right side is a diagrammatic representation extended on the time axis, and The left side is the fundamental structure of the model where O_t shows the hidden and the output layers, and I_t indicates the input at time t, respective to H_t. The study incorporates the RNN and CNN methods to present the CRNN employed for intrusion classification in the WSN. The CRNN includes one layer of RNN and four layers of CNN. The 1st layer output is 32, inputted to the 2nd layer afterwards, passing over the maximum pooling layer. The 2nd layer output is 64 and then inputted to the 3rd layer afterwards, passing over the max pooling layer. The 3rd layer output is 128, which is inputted to the subsequent layer afterwards, the max pooling layer. The 4th output layer is 256 and is outputted to the RNN layer. The process of the pooling layer is to increase the computation speed and decrease the computation complexity. The study adopts the max pooling layer that reduces the matrix by taking the largest value, as follows.

$$\mu_\beta \leftarrow \frac{1}{m}\sum_{i=1}^{m} x_i \tag{2}$$

$$\sigma_\beta^2 \leftarrow \frac{1}{m}\sum_{i=1}^{m}\left(x_i-\mu_\beta\right)^2 \tag{3}$$

$$\hat{x}_i \leftarrow \frac{x_i-\mu_\beta}{\sqrt{\sigma_\beta^2+\epsilon}} \tag{4}$$

$$\mathrm{y_i} \leftarrow \gamma\hat{x}_\mathrm{i}+\beta \equiv BN_{\gamma\beta}(x_i) \tag{5}$$

Moreover, Dropout is used to reduce the existence of over-fitting. It is a method utilized in the DL method for reducing over-fitting. Once the training NN is done, it is utilized for randomly disconnecting a few neurons, viz., this neuron does not participate during training. Afterwards, iterated for optimization, every iteration implements this random sampling to create a subnet from the new network. Also, its architecture is not similar to the original network, hence avoiding the overfitting problem. Figure 2 illustrates the structure of CRNN with the Hopfield Layer.

The size of 1st convolution layer is 3233, and then transmitted to the 2nd convolution layer afterwards the Dropout, ReLU function, and the max pooling layer. The size of 2nd convolution layer is 6433, and then transmitted to the 3rd layer afterwards the Dropout, ReLU function, and max pooling layer. The 3rd convolution layer is 12833, then transmitted to the 4th convolution layer afterwards the Dropout, ReLU function, and max pooling layer. The 4th complex layer is 25633 and is sent to the RNN layer after the Dropout, the ReLU function, and the max pooling layer. The RNN layer is 25128 and lastly outputted after being organized by the RNN.

As the parameter of the prior layer changes during training, the distribution of every input layer changes. The internal covariance migration phenomenon needs a low learning rate, resulting in complexity in NN training. To resolve the situation of internal covariant migration, the BN technique can be implemented before the activation function and in every convolution layer.

The ReLU has added every convolution layer, and the function is utilized afterwards. The mathematical formula of Leaky ReLU is given below:

$$y_{\bar{t}} = \begin{cases} X_i, if x_{\mathrm{i}} \geq 0 \\ \frac{x_i}{a_i}, if x_{\mathrm{i}} < 0 \end{cases} \tag{6}$$

Where a_i denotes a fixed parameter between 1 and $+\infty$.

In addition, the Hopfield layer is included in the CRNN model for enhanced results. It is widely known that Hopfield neural network (HNN) simulates and describes brain activities in terms of memory and learning process [30]. In these types of neurons, the circuit equation is defined as follows:

$$C_i \frac{dx_i}{dt} = -\frac{x_i}{R_i} + \sum_{j=1}^{n} w_{i_j} \tanh\left(x_j\right) + I_i \tag{7}$$

In Eq. (7), R_i denotes a resistor based on the membrane robustness between the outside and inside of the neuron. I_i symbolizes the input bias current. $\tanh(x_j)$ denotes the smooth neuron activation function demonstrating the voltage input from the $j\text{-}th$ neurons. x_i denotes the state variable respective to the voltage across the capacitor C_i. The matrix $W = w_{ij}$ is an $n \times n$ synaptic weight matrix. Consider that $C_i = 1, R_i = 1, I_i = 0$ and $n = 4$. The synaptic weight w_{ij} has been chosen using the trial and error method for generating irregular dynamical behaviors.

$$W = \begin{bmatrix} w_{11} & w_{12} & w_{13} & w_{14} \\ w_{21} & w_{22} & w_{23} & w_{24} \\ w_{31} & w_{32} & w_{33} & w_{34} \\ w_{41} & w_{42} & w_{43} & w_{44} \end{bmatrix} = \begin{bmatrix} w_{11} & -6 & 4 & 1 \\ 2 & w_{22} & -1 & 0 \\ -1 & 4 & 1.5 & w_{34} \\ w_{41} & 4 & -5 & 2 \end{bmatrix} \tag{8}$$

The smooth non-linear 4th order differential equation highlights the dynamics of four neurons based Hopfield NNs are considered in a non-dimensional structure as follows:

$$\begin{cases} \dot{x}_1 = -x_1 + w_{11} \tanh(x_1) - 6 \tanh(x_2) + 4 \tanh(x_3) + \tanh(x_4) \\ \dot{x}_2 = -x_2 + 2 \tanh(x_1) + w_{22} \tanh(x_2) + \tanh(x_3) \\ \dot{x}_3 = -x_3 - \tanh(x_1) + 4 \tanh(x_2) + 1.5 \tanh(x_3) + w_{34} \tanh(x_4) \\ \dot{x}_4 = -x_4 + w_{41} \tanh(x_1) + 4 \tanh(x_2) - 5 \tanh(x_3) + 2 \tanh(x_4) \end{cases} \tag{9}$$

3.3. Hyperparameter Tuning using MSO Algorithm

For optimum tuning selection of the CRNN method, the MSO algorithm is used and thereby enhances the classification performance of the CRNN model. Wang proposed an MSO algorithm, a novel swarm intelligence technique that can be stimulated by the most representative features of phototaxis [31], moths and Lévy flights (LFs). The moth has a small distance from the better one and will be flying towards the better individual by LFs. The remaining will fly to the better one in line. The population was split into two subgroups.

The moth in subgroup 1 is nearer to the optimum individual than in subgroup 2. The offspring of subpopulations 1 and 2 are generated by LFs and fly straightly, correspondingly. MS is extensively used for resolving many different problems of complicated optimization in real-time. Despite its wider usage and quick searches with higher accuracy, MS suffer from a poor balance between exploration and exploitation. LF has a random walk with a continuous heavy-tailed distribution. Even though LF enhances the achievement of the MS method, in the later phase of the algorithm, the MS is jumped away from the optimum solution due to its alternative pattern with longer and shorter jumps for LFs. Thus, several researcher workers have developed an MS variant of t to enhance the global search capability.

