SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V10I5P106

Volume 10 Issue 5, 62-75, May 2023

Original Article

Artificial Ecosystem Optimizer with Convolutional Recurrent Neural Network for 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: 06 March 2023 Revised: 11 April 2023 Accepted: 07 May 2023 Published: 31 May 2023

Abstract *- Wireless Sensor Network (WSN) encompasses Sensor Nodes (SNs) used to gather data regarding surroundings. Some features that make WSNs vulnerable to security attacks are open wireless medium, distributed nature, and multi-hop data forwarding. Several security-based solutions for WSNs were devised, like secure routing or security mechanisms, authentication, and key exchange for particular attacks. Such security mechanisms can ensure security at a certain level but cannot eradicate various security attacks. Intrusion Detection System (IDS) was crucial in preventing and detecting security attacks. This study develops an Artificial Ecosystem Optimizer with Convolutional Recurrent Neural Network for IDS (AEOCRNN-IDS) in WSN. The main aim of the AEOCRNN-IDS model lies in recognising and classifying intrusions present in the network. Data preprocessing is done in the suggested AEOCRNN-IDS model to make the data compatible for further processing. The AEOCRNN-IDS approach uses the CRNN technique in this study for intrusion detection and classification. Since hit-and-miss tuning selection is a dreary process, the AEOCRNN-IDS approach implements the AEO method for optimal tuning. The experimental validation of the AEOCRNN-IDS system was tested employing an intrusion database from the Kaggle repository. The extensive experimental analysis stated the authority of the AEOCRNN-IDS approach on IDS in the WSN.*

Keywords *- Wireless Sensor Networks, Intrusion detection system, Security, Deep learning, Artificial ecosystem optimizer.*

1. Introduction

WSNs are not similar to the classical computer network, but it connects SN through radio networks deprived of a centralized control model [1]. It is the same as distributed transmission in which neighbourhood nodes can be handled by all nodes in a system. This network can be applied in various atmospheres, mostly overhead water monitoring mechanisms [2]. It can be formulated and exposed to some assaults in a collaborative environment. This is due to the broad Internet usage and the several security issues in several DoS formats [3, 4]. It has been the primary concern of each network security issue as it produces enormous volumes of data traffic for exhausting all targeted sources of the system and inactivating the transmission link by halting the server in processing legal requests for users to do transactions [5].

The DDOS operable computational sources were memory, the computer's processing unit, and network bandwidth. Its capacity has beaten the transmission channels. If DDOS is started, unnecessary traffic data floods the targeted channel into a transmission connection [6, 7]. Sometimes, assault intends to have a network node inoculating more unnecessary requests with every communication link to the node.

The Intrusion Detection System (IDS) was introduced by Denning in 1987; after that, with several developments and optimized techniques enforced on it [8], IDS proved an effective technology for confronting cyberattacks. IDS is classified into two classes: network-based and host-based, based on the location of the IDS modules in the network [9, 10].

A host-related IDS analyzes and monitors application actions for devices running on network and system configurations. The benefit of a host-related IDS is that it scrutinizes historical datasets to find savvy intruders that use unconventional techniques, which seems to be tough to find in real-time [15]. However, it includes disadvantages: it consumes memory, processing time, other resources, and host storage [16]. It may observe an extensive network with

minimal utilization, but at the same time, it has an optimally-grained recognition capability [17]. DL techniques for ID have been studied by numerous authors in recent years [18]. The vast network data made ID issues agreeable to deep learning (DL) techniques.

This study develops an Artificial Ecosystem Optimizer with Convolutional Recurrent Neural Network for IDS (AEOCRNN-IDS) in WSN. The main aim of the AEOCRNN-IDS model lies in recognising and classifying intrusions in the network. Data preprocessing is done in the suggested AEOCRNN-IDS model to make the data compatible for further processing. The AEOCRNN-IDS approach uses the CRNN technique in this study for intrusion detection and classification. Since hit-and-miss tuning selection is a dreary process, the AEOCRNN-IDS technique implements the AEO method for optimal tuning. The experimental validation of the AEOCRNN-IDS system was tested employing an intrusion database from the Kaggle repository.

2. Related Works

Liu et al. [15] projected a model called WSN intelligent intrusion detection (ID) by introducing the arithmetic optimized algorithm (AOA) in evolutionary computation and introducing the kNN in ML to constitute an edge intelligence structure that mainly executes the IDS whenever the WSN faces a DoS outbreak. To enrich the method's precision, the author used a parallel method to improvise the transmissions among the populace and leverage the Lévy flight method for adjusting the optimizing process. The presented PL-AOA technique efficiently guarantees the enhancement of the kNN technique and is performed effectively in the benchmark function test. In [16], an IDS was demonstrated to assure WSN security. As the anomaly, signature, and misuse-based recognition techniques for IDSs were not sufficient to grant security alone, a hybridized technique has been modelled where such techniques are utilized together. During the hybrid method, anomaly rules are determined for detecting the attack, and RF, ML approaches, J48, and BayesNet are utilized for classifying abnormal and regular traffic.

In [17], the authors present a design that executes a secure remote healthcare model. The author aimed to render a secure structure for remote healthcare methods that preserved the system data securely from common network assaults, which include User to Root (U2R) attacks and DoS. In this way, the author devised an IDS utilizing one of the ML techniques, SVM. Wen et al. [18] modelled an improved convolutional DBN-related ID model (ICDBN_IDM), including a redundancy detection technique related to an achievement investigation policy and the convolutional DBN. The duplication recognition may remove ineffective data and nodes and save the whole network's energy consumption. Shakya [19] presented an integration of ML and a modified MLGWO algorithm to formulate an enhanced IDS. The false alarm rates can be minimized in the WSN by reducing the processing period while enhancing the accuracy of ID and rate of detection by decreasing the resultant features.

[20], presented a new T-Distributed Stochastic Neighbour Embedding and RF method for classifying cyberattacks. This method includes 3 three steps. Firstly, the inspection of feature correlations was offered. Secondly, used a technique called the T-SNE data dimensional reduction. Benaddi et al. [21] modelled a new DRL-related IDS for IoTs and WSNs that utilizes the Markov Decision Process formalism to enrich the performance of IDS decisions. To assess the system achievement, the author compared the baseline standard of usual RL and the supervised technique of ML-KNN.

3. The Proposed Model

In this research, we have developed a novel AEOCRNN-IDS system for recognizing and classifying intrusions in the network. Three operation stages in the proposed AEOCRNN-IDS model occur data preprocessing, CRNN-based classification, and the AEO-based tuning process. Fig. 1 exhibits the comprehensive procedure of the AEOCRNN-IDS methodology.

3.1. Data Preprocessing

In the proposed AEOCRNN-IDS model, data preprocessing is performed to make the data compatible for further processing. Initially, the data transformation process occurs when the categorical data is converted into numerical data. Then, the data scaling process is performed using Min-Max normalization. It executed a linear alteration on the original dataset. $MaxA$ and $MinA$ are the maximum and minimum values of an attribute A. Min-Max normalized mapped values ofA to v' in the range by calculating $new\_MinA,\ new\_MaxA$. The threshold value for the Min-Max range was set as zero and one.

$$\mathrm{V}' = \frac{\mathrm{V} - \mathrm{Min\ A}}{\mathrm{Max\ A} - \mathrm{Min\ A}} (\mathrm{new\_MaxA} - \mathrm{new\_MinA}) + \mathrm{new\_MinA} \tag{1}$$

3.2. Intrusion Detection by Utilizing CRNN Model

The AEOCRNN-IDS methodology uses the CRNN technique in this study to recognise and classify intrusion. The CRNN model significantly increases the receptive field's size and can adaptively capture global features with sequential information and local features with rich semantics [22]. The CRNN model involves two significant elements. Extracting local features with CNN and recurrent connection local aspects to make global factors with time-sequence data. Fig. 2 illustrates the framework of the RNN method.

The CNN part is initially employed for handling input vibrating signals processed by variance normalized and mean

subtraction. This part follows fundamental principles that CNN consisted of alternatively stacking pooling and convolutional layers. The residual block architecture and batch normalization technique are applied to accelerate convergence and network training. The CNN section involves four residual blocks and involves two convolutional layers. Each residual block subsample its input. Note that these CNN parts' first and last layers are specially developed due to adopted pre-activation blocks.

Every feature in CNN covers around 901 sample points of novel vibration signal, representing that extracting feature was local and without sequential data. Next, the LSTM is integrated to manage the sequenced local feature for overcoming the shortcomings of CNN. The LSTM input in every timestamp is one feature point from the CNNs final layer, unlike the conventional RNN-based technique that utilizes features. Next, the hidden state of LSTM was calculated.

Finally, a given loss function can determine the optimization and update of network parameters. The trained set was composed of network data over its life cycles. It is represented as $\{(x_t, y_t)|1 \le l \le T\}$, where $x_t \in R^N$, $y_t \in [0,1]$ and T signify lifespan. y_t Denotes accurate labelling at t time which indicates the per cent of the remaining lifetime of SN at present. This method is frequently implemented to resolve the problems of threshold ambiguity failing from the domain of data-driven HI architecture. Finally, threshold failure becomes complex to define since the health indicator value of distinct nodes generally has more significant mathematical fluctuation:

$$J = \frac{1}{2}\sum_{t=1}^{T} \| y_t - \widehat{y_t} \|_2^2 \quad (2)$$

In Eq. (2), $\hat{y}_t$ indicates the predicted value. Once the model is given training for all 100 steps under 32 batch sizing, the existing method was estimated on the testing set. This method loss on the testing set was observed from beginning to end.

3.3. Hyperparameter Tuning using AEO Algorithm

The AEOCRNN-IDS technique, the AEO algorithm is employed for optimal hyperparameter tuning. AEO is a populace-based algorithm simulated by energy flow in the ecosystem [23]. Generally, the AEO mechanism is based on Production, Consumption, and Decomposition processes. Production balance exploitation and exploration. Consumption improves exploration. Decomposition enhances exploitation. The ecosystem population consists of producers, consumers, and decomposers. Others are consumers, separated into herbivores, carnivores, and omnivores. The value of the primary function or fitness function can estimate the energy level of every population.

3.3.1. Production

The producers are individuals in the ecosystem which produce food energy with water, sunlight, carbon dioxide and nutrition provided by the decomposer. This process helps AEO produce separate solutions drifting in random locations created to better locations with the rise in iteration. Also, this guides the consumption procedure. Such behaviours significantly contribute to the balance betwixt exploitative and explorative searching. In the following, the production process can be mathematically expressed as,

$$X_1(t+1) = (1-a)X_n(t) + aX_{rand} \quad (3)$$

$$a = \left(1 - \frac{t}{T}\right) r_1 \quad (4)$$

$$X_{rand} = r(U - L) + L \quad (5)$$

From the expression, n represents the populace size. T indicates the maximal iterations, $and\ U,$ and L show the higher and lower bounds of the search space where a indicates the weight coefficient. r_1 and r are randomly generated values within [0,1]. X_{rand} shows the location of the individual that is arbitrarily generated in the searching space. $X_1(t+1)$ represents the preceding formula.

3.3.2. Consumption

After the producer achieves production operators, every consumer acts on the consumption feature. All the consumers eat consumer or producer with the lowest energy even if it can consume both. Herbivore only eats producers. Likewise, carnivores only eat users with the highest energy level, and omnivores could eat consumers and producers. The consuming technique enables AEO to update the solution separately, which concerns the arbitrarily selected individual solution with the highest energy level, the solution given by the producer, or both. The random integer $b \in [0,1]$ is generated. When the b value lies between 1/3 to 2/3, the consumption efficiency utilises the Omnivore. If b is less than 1/3, the efficacy of Herbivore could be achieved. Once the value of b surpasses 2/3, afterwards, the Carnivore procedure could be implemented. This procedure improves the exploration phase,

$$C = \frac{1}{2} V_1 / |V_2| \quad (6)$$

$$V_1 \sim N(0,1) \quad (7)$$

$$V_2 \sim N(0,1) \quad (8)$$

Where $N(0,1)$ denotes a standard dispersion with 0 standard and mean deviation. Herbivore: when the consumer is selected arbitrarily, then they only eat producer:

$$X_i(t+1) = X_i(t) + C * \left(X_i(t) - X_j(t)\right), i \in [2, \dots, n] \quad (9)$$

Carnivore: When the consumer was chosen arbitrarily, then Carnivore eat only consumer with the highest energy level,

$$X_i(t+1) = X_i(t) + C * \Big(X_i(t) - X_j(t)\Big), \quad i \in [2,n]; j = randi([2i-1]) \tag{10}$$

Omnivore: When a consumer is chosen randomly, the consumer eats with the highest energy level and producer.

$$X_i(t+1) = X_i(t) + C * (r_2 * (X_i(t) - X_1(t)) + (1 - r_2)(X_i(t) - X_j(t)) ;$$

$$i = 3, \ldots . n; j = randi[2i-1] \tag{11}$$

The AEO algorithm derived a Fitness Function (FF) for optimal classifying output. It determined a positive value to demonstrate the great outcome of the candidate's solution. During this article, the lesser error rate of the classifier was treated as FF, as illustrated in Eq. (12).

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

$$= \frac{number\ of\ misclassified\ sampling}{Total\ number\ of\ sampling} * 100 \tag{12}$$

4. Results and Discussion

This segment examines the outputs on the WSN-ID database [24]. It is utilized in simulation experiments and processes to produce a dataset of 23 factors. Four kinds of DoS outbreaks are determined in WSN-DS: Flooding, Blackhole, Scheduling Attacks, and Grayhole, as given in Table 1.

Fig. 3 demonstrates the classifier outputs of the AEOCRNN-IDS approach under 80 and 20 percent of TR/TS data. Fig. 3a shows that the confusion matrices presented by the AEOCRNN-IDS approach have identified instances of 271729, 7670, 10902, 2642, and 4801 under classes of regular, BH, GH, flooding, and TDMA. Then, Fig. 3b portrays the confusion matrices presented by the AEOCRNN-IDS model has identified instances of 67909, 1963, 2680, 611, and 1288 under normal, BH, GH, flooding, and TDMA classes. Likewise, Figs. 3c-3d illustrates the PR examination of the AEOCRNN-IDS approach under TR/TS data. The figures stated that the AEOCRNN-IDS approach had reached greater PR performance in the class. At last, Figs. 3e-3f illustrates the ROC study of the AEOCRNN-IDS model under the TR/TS dataset. The figure represented that the AEOCRNN-IDS method has led to proficient outputs with higher values of ROC in several class labels.

Table 2 and Fig. 4 give a complete ID output of the AEOCRNN-IDS technique with 80 and 20 percent of TR/TS data. The outputs denoted that the AEOCRNN-IDS technique has proficiently identified different types of attacks. As a sample, with 80 per cent of the TR dataset, the AEOCRNN-IDS model has attained an average $accu_y$ of 99.74%, $sens_y$ of 99.34%, $spec_y$ of 99.83%, F_{score} Of 99.34%, and MCC of 95.39%. Meanwhile, with 20% of the TS dataset, the AEOCRNN-IDS model has attained an average $accu_y$ of 99.74%, $sens_y$ of 99.36%, $spec_y$ of 99.84%, F_{score} of 99.36%, and MCC of 95.43%.