3.3.1. Lévy Flights

Lévy flight (LF) is a random walking method that fulfils heavy-tailed distribution, making more significant jumps at local locations with higher probability.

Algorithm 1: Pseudocode of MSO algorithm

Begin
Initialization: Random initialization of population of NP moths, the maximum generation Max_Gen;
Determine individuals based on location;
While $T < Max\_Gen$ do
    Arrange every moth based on fitness;
    For $i = 1$ to $NP/2$ (subgroup 1), do
        Determine x_i^{t+1} using Lévy flights;
    End for i
        For $i = NP/2 + 1$ to NP (sub-group 2), do
        If $rand\ > 0.5$ then
            Determine x_i^{t+1} by Eq. (13);
            Else
            Determine x_i^{t+1} by Eq. (14);
        End If
    End for i
    Compute population based on upgraded localization;
$T = T + 1,$
    End while
    Display optimal solution
End

The density likelihood distribution of LF has three fundamental characteristics: sharp peaks, trailing and asymmetry. The moth flies towards the better individual using LF. For every individual i in subpopulation1, the position is upgraded by LFs, as follows.

$$x_i^{t+1} = x_i^t + \alpha L(s) \tag{10}$$

In Eq. (10), x_i^{t+1} denotes the updated location, and x_i^t indicates the original location at t generation. $L(s)$ signifies the step drawn for LFs. α denotes the scalings factor that is shown below:

$$\alpha = \frac{S_{\max}}{t^2} \tag{11}$$

Where $S_{\max}$ specified the max walk step. $L(s)$ can be expressed by:

$$L(s) = \frac{(\beta-1)\Gamma(\beta-1)\sin\left(\frac{\pi(\beta-1)}{2}\right)}{\pi s^{\beta}} \tag{12}$$

In Eq. (12), $L(s)$ denotes the gamma function, and s represents the location of the moth individual that is greater than 0. $\beta = 1.5$.

3.3.2. Fly Straightly

It is noted that phototaxis is moth tends to fly towards the illumination source. The change in angle will be discernible clearly once the moth gets closer towards the illumination source for navigating with the short distancing.

Table 1. Details of database

Class	No. of Samples
Normal	340066
Blackhole	10049
Grayhole	14596
Flooding	3312
Scheduling Attacks	6638
Total Number of Samples	374661

$$x_i^{t+1} = \lambda \times \left(x_i^t + \varphi \times (x_{best}^t - x_i^t)\right) \tag{13}$$

In Eq. (13), φ represent an acceleration factor. x_{besi}^t indicates the better moth at t-th generation. Λ show the scale factor that could control the convergence rate and enhance population diversity. At the same time, once the moth flies further than the illumination source, then the location for moth i can be expressed by:

$$x_i^{t+1} = \lambda \times \left(x_i^t + \frac{1}{\phi} \times (x_{best}^t - x_i^t)\right) \tag{14}$$

In Eq. (14), x_{best}^t and x_i^t denote the better and original location for moth i; correspondingly, λ denotes the scaling feature, and ϕ represents the acceleration feature. The MSO approach not only derives a fitness function from achieving the improved achievement of classifying but also determines a +ve integer for characterizing the superior achievement of the solution candidate. The lessening of the classifier error rate is considered the fitness function.

$$fitness(x_i) = ClassifierErrorRate(x_i)$$

$$= \frac{No.of\ misclassified\ samples}{Total\ no.of\ samples} * 100 \tag{15}$$

4. Results and Discussion

In this section, the experimental results analysis of the MSODL-ID method is investigated on the WSN-DS database [32], which encompasses 374661 sampling with five classes, as defined in the below Table 1.

Figure 3 demonstrates the classifier results of the MSODL-ID technique under 80:20 of TRP/TSP. Figure 3a depicts the confusion matrices provided by the MSODL-ID approach under 80% of TRP. The figure indicated that the MSODL-ID model had identified 271533 samples under normal, 7664 samples under BH, 11008 samples under GH, 2618 samples under FD, and 4795 samples under TDMA. Also, Figure 3b illustrates the confusion matrices produced by the MSODL-ID system under 20% of TSP.

The figure indicated that the MSODL-ID approach had identified 67866 samples under normal, 1956 samples under BH, 2703 samples under GH, 609 samples under FD, and 1282 samples under TDMA.