Fig. 5 illustrates the classifier outputs of the AEOCRNN-IDS method on 70 and 30 percent of TR/TS data. Fig. 6a portrays the confusion matrices presented by the AEOCRNN-IDS approach has identified instances of 237659, 6963, 9695, 2344, and 4195 under classes of normal, BH, GH, flooding, and TDMA. Afterwards, Fig. 6b illustrates the confusion matrices presented by the AEOCRNN-IDS approach has identified instances of 101829, 3014, 4170, 934, and 1863 under classes of normal, BH, GH, flooding, and TDMA. Also, Figs. 6c-6d illustrates the PR evaluation of the AEOCRNN-IDS approach under TR/TS data. The figures specified that the AEOCRNN-IDS method had gained maximal PR accomplishment under the total classes. Lastly, Figs. 6e-6f demonstrates the ROC examination of the AEOCRNN-IDS methodology under the TR/TS dataset. The figure illustrated that the AEOCRNN-IDS methodology gave an advanced output with a maximum value of ROC in several class labelling.

Table 3 and Fig. 6 present the total ID outputs of the AEOCRNN-IDS approach with 70 and 30 percent of TR/TS data. The outputs demonstrate that the AEOCRNN-IDS method has proficiently identified diverse kinds of outbreaks. As a sample, with 70 percent of the TR dataset, the AEOCRNN-IDS method has attained an average $accu_y$ of 99.79%, $sens_y$ of 99.46%, $spec_y$ of 99.87%, F_{score} Of 99.46%, and MCC of 96.14%. In the meantime, with 30 per cent of TS datasets, the AEOCRNN-IDS technique has reached an average $accu_y$ of 99.79%, $sens_y$ of 99.48%, $spec_y$ of 99.87%, F_{score} of 99.48%, and MCC of 96.02%. Fig. 7 presents the AEOCRNN-IDS approach's loss value and $accu_y$ Of the 70 and 30 percent of TR/TS data. The figure shows that the $accu_y$ gradient value to enhance and loss gradient value to a lesser with maximum epoch counts. The trained loss was notably lesser, and validation accuracy was greater on 70 and 30 percent of the TR/TS dataset.

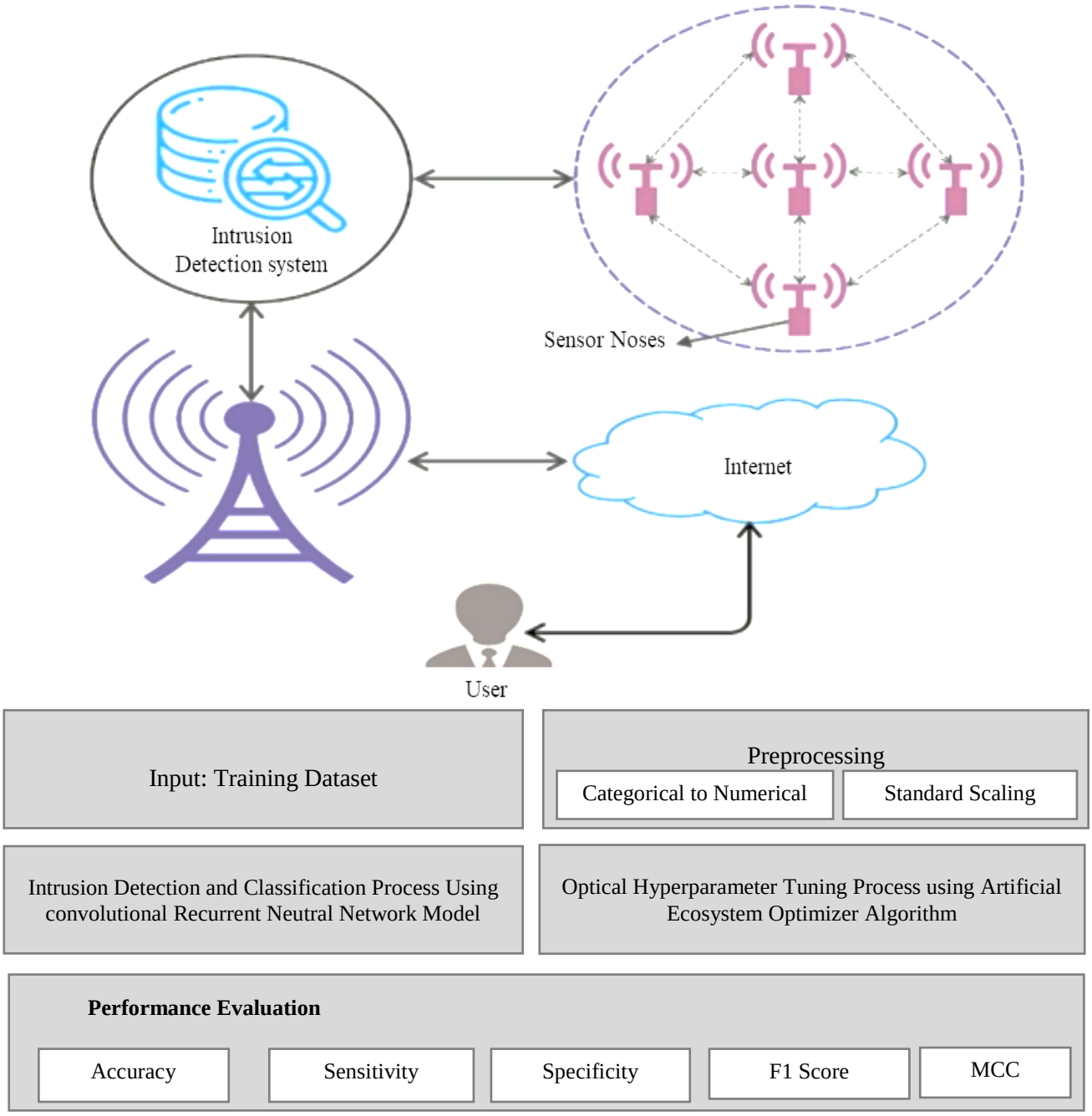


Fig. 1 Overall procedure of AEOCRNN-IDS method

Table 1. Dataset details

Class	Sample Numbers
Normal	340066
Blackhole	10049
Grayhole	14596
Flooding	3312
Scheduling Attacks	6638
Total Sample Numbers	374661

The comparative evaluation of the AEOCRNN-IDS model with other ML classification approaches is represented in Table 4 [15, 25]. Fig. 8 reports a relative $accu_y$ Evaluation of the AEOCRNN-IDS method with current algorithms. The outcomes denoted that the GB approach has reached a reduced $accu_y$ Of 94.23%. Afterwards, the XGBoost system has shown a somewhat higher $accu_y$ Of 95.91%. Meanwhile, the KNN, KNN-PSO, and Adaboost methods have accomplished considerable $accu_y$ values of 96.30%, 96.40%, and 96.47% respectively. But the better performance of the AEOCRNN-IDS model is confirmed by the maximum $accu_y$ of 99.79%.

Fig. 9 shows a short $sens_y$ Assessment of the AEOCRNN-IDS model with present methods. The outcomes implied that the GB method had gained a reduced $sens_y$ Of 96.95%. Simultaneously, the XGBoost method has shown a slightly improved $sens_y$ Of 94.75%. In the meantime, the Adaboost, KNN, and KNN-PSO approaches have accomplished considerable $sens_y$ values of 94.96%, 96.99%, and 94.10% correspondingly. But the better performance of the AEOCRNN-IDS technique is confirmed by the maximum $sens_y$ of 99.46%.