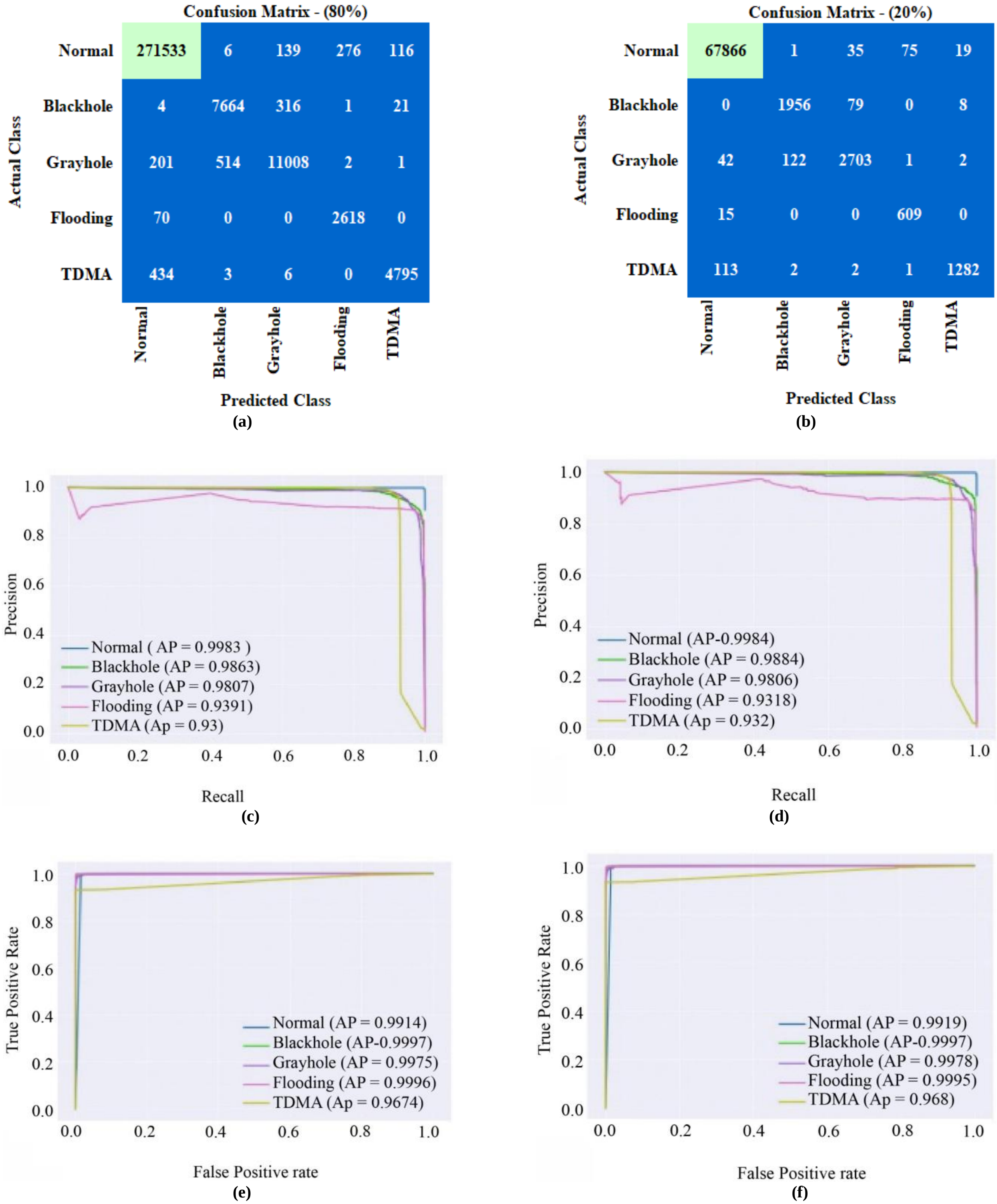

Fig. 3 Results of (80:20) training set a) Confusion matrices b) Confusion matrices c) PR-curve d) PR-curve e) ROC testing set f) ROC

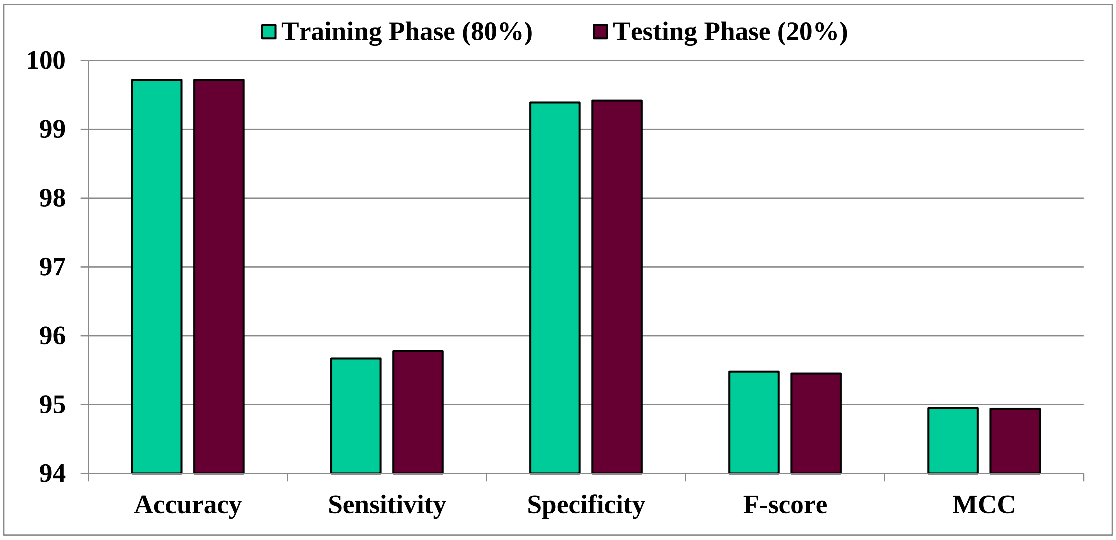

Fig. 4 Average outcome of MSODL-ID approach on 80:20 of TRP/TSP

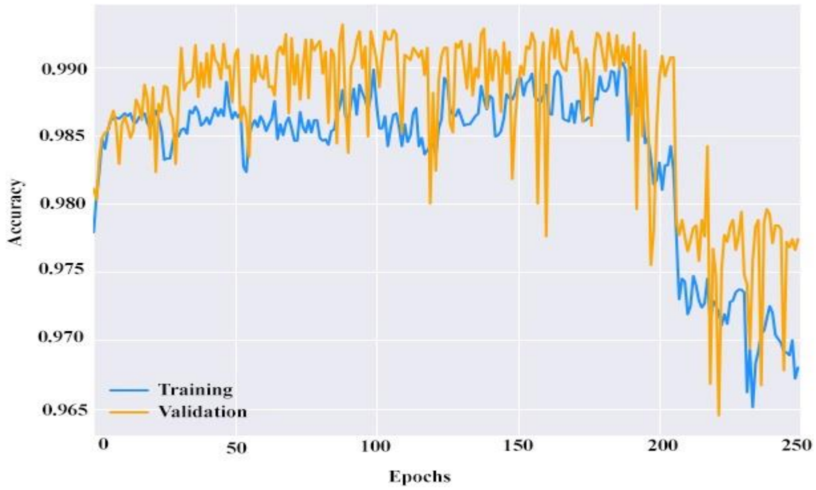

Fig. 5 TACY and VACY outcome of MSODL-ID method on 80:20 of TRP/TSP

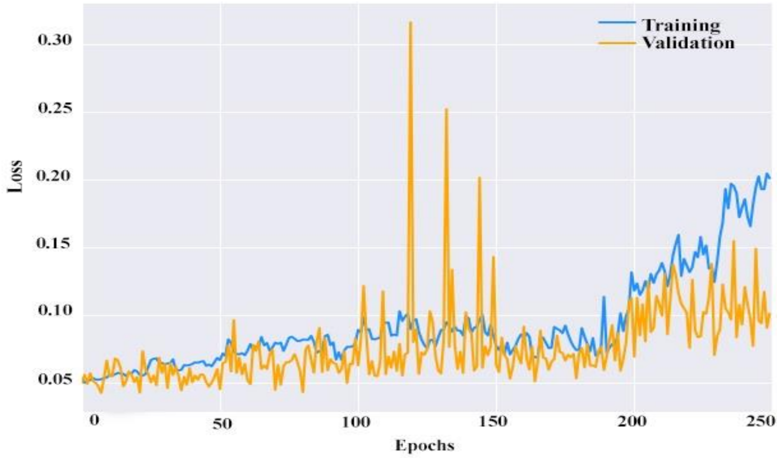

Fig. 6 TLOS and VLOS outcome of MSODL-ID approach on 80:20 of TRP/TSP

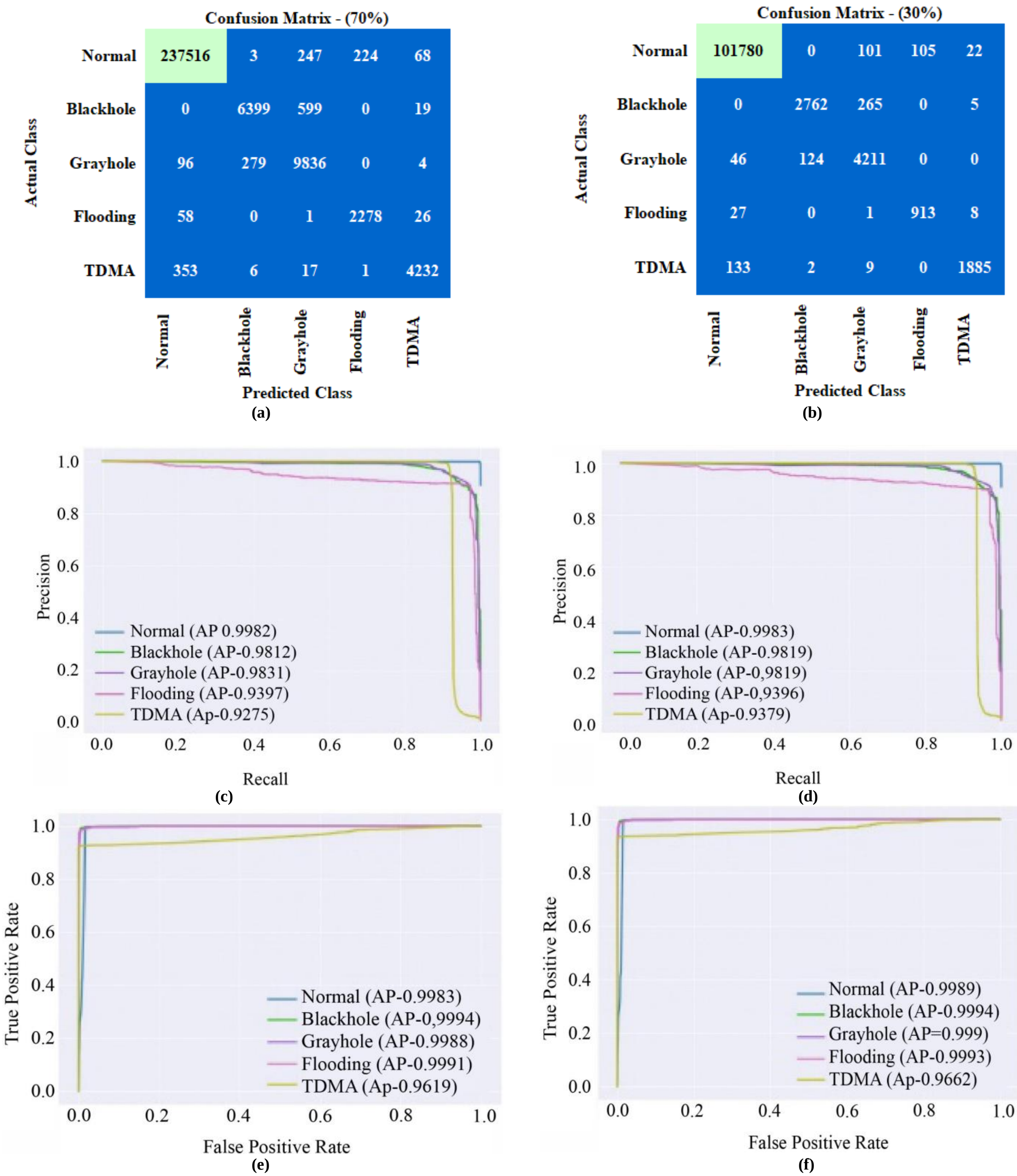

Fig. 7 Results of (70:30) training set a) Confusion matrices b) Confusion matrices c) PR-curve d) PR-curve e) ROC testing Set f) ROC

Table 2. IDS outcome of MSODL-ID method on 80:20 of TRP/TSP

Training / Testing Phase (80:20)					
Labels	$\mathbf{Accu_y}$	$\mathbf{Sens_y}$	$\mathbf{Spec_y}$	$\mathbf{F_{score}}$	**MCC**
Training Phase					
Normal	99.58	99.80	97.44	99.77	97.51
Blackhole	99.71	95.73	99.82	94.66	94.52
Grayhole	99.61	93.88	99.84	94.92	94.72
Flooding	99.88	97.40	99.91	93.75	93.76
TDMA	99.81	91.54	99.95	94.29	94.23
Average	99.72	95.67	99.39	95.48	94.95
Testing Phase					
Normal	99.60	99.81	97.55	99.78	97.61
Blackhole	99.72	95.74	99.83	94.86	94.72
Grayhole	99.62	94.18	99.84	95.03	94.83
Flooding	99.88	97.60	99.90	92.98	93.02
TDMA	99.80	91.57	99.96	94.58	94.53
Average	99.72	95.78	99.42	95.45	94.94

Likewise, Figures 3c-3d exhibits the PR analysis of the MSODL-ID model under 80:20 of TRP/TSP. The figures demonstrated that the MSODL-ID method had attained maximum PR achievement under total classes. Finally, figures 3e-3f illustrate the ROC investigation of the MSODL-ID method under 80:20 of TRP/TSP. The figure portrayed that the MSODL-ID technique has given an outcome in superior outcomes with higher ROC values under various class labels.

In Table 2 and Figure 4, the IDS outputs of the MSODL-ID technique are reported for 80:20 of TRP/TSS. The results reveal that the MSODL-ID technique accurately recognizes all different types of attacks. For instance, with 80% of TRP, the MSODL-ID technique gains an average $accu_y$ of 99.72%, $sens_y$ of 95.67%, $spec_y$ of 99.39%, F_{score} of 95.48%, and MCC of 94.95%. Meanwhile, with 20% of TSP, the MSODL-ID technique gains an average $accu_y$ of 99.72%, $sens_y$ of 95.78%, $spec_y$ of 99.42%, F_{score} of 95.45%, and MCC of 94.94%.

The TACY and VACY of the MSODL-ID method on 80:20 of TRP/TSP have been defined in Figure 5. The figure indicated that the MSODL-ID approach had exhibited improved achievement with maximum TACY and VACY values. It is evident that the MSODL-ID method has obtained higher TACY outcomes.

The TLOS and VLOS of the MSODL-ID method on 80:20 of TRP/TSP have been defined in Figure 6. The figure concluded that the MSODL-ID approach had illustrated improved achievement with minimum TLOS and VLOS values. It is evident that the MSODL-ID method has given an outcome in lesser VLOS.