Fig. 10 exhibits the detailed comparative $spec_y$ Valuation of the AEOCRNN-IDS algorithm with existing methods. The outcomes show that the GB technique has reached a reduced $spec_y$ Of 94.55%. Also, the XGBoost methodology has shown a somewhat enhanced $spec_y$ of 94.14%. In the meantime, the Adaboost, KNN, and KNN-PSO methods have accomplished considerable $spec_y$ values of 94.47%, 96.20%, and 94.21% correspondingly. But the better performance of the AEOCRNN-IDS approach is confirmed by the maximum $spec_y$ of 99.87%.

Fig. 11 portrays a comparative F_{score} Investigation of the AEOCRNN-IDS approach with other methods. The outcome implied that the GB technique had gained a reduced F_{score} Of 92.43%. Besides, the XGBoost method has shown a somewhat enhanced $accu_y$ Of 90.70%. In the meantime, the Adaboost, KNN, and KNN-PSO models have accomplished considerable. F_{score} values of 91.09%, 90.79%, and 92.59% correspondingly. But the better performance of the AEOCRNN-IDS method is confirmed by the maximum F_{score} Of 99.46%. These results demonstrated the higher achievement of the AEOCRNN-IDS method over other current methods.

Table 2. ID output of AEOCRNN-IDS technique on 80:20 of TR/TS data

80:20 of Training / Testing					
Labels	**Accuracy**	**Sensitivity**	**Specification**	**F-Score**	**MCC**
Training					
Normal	99.59	99.87	96.81	99.78	97.55
Blackhole	99.75	95.80	99.86	95.40	95.28
Grayhole	99.60	92.97	99.87	94.81	94.62
Flooding	99.90	98.29	99.91	94.51	94.53
TDMA	99.83	91.66	99.98	94.99	94.97
Average	**99.74**	**99.34**	**99.83**	**99.34**	**95.39**
Testing					
Normal	99.61	99.87	97.03	99.78	97.66
Blackhole	99.76	96.08	99.86	95.59	95.47
Grayhole	99.63	93.38	99.88	95.04	94.86
Flooding	99.90	97.92	99.91	94.07	94.09
TDMA	99.82	92.00	99.97	95.09	95.06
Average	**99.74**	**99.36**	**99.84**	**99.36**	**95.43**

Table 3. ID output of AEOCRNN-IDS technique on 70:30 of TR/TS data

70:30 of Training / Testing					
Labels	**Accuracy**	**Sensitivity**	**Specification**	**F-Score**	**MCC**
Training					
Normal	99.65	99.83	97.81	99.80	97.88
Blackhole	99.84	99.23	99.85	96.99	96.93
Grayhole	99.72	94.91	99.91	96.31	96.18
Flooding	99.90	99.20	99.91	94.73	94.77
TDMA	99.83	91.02	99.99	94.94	94.95
Average	**99.79**	**99.46**	**99.87**	**99.46**	**96.14**
Testing					
Normal	99.67	99.82	98.15	99.82	98.03
Blackhole	99.83	99.41	99.84	96.90	96.84
Grayhole	99.73	95.18	99.92	96.54	96.41
Flooding	99.88	98.42	99.90	93.45	93.51
TDMA	99.84	91.82	99.98	95.29	95.28
Average	**99.79**	**99.48**	**99.87**	**99.48**	**96.02**

Table 4. Relative evaluation of AEOCRNN-IDS algorithm with ML classifiers

Models	$Accu_y$	$Sens_y$	$Spec_y$	F_{score}
AEOCRNN-IDS	99.79	99.46	99.87	99.46
Ada-Boost	96.30	94.96	94.47	91.09
GB	94.23	96.95	94.55	92.43
XG-Boost	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

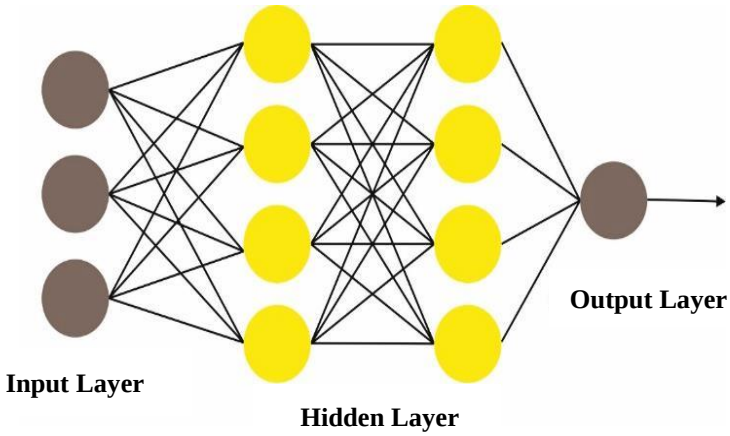
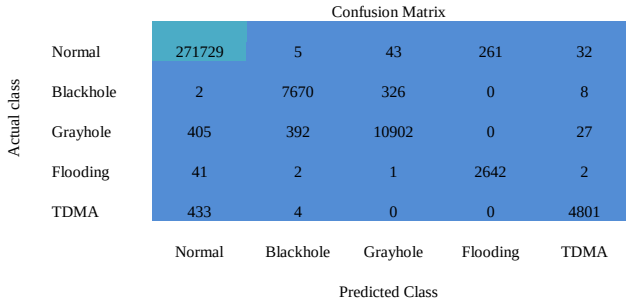
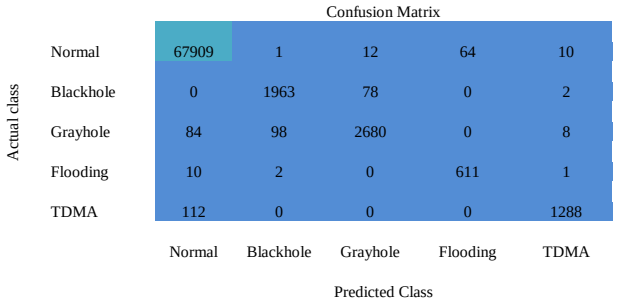


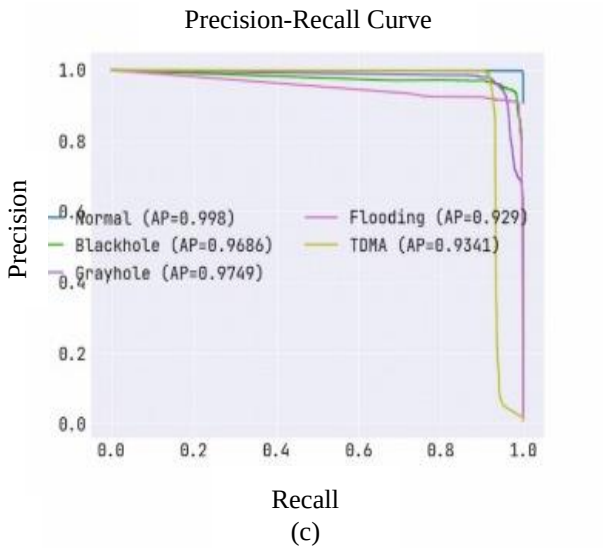
Fig. 2 Architecture of RNN



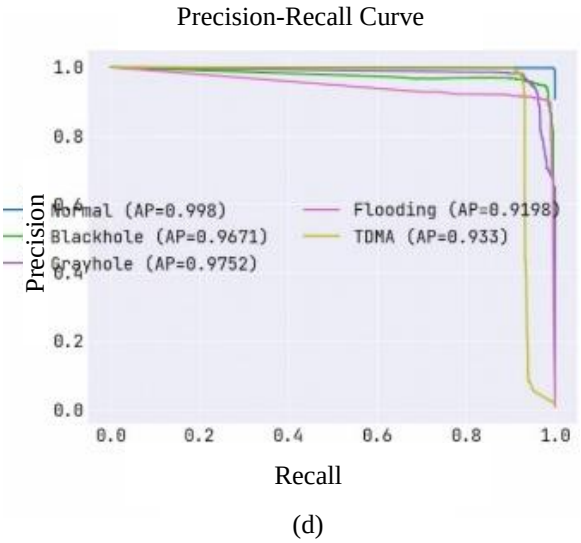
(a)