Table 3. IDS outcome of MSODL-ID method on 70:30 of TRP/TSP

Training / Testing Phase (70:30)					
Labels	$\mathbf{Accu_y}$	$\mathbf{Sens_y}$	$\mathbf{Spec_y}$	$\mathbf{F_{score}}$	**MCC**
Training Phase					
Normal	99.60	99.77	97.91	99.78	97.61
Blackhole	99.65	91.19	99.89	93.39	93.24
Grayhole	99.53	96.29	99.66	94.06	93.84
Flooding	99.88	96.40	99.91	93.63	93.61
TDMA	99.81	91.82	99.95	94.49	94.43
Average	99.69	95.09	99.46	95.07	94.55
Testing Phase					
Normal	99.61	99.78	98.02	99.79	97.70
Blackhole	99.65	91.09	99.88	93.31	93.16
Grayhole	99.51	96.12	99.65	93.91	93.69
Flooding	99.87	96.21	99.91	92.83	92.83
TDMA	99.84	92.90	99.97	95.47	95.42
Average	99.70	95.22	99.49	95.06	94.56

Figure 7 demonstrates the classifier results of the MSODL-ID technique under 70:30 of TRP/TSP. Figure 7a depicts the confusion matrices provided by the MSODL-ID technique under 70% of TRP. The figure indicated that the MSODL-ID model had identified 237516 samples under normal, 6399 samples under BH, 9836 samples under GH, 2278 samples under FD, and 4232 samples under TDMA. Also, Figure 7b illustrates the confusion matrices produced by the MSODL-ID system under 30% of TSP.

The figure indicated that the MSODL-ID technique had identified 101780 samples under normal, 2762 samples under BH, 4211 samples under GH, 913 samples under FD, and 1885 samples under TDMA. Similarly, Figures. 7c-7d exhibits the PR analysis of the MSODL-ID method under 70:30 of TRP/TSP. The figures demonstrated that the MSODL-ID method had attained maximum PR achievement under total classes. Lastly, Figures 7e-7f illustrate the ROC inspection of the MSODL-ID method under 70:30 of TRP/TSP. The figure exhibited that the MSODL-ID method has given an outcome in superior outcomes with high ROC values under various class labels.

In Table 3 and Figure 8, the IDS results of the MSODL-ID technique are reported for 70:30 of TRP/TSS. The outcomes reveal that the MSODL-ID method accurately recognizes all different types of attacks. For instance, with 70% of TRP, the MSODL-ID method gains an average $accu_y$ of 99.69%, $sens_y$ of 95.09%, $spec_y$ of 99.46%, F_{score} of 95.07%, and MCC of 94.55%. Meanwhile, with 30% of TSP, the MSODL-ID method gains an average $accu_y$ of 99.70%, $sens_y$ of 95.22%, $spec_y$ of 99.49%, F_{score} of 95.06%, and MCC of 94.56%.

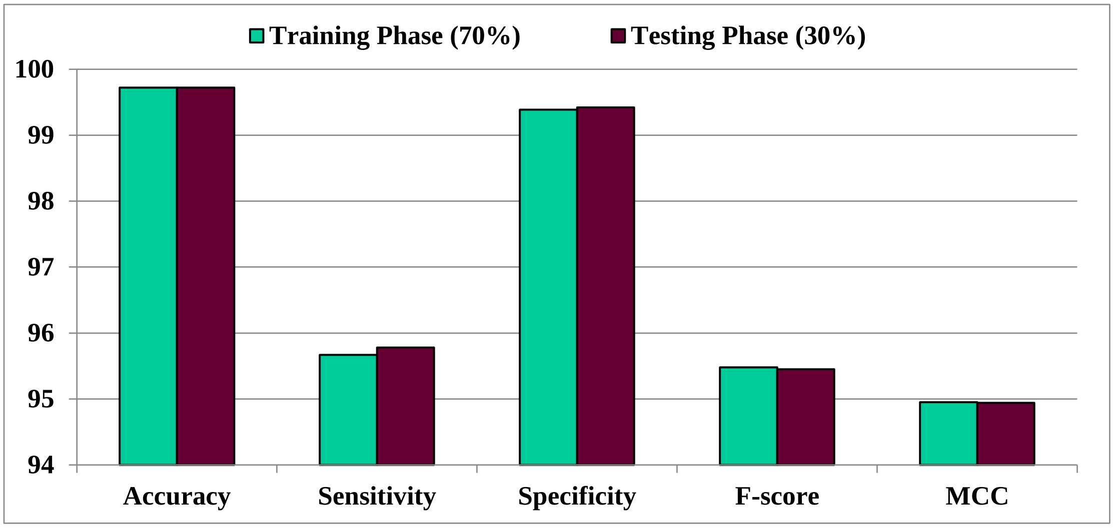

Fig. 8 Average outcome of MSODL-ID approach on 70:30 of TRP/TSP

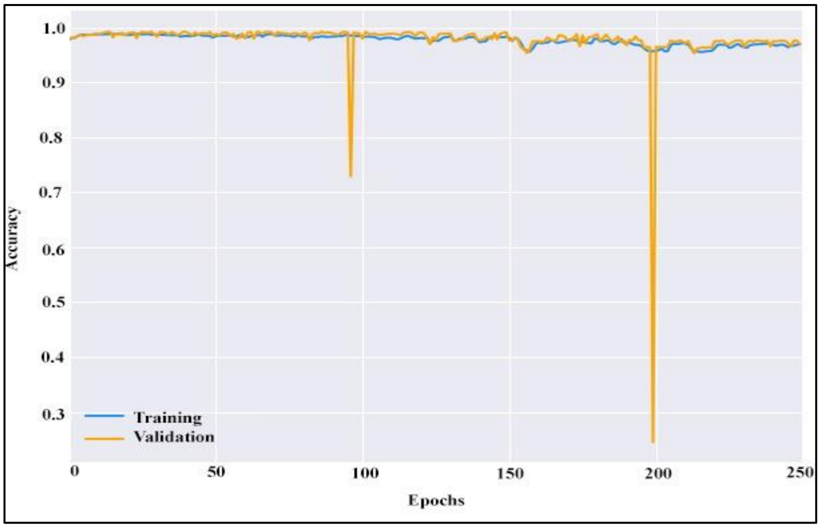

Fig. 9 TACY and VACY outcome of MSODL-ID method on 70:30 of TRP/TSP

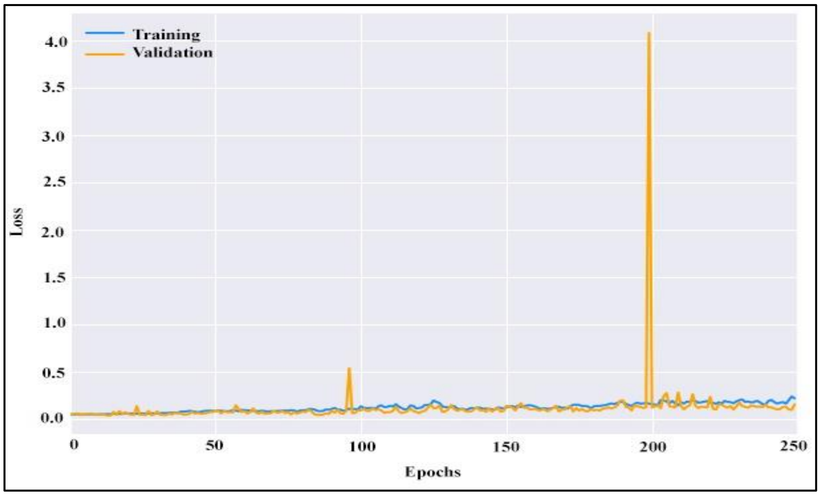

Fig. 10 TLOS and VLOS outcome of MSODL-ID method on 70:30 of TRP/TSP

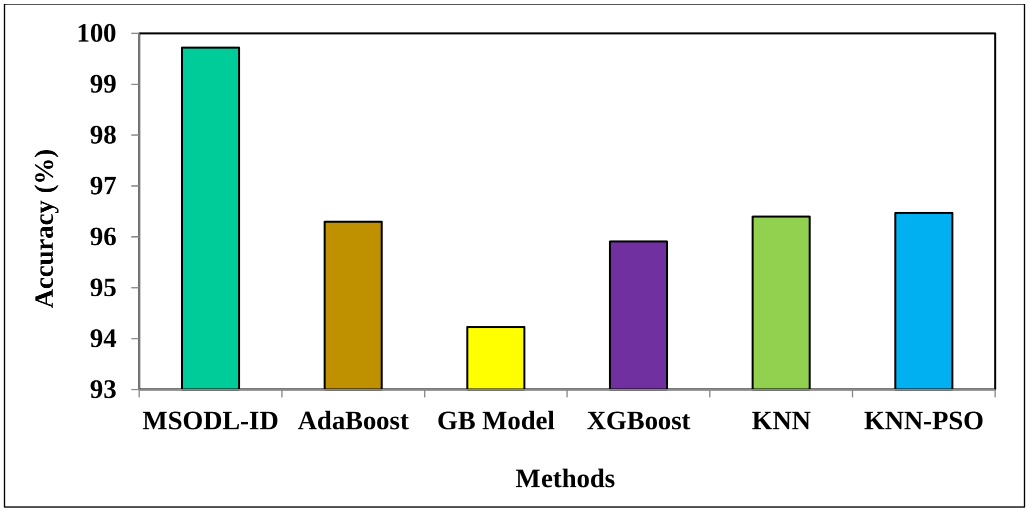

Fig. 11 $Accu_y$ outcome of MSODL-ID technique with other IDS methods

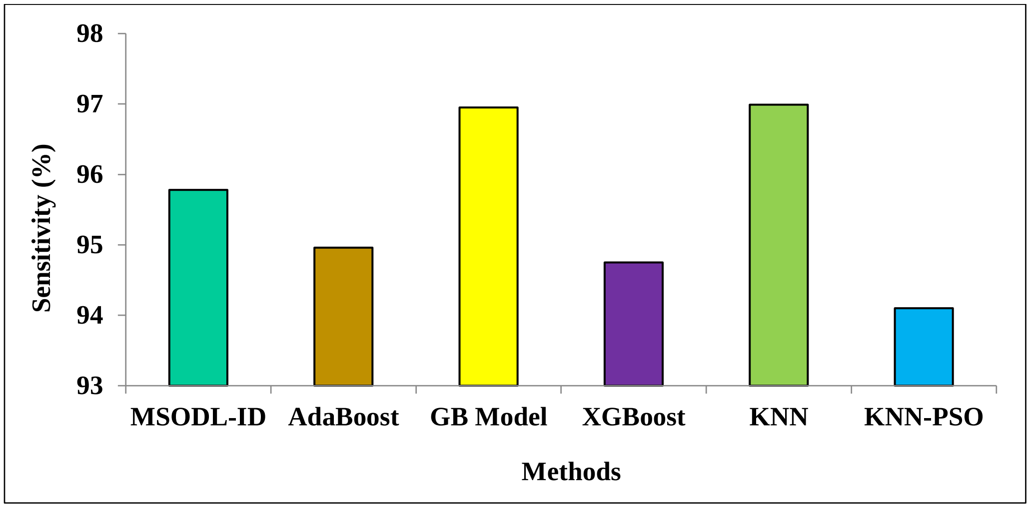

Fig. 12 $Sens_y$ outcome of MSODL-ID technique with other IDS methods

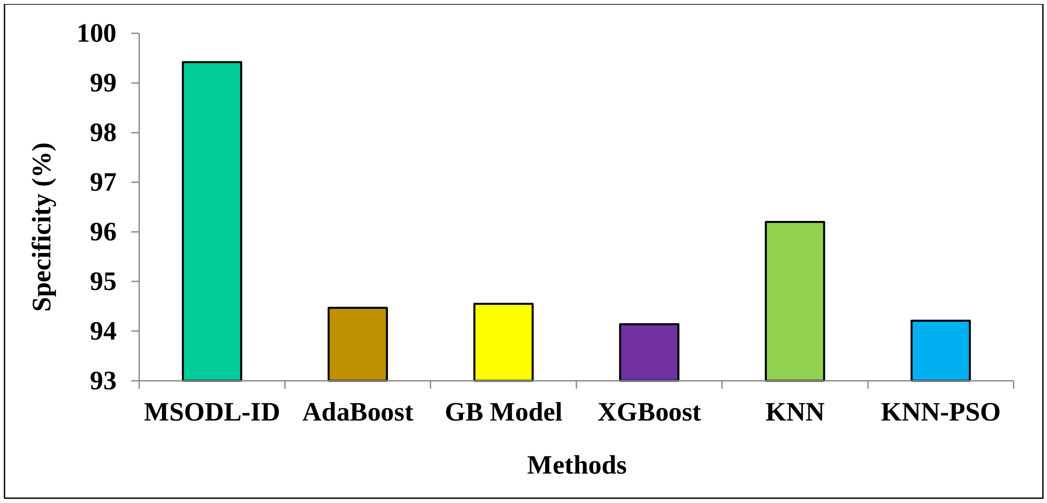

Fig. 13 $Spec_y$ outcome of MSODL-ID technique with other IDS methods

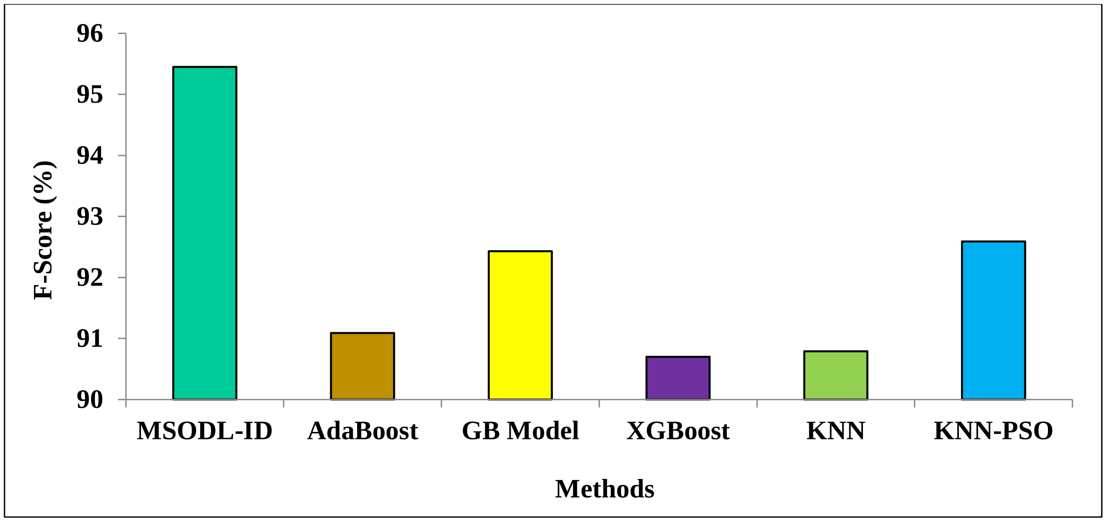

Fig. 14. F_{score} outcome of MSODL-ID technique with other IDS methods

Table 4. Comparative outcome of MSODL-ID approach with other IDS techniques

Methods	$Accu_y$	$Sens_y$	$Spec_y$	F_{score}
MSODL-ID	99.72	95.78	99.42	95.45
AdaBoost	96.30	94.96	94.47	91.09
GB Model	94.23	96.95	94.55	92.43
XGBoost	95.91	94.75	94.14	90.70
KNN	96.40	96.99	96.20	90.79
KNN-PSO	96.47	94.10	94.21	92.59

The TACY and VACY of the MSODL-ID method on 70:30 of TRP/TSP are defined in Figure 9. The figure is implicit that the MSODL-ID model has exhibited maximum achievement with improved TACY and VACY values. It is evident that the MSODL-ID method has given an outcome in higher TACY.

The TLOS and VLOS of the MSODL-ID method on 70:30 of TRP/TSP are defined in Figure 10. The figure represents that the MSODL-ID model has exhibited maximum achievement with the lower TLOS and VLOS values. It is evident that the MSODL-ID approach has given an outcome in minimum VLOS.

Table 4 deliberates the comparison results of the MSODL-ID technique with other IDS models [28, 33]. In Figure 11, a relative $accu_y$ assessment of the MSODL-ID approach is made.

The experimental outcomes imply that the GB model shows a lower $accu_y$ of 94.23%, while the XGBoost model reaches a slightly improvised $accu_y$ of 95.91%. Concurrently, the AdaBoost, KNN, and KNN-PSO models accomplish moderately closer $accu_y$ of 96.30%, 96.40%, and 96.47% correspondingly. But the MSODL-ID method gains maximum performance with $an\ accu_y$ of 99.72%.

In Figure 12, a relative $sens_y$ assessment of the MSODL-ID method is made. The experimental outcomes imply that the KNN-PSO method shows a lower $sens_y$ of 94.10%, while the XGBoost model reaches a slightly improvised $sens_y$ of 94.75%. Concurrently, the AdaBoost, GB, and KNN methods achieve moderately closer $sens_y$ of 94.96%, 96.95%, and 96.99%, correspondingly. But the MSODL-ID method gains maximum performance with a $sens_y$ of 95.78%.