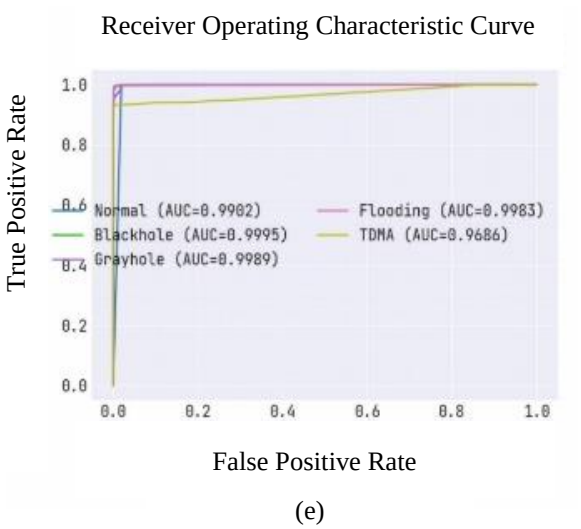
(b)



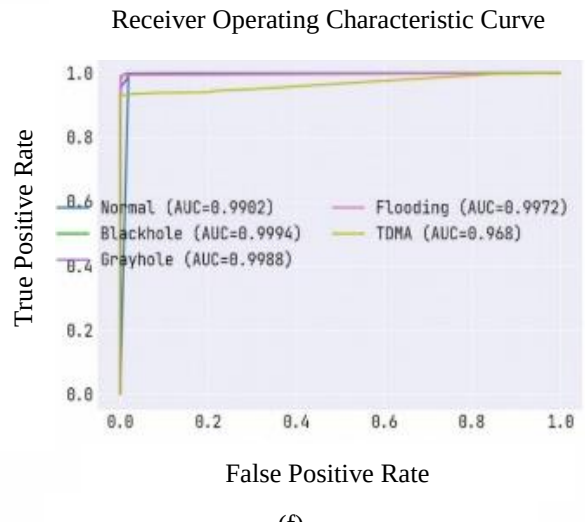
(c)



(d)



(e)



(f)

Fig. 3 Outcome of (80:20) Training a) Confusion matrix b) Confusion matrix c) PR curve d) PR curve e) ROC testing Set f) ROC