In Figure 13, a relative $spec_y$ assessment of the MSODL-ID method is made. The experimental outcomes imply that the XGBoost method reveals a lower $spec_y$ of 94.14%, while the KNN-PSO method obtains a slightly improvised $spec_y$ of 94.21%. Concurrently, the AdaBoost, GB, and KNN models achieve moderately closer $spec_y$ of 94.47%, 94.55%, and 96.20%, correspondingly. But the MSODL-ID method gains maximum performance with a $spec_y$ of 99.42%.

In Figure 14, a relative F_{score} assessment of the MSODL-ID technique is made. The experimental outcomes show that the XGBoost model shows a lower F_{score} of 90.70%, whereas the KNN model reaches a slightly improvised F_{score} of 90.79%. Concurrently, the AdaBoost, GB, and KNN-PSO models achieve moderately closer F_{score} of 91.09%, 92.43%, and 92.59%, correspondingly. But the MSODL-ID method gains maximum performance with $a\ F_{score}$ of 95.45%. These results assured the supremacy of the MSODL-ID technique on the intrusion detection process in WSN.

5. Conclusion

In this study, we have designed an automated intrusion detection technique using the MSODL-ID model for WSN. The MSODL-ID technique aims to effectually identify the occurrence of malicious activities or intrusions in the network. It follows a three-stage process: preprocessing, CRNN with Hopfield-based intrusion detection, and MSO-based hyperparameter tuning. Initially, the MSODL-ID technique undergoes two stages of preprocessing: data conversion and data scaling. Next, the MSODL-ID technique exploited the CRNN model with the Hopfield layer for intrusion detection purposes. The MSO algorithm is used for optimum hyperparameter selection of the CRNN model and thereby enhances the classification performance of the CRNN model. The simulation analysis of the MSODL-ID system is tested by means of Kaggle datasets, and the outcomes exhibit the promising performance of the MSODL-ID system over other recent DL techniques. In future, the feature selection process can be designed to increase the performance of the MSODL-ID technique.

References

[1] Sumit Pundir et al., “Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges,” *IEEE Access*, vol. 8, pp. 3343-3363, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Aftab Alam Abdussami, and Mohammed Faizan Farooqui, “Incremental Deep Neural Network Intrusion Detection in Fog Based IOT Environment: An Optimization Assisted Framework,” *Indian Journal of Computer Science and Engineering*, vol. 12, no. 6, pp. 1847-1859, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] N.V.L. Ch.Satya Keerthi et al., "Intrusion Detection System Using Genetic Algorithm," *International Journal of P2P Network Trends and Technology*, vol. 1, no. 2, pp. 1-7, 2011. [Publisher Link]

[4] Weidong Fang et al., “TMSRS: Trust Management-Based Secure Routing Scheme in Industrial Wireless Sensor Network with Fog Computing,” *Wireless Networks*, vol. 26, no. 5, pp.3169-3182, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Nausheen Sahar, Ratnesh Mishra, and Sidra Kalam, “Deep Learning Approach-Based Network Intrusion Detection System for Fog-Assisted IoT,” *In Proceedings of International Conference on Big Data, Machine Learning and Their Applications*, pp. 39-50, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Md Arafatur Rahman et al., “Scalable Machine Learning-Based Intrusion Detection System for IoT-Enabled Smart Cities,” *Sustainable Cities and Society*, vol. 61, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Sohail Saif et al., “HIIDS: Hybrid Intelligent Intrusion Detection System Empowered with Machine Learning and Metaheuristic Algorithms for Application in IoT Based Healthcare,” *Microprocessors and Microsystems*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Phyu Thi Htun, and Kyaw Thet Khaing, “Anomaly Intrusion Detection System using Random Forests and k-Nearest Neighbor,” *International Journal of P2P Network Trends and Technology* , vol. 3, no. 1, pp. 39-43, 2013. [Google Scholar] [Publisher Link]

[9] Thavavel Vaiyapuri et al., “Deep Learning Approaches for Intrusion Detection in IIoT Networks–Opportunities and Future Directions,” *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 4, pp. 86-92, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] M.P. Ramkumar et al., “Intrusion Detection Using Optimized Ensemble Classification in Fog Computing Paradigm,” *Knowledge-Based Systems*, vol. 252, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Cristiano Antonio de Souza et al., “Intrusion Detection and Prevention in Fog Based IoT environments: A Systematic Literature Review, *Computer Networks*, vol. 214, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Victor Chang et al., “A Survey on Intrusion Detection Systems for Fog and Cloud Computing,” *Future Internet*, vol. 14, no. 3, pp. 89, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Maamar Ali Saud AL Tobi et al., “Machinery Faults Diagnosis using Support Vector Machine (SVM) and Naïve Bayes classifiers,” *International Journal of Engineering Trends and Technology*, vol. 70, no. 12, pp. 26-34, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] S. Shashikala, and G. K. Ravikumar, "Deep Studying Signature for Obstruction obscure in Copy Move Image Forgeries," *International Journal of Engineering Trends and Technology*, vol. 70, no. 10, pp. 262-270, 2022. [CrossRef] [Publisher Link]

[15] S. Revathi, and A. Malathi."Network Intrusion Detection Using Hybrid Simplified Swarm Optimization Technique," *International Journal of P2P Network Trends and Technology*, vol. 3, no. 5, pp. 6-10, 2013. [Google Scholar] [Publisher Link]

[16] Stanislav Yamashkin et al., "Metageosystem Analysis Based on a System of Machine Learning and Simulation Algorithms," *International Journal of Engineering Trends and Technology*, vol. 70, no. 12, pp. 1-12, 2022. [CrossRef] [Publisher Link]

[17] Ranjeet B. Kagade, and Santhosh Jayagopalan, “Optimization Assisted Deep Learning Based Intrusion Detection System in Wireless Sensor Network with Two-Tier Trust Evaluation,” *International Journal of Network Management*, vol. 32, no. 4, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Pooja Manisha, and Yudhvir Singh, "Security Issues and Sybil Attack in Wireless Sensor Networks," *International Journal of P2P Network Trends and Technology (IJPTT)*, vol. 3, no. 1, pp. 1-6, 2013. [Google Scholar] [Publisher Link]

[19] S. Muruganandam et al., “A Deep Learning Based Feed Forward Artificial Neural Network to Predict The K-Barriers for Intrusion Detection Using a Wireless Sensor Network,” *Measurement: Sensors*, vol. 25, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Mohammed Otair et al., "An Enhanced Grey Wolf Optimizer Based Particle Swarm Optimizer for Intrusion Detection System in Wireless Sensor Networks," *Wireless Networks*, vol. 28, no. 2, pp.721-744, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] R. Surendiran, and K. Alagarsamy, "A Crtitical Approach for Intruder Detection in Mobile Devices," *SSRG International Journal of Computer Science and Engineering*, vol. 1, no. 4, pp.6-14, 2014. [CrossRef] [Publisher Link]

[22] Sibi Amaran, and R. Madhan Mohan, "Intrusion Detection System Using Optimal Support Vector Machine for Wireless Sensor Networks," *International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, pp. 1100-1104, 2021. [Google Scholar] [Publisher Link]

[23] S. Gavaskar, E. Ramaraj, and R. Surendiran, "A Compressed Anti IP Spoofing Mechanism Using Cryptography," *IJCSNS International Journal of Computer Science and Network Security*, vol. 12, no. 11, pp.137-140, 2012. [Google Scholar] [Publisher Link]

[24] Ch. Mounika, and Ch. Suresh Babu, "A Novel Security Based Data Transmission Protocol for Cluster Based Wireless Sensor Networks," *International Journal of Computer and organization Trends*, vol. 6, no. 1, pp. 1-7, 2016. [CrossRef] [Publisher Link]

[25] Shaimaa Ahmed Elsaid, and Nouf Saleh Albatati, "An Optimized Collaborative Intrusion Detection System for Wireless Sensor Networks," *Soft Computing*, vol. 24, no. 16, pp.12553-12567, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[26] P. Manjula, Priya, and S.Baghavathi, "An Effective Network Intrusion Detection and Classification System for Securing WSN using VGG-19 and Hybrid Deep Neural Network Techniques," *Journal of Intelligent & Fuzzy Systems*, vol. 43, no. 5, pp.1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] Dai Jianjian, Tao Yang, and Yang Feiyue, "A Novel Intrusion Detection System Based on IABRBFSVM for Wireless Sensor Networks," *Procedia Computer Science*, vol. 131, pp.1113-1121, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[28] Mnahi Alqahtani et al., "A Genetic-Based Extreme Gradient Boosting Model for Detecting Intrusions in Wireless Sensor Networks," *Sensors*, vol. 19, no. 20, pp. 4383, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[29] Yu-Huei Cheng et al., "Automatic Music Genre Classification Based on CRNN," *Engineering Letters*, vol. 29, no. 1, pp. 312-316, 2021. [Google Scholar] [Publisher Link]

[30] Z. Tabekoueng Njitacke, J. Kengne, and H.B. Fotsin, "Coexistence of Multiple Stable States and Bursting Oscillations in a4d Hopfield Neural Network," *Circuits, Systems, and Signal Processing*, vol. 39, pp.3424-3444, 2020. [CrossRef] [Publisher Link]

[31] K. Shankar, Eswaran Perumal, and R. M. Vidhyavathi, "Deep Neural Network with Moth Search Optimization Algorithm Based Detection and Classification of Diabetic Retinopathy Images," *SN Applied Sciences*, vol. 2, no. 748, pp.1-10, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[32] Iman Almomani, Bassam Al-Kasasbeh, and Mousa AL-Akhras, "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," *Journal of Sensors*, vol. 2016, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[33] Gaoyuan Liu et al., "An Enhanced Intrusion Detection Model Based on Improved kNN in WSNs," *Sensors,* vol. 22, no. 4, pp. 1407, 2022. [CrossRef] [Google Scholar] [Publisher Link]