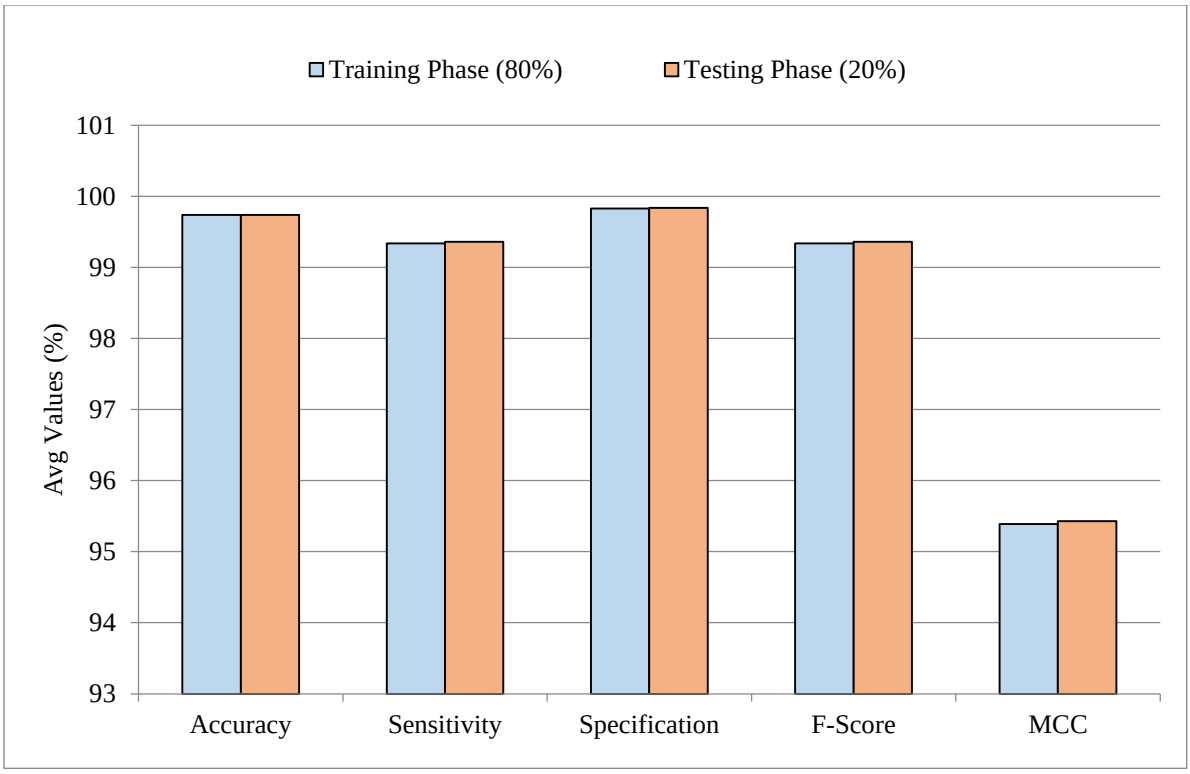


Fig. 4 Average output of AEOCRNN-IDS technique on 80:20 of TR/TS datasets

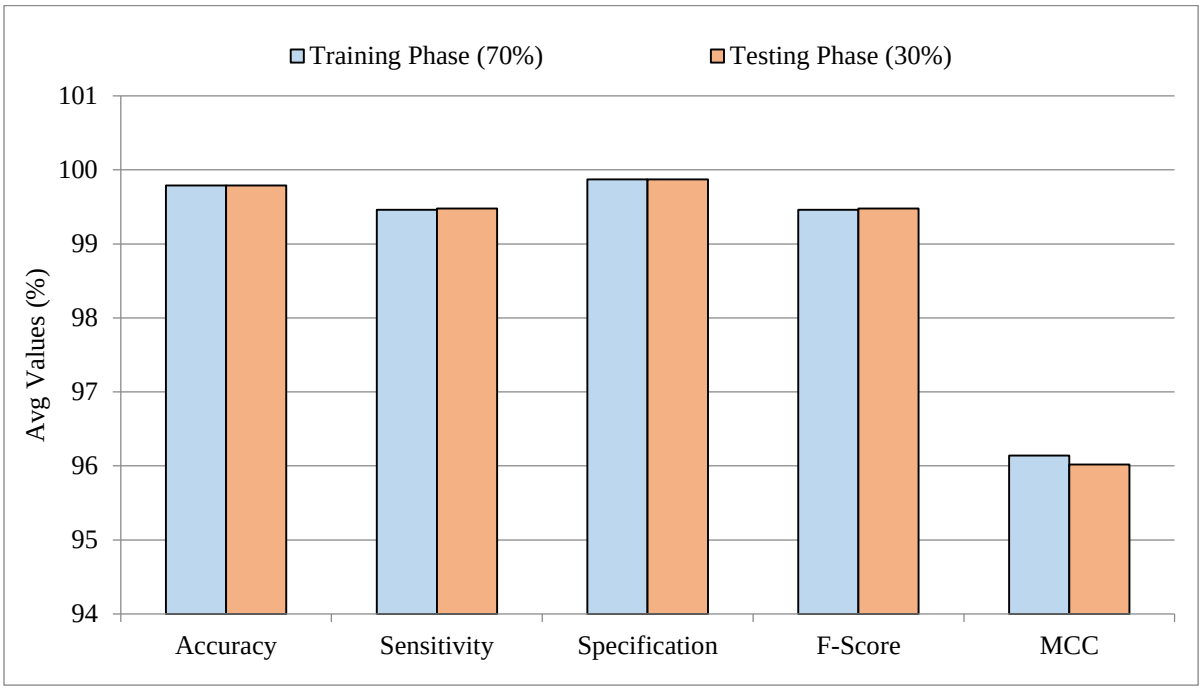
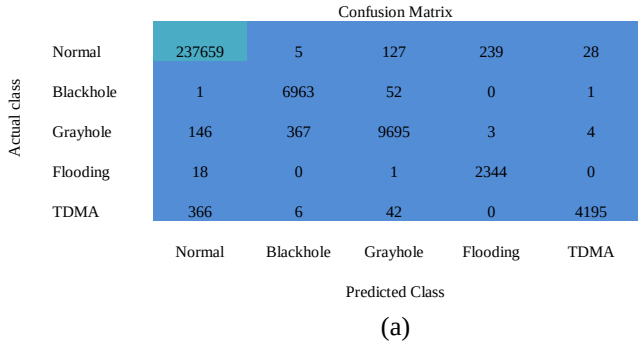
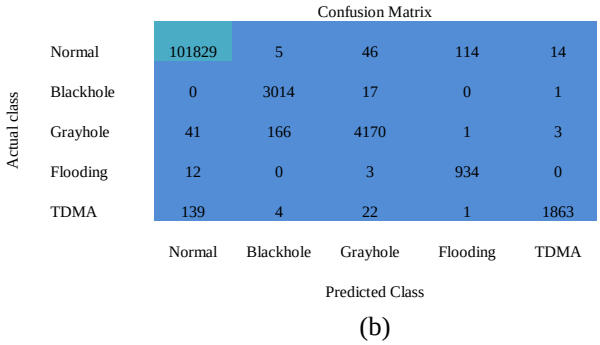


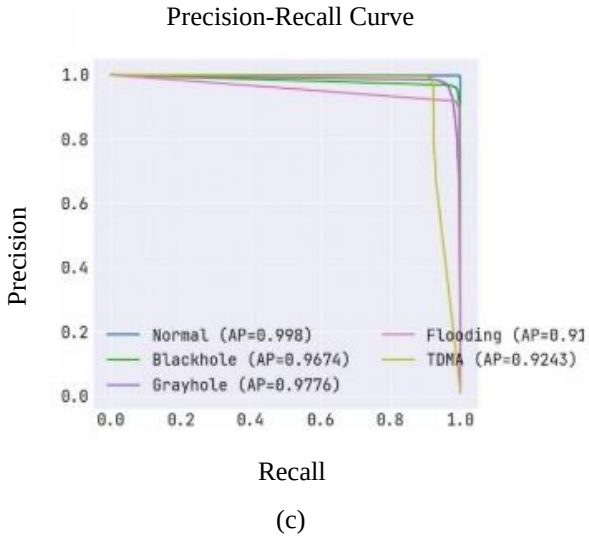
Fig. 5 Average output of AEOCRNN-IDS model on 70:30 of TR/TS datasets



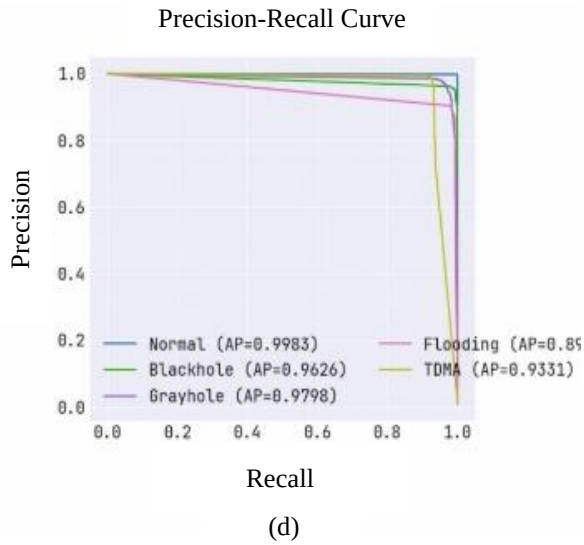
(a)



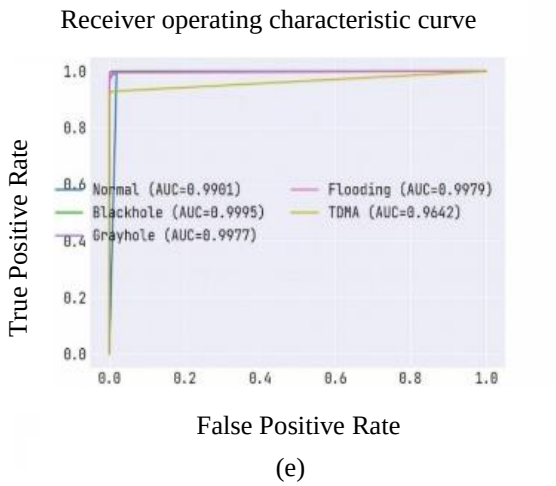
(b)



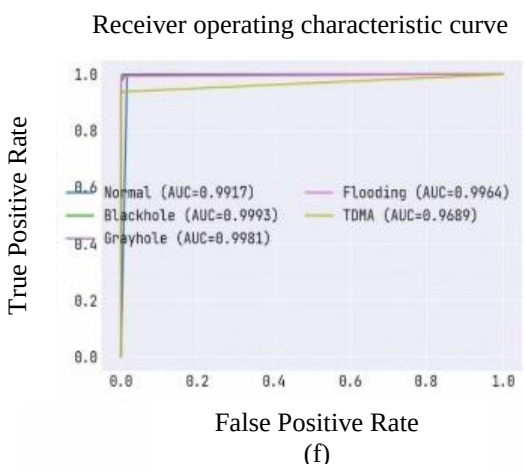
(c)



(d)



(e)



(f)

Fig. 6 Output of (70:30) Training a) Confusion matrix b) Confusion matrix c) PR curve d) PR curve e) ROC testing Set f) ROC

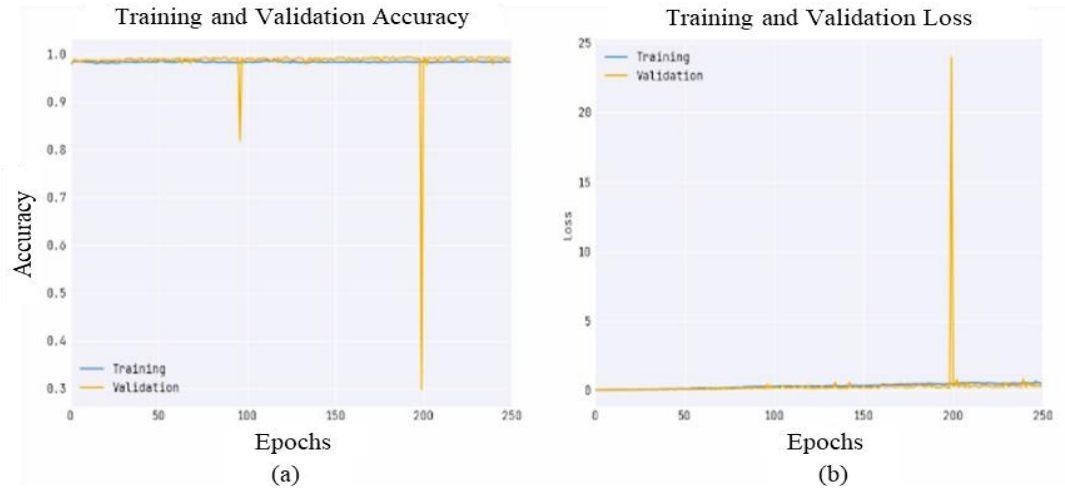


Fig. 7 Accu_y and loss evaluation of the AEOCRNN-IDS model under 70:30 of the TR/TS dataset

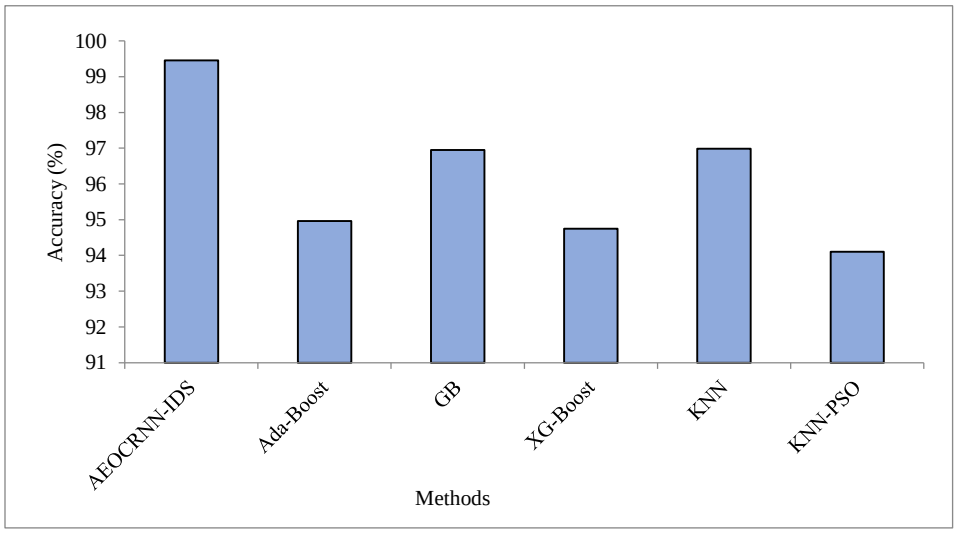


Fig. 8 $Accu_y$ evaluation of the AEOCRNN-IDS model with ML classifiers

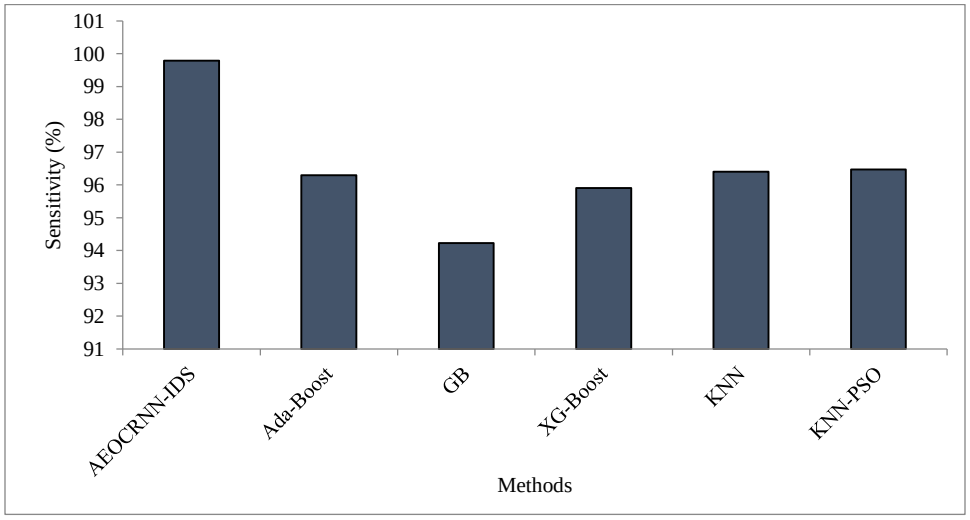


Fig. 9 $Sens_y$ analysis of AEOCRNN-IDS system with ML classifiers

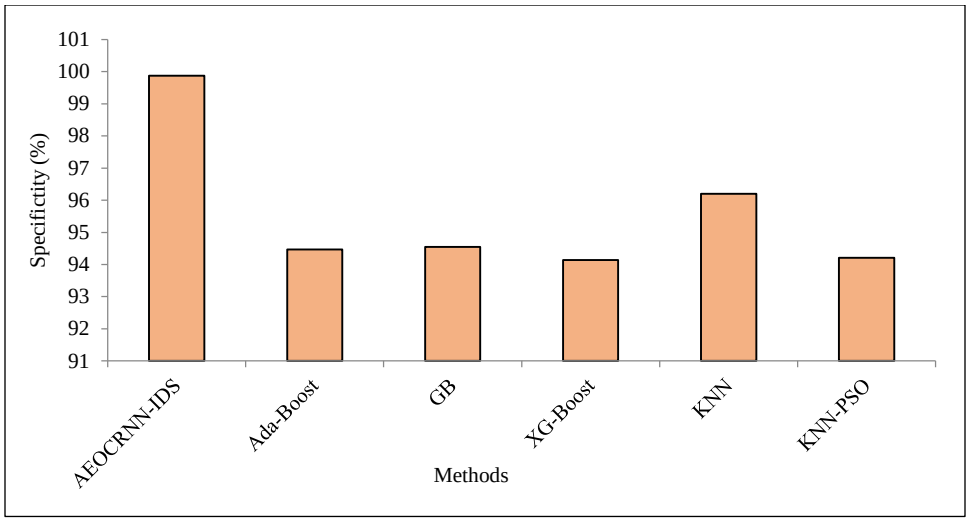


Fig. 10 $Spec_y$ analysis of AEOCRNN-IDS system with ML classifiers

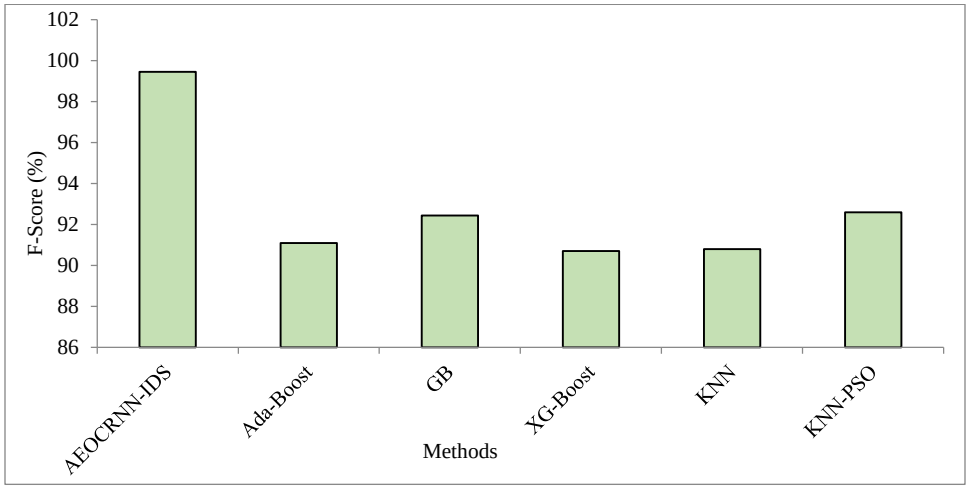


Fig. 11 F_{score} analysis of AEOCRNN-IDS approach with ML classifiers

5. Conclusion

In this research, we have presented a novel AEOCRNN-IDS model for recognizing and classifying intrusions in the network. In the proposed AEOCRNN-IDS model, data preprocessing is done to make the data compatible for more processing. The AEOCRNN-IDS technique uses the CRNN model in this study for ID and classification. Since hit-and-miss tuning selection is a dreary procedure, the AEOCRNN-IDS technique implements the AEO approach for the optimum tuning process. The experimental validation of the AEOCRNN-IDS methodology was tested employing an intrusion database from the Kaggle repository. The extensive experimental investigation stated the supremacy of the AEOCRNN-IDS system on ID in the WSN. A feature selection technique can be included in the coming days to improve the achievement of the AEOCRNN-IDS approach.

References

[1] E. Baraneetharan, "Role of Machine Learning Algorithms Intrusion Detection in WSNs: A Survey," *Journal of Information Technology and Digital World*, vol. 2, no. 3, pp. 161-173, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Mohammed S. Alsahli et al., "Evaluation of Machine Learning Algorithms for Intrusion Detection System in WSN," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 5, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Abhilash Singh et al., "LT-FS-ID: Log-Transformed Feature Learning and Feature-Scaling-Based Machine Learning Algorithms to Predict the K-Barriers for Intrusion Detection using Wireless Sensor Network," *Sensors*, vol. 22, no. 3, p. 1070, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Saurabh Deshpande et al., "A Comparative Analysis of Machine Deep Learning Algorithms for Intrusion Detection in WSN," *In Security Issues and Privacy Threats in Smart Ubiquitous Computing*, pp. 173-193, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Abhilash Singh et al., "AutoML-ID: Automated Machine Learning Model for Intrusion Detection using Wireless Sensor Network," *Scientific Reports*, vol. 12, no. 1, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] GeetaSingh, and NeeluKhare, "A Survey of Intrusion Detection from the Perspective of Intrusion Datasets and Machine Learning Techniques," *International Journal of Computers and Applications*, vol. 44, no. 7, pp. 659-669, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Hamza Elbahadır, and Ebubekir Erdem, "Modeling Intrusion Detection System using Machine Learning Algorithms in Wireless Sensor Networks," *In 2021 6th International Conference on Computer Science and Engineering (UBMK)*, pp. 401-406, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Pankaj Ramchandra Chandre, Parikshit Mahalle, and Gitanjali Shinde, "Intrusion Prevention System using Convolutional Neural Network for Wireless Sensor Network," *International Journal of Artificial Intelligence (IJ-AI)*, vol. 11, no. 2, pp. 504-515, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] S. Suma Christal Mary et al., "Selfish Herd Optimization with Improved Deep Learning Based Intrusion Detection for Secure Wireless Sensor Network," *SSRG International Journal of Electronics and Communication Engineering*, vol. 10, no. 4, pp. 1-8, 2023. [CrossRef] [Publisher Link]

[10] D. Narmatha, W. Jenifa, and Pushpa Mettilsha, "Implementation of Cognitive Wireless Sensor Network with Energy Aware Cooperative Spectrum Sensing by Different Censoring Techniques," *SSRG International Journal of Electronics and Communication Engineering*, vol. 7, no. 5, pp. 24-32, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] R. Anushiya, and V.S. Lavanya, "A New Deep-Learning with Swarm Based Feature Selection for Intelligent Intrusion Detection for the Internet of Things," *Measurement: Sensors*, vol. 26, p. 100700, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Rashid Md Mamunur, "A Novel Intrusion Detection System in IoT Networks Leveraging Blockchain-Enabled Federated Learning, 2023. [Online] Available: https://repository.pknu.ac.kr:8443/handle/2021.oak/32882

[13] KhurramHussain et al., "Hybrid of WOA-ABC and Proposed CNN for Intrusion Detection System in Wireless Sensor Networks," *Optik*, vol. 271, p. 170145, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Judy Simon et al., "Hybrid Intrusion Detection System for Wireless IoT Networks using Deep Learning Algorithm," *Computers and Electrical Engineering*, vol. 102, p. 108190, 2022. [CrossRef] [Google Scholar] [Publisher Link]

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

[16] Hamza Elbahadır, and Ebubekir Erdem, "Modeling Intrusion Detection System using Machine Learning Algorithms in Wireless Sensor Networks," *In 2021 6th International Conference on Computer Science and Engineering (UBMK)*, pp. 401-406, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Mohammad RezaBegli, Farnaz Derakhshan, and Hadis Karimipour, "A Layered Intrusion Detection System for Critical Infrastructure using Machine Learning," *In 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, pp. 120-124, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] Weimin Wen et al., "An Intrusion Detection Model using Improved Convolutional Deep Belief Networks for Wireless Sensor Networks," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 36, no. 1, pp. 20-31, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Subarna Shakya, "Modified Gray Wolf Feature Selection and Machine Learning Classification for Wireless Sensor Network Intrusion Detection," *IRO Journal on Sustainable Wireless Systems*, vol. 3, no. 2, pp. 118-127, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Mohamed Hammad, Nabil Hewahi, and Wael Elmedany, "T-SNERF: A Novel High Accuracy Machine Learning Approach for Intrusion Detection Systems," *IET Information Security*, vol. 15, no. 2, pp. 178-190, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Hafsa Benaddi et al., "A Deep Reinforcement Learning Based Intrusion Detection System (DRL-IDS) for Securing Wireless Sensor Networks and Internet of Things," *In International Wireless Internet Conference*, pp. 73-87, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[22] Longting Chen et al., "Health Indicator Construction of Machinery Based on End-to-End Trainable Convolution Recurrent Neural Networks," *Journal of Manufacturing Systems*, vol. 54, pp. 1-11, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] Kuntal Bhattacharjee, Kathan Shah, and Jatin Soni, "Solving Economic Dispatch using Artificial Eco System-Based Optimization," *Electric Power Components and Systems*, vol. 49, no. 11-12, pp. 1034-1051, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] 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]

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

[26] Shraddha Kamble, B.K Mishra, and Rajesh Bansode, "Detection of Routing Misbehaving Links in MANET by Advance EAACK Scheme," *International Journal of P2P Network Trends and Technology (IJPTT)*, vol. 6, no. 3, pp. 1-5, 2016. [CrossRef] [Publisher Link]

[27] Harikishan, and P. Srinivasulu, "Intrusion Detection System using Fuzzy Inference System," *International Journal of Computer & organization Trends (IJCOT)*, vol. 3, no. 4, pp. 59-66, 2013. [Google Scholar] [Publisher Link]

[28] S. Navya Sai, and K. KishoreRaju, "Improved Privacy Preserving Decision Tree Approach for Network Intrusion Detection," *International Journal of Computer & organization Trends (IJCOT)*, vol. 6, no. 1, pp. 55-60, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[29] S. Kulkarni Sagar, and A. Kahate Sandip, "Review of a Semantic Approach to Host-Based Intrusion Detection Systems using Contiguous and Discontiguous System Call Patterns," *SSRG International Journal of Computer Science and Engineering*, vol. 2, no. 6, pp. 9-12, 2015. [CrossRef] [Publisher Link]

[30] Mohammad Dawood Momand, Vikas Thada, and Utpal Shrivastava, "Intrusion Detection System in IoT Network," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 4, pp. 11-15, 2020. [CrossRef] [Publisher Link]