Hybrid Metaheuristics with Deep Learning Assisted Intrusion Detection on Cyber-Physical Smart Grid Environment

Manal M. Nasir [1,*], Salim M. Hebrisha[2]
[1]Gwinnett Technical College (GTC), Lawrenceville , GA, 30043, USA
[2]Libyan Iron and Steel Company (LISCO), Misrata, Libya
Emails: Mnasir@gwinnetttech.edu; salimhibrisha@gmail.com

Abstract

Smart grids (SGs) offer can ensure that users with a continuous power supply, decreased line losses, improved renewable output and storing, user participation in current electricity, and demand-side responsiveness. The development of cyberphysical SG (CPSG) systems has transformed the standard power grid by allowing bi-directional energy flow among utilities and users. But, because of increased data change among consumers, it is presented a major problem to the firewall systems for the transmission networks at either cyber or physical planes. Intrusion Detection Systems (IDSs) can role an essential play in maintaining SGs systems against cyber threats by generating a second wall of defense, complementing conventional preventive security procedures (for instance, authorization, encryption, and authentication). Therefore, this article concentrates on the design and development of Hybrid Metaheuristics with Deep Learning Assisted Intrusion Detection in a Cyber-Physical Smart Grid (HMDL-IDCPSG) infrastructure. The major objective of the HMDL-IDCPSG system provides the effectual recognition of the intrusions using feature selection and classification processes in the CPSG infrastructure. In the presented HMDL-IDCPSG method, a binary dragonfly algorithm with the hybrid directed differential operator (BDA-DDO) algorithm could be implemented for the feature selection (FS) method. Besides, attention-based bi-directional long short-term memory (ABiLSTM) algorithm could be carried out for the recognition and classification of the intrusions. At last, the sparrow search algorithm (SSA) can be exploited for highest chosen the hyperparameter values of the ABiLSTM algorithm which supports in achieving a better solution. For demonstrating the greater outcome of the HMDL-IDCPSG technique, a comprehensive simulation value can be executed. The obtained results reported the supremacy of the HMDL-IDCPSG methodology with other existing approaches

Keywords: Cybersecurity; Intrusion detection; Feature selection; Deep learning; Smart grids; Cyber-physical systems

1. Introduction

An advanced power grid extensively identified as a smart grid (SG) includes a bi-directional interchange of data and energy among the end-users [1]. It contains improved measuring and communication technologies, which have control methods, executed at the cyber plane of cyber physical-SG (CPSG) systems providing grid digitalization and robustness. Although the standard power grid depends on supervisory control and data acquisition (SCADA) systems to monitor and control applications, CPSG systems utilize the latest technologies like phasor measurement unit (PMU) for highly complex control functions and higher resolution monitoring [2]. Since the network size and various kinds of attack extend to develop, these communication networks can be susceptible to great cyber vulnerability exceed ever before. Nowadays, users are directly interacted with the grid utilizing smart appliances and improving the possibility of cyberattacks in the CPSG platform [3]. Additionally, the interventions occurred at cyber and physical planes affected by both manual and natural attacks. Hence, it has essential for differentiating the power system interventions to help the cyberattacks identification and controlling abilities [4].

In this system, including the inter-dependency of communication technology at diverse network levels, the system develops highly vulnerable to cyberattacks like external and internal [5]. An IDS's main function is used for

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024

monitoring the traffic data flow and identifying suspicious activities or attacks by detecting unauthorized accessibility and consequently increasing an alarm informing an administrator to prevent these security issues or automatically the alleviation method [6]. IDSs are often classified into 2-types. Anomaly-based IDS detection attacks depend on some abnormality from normal activities. But signature-based IDS is compared with the traffic flow with known attack models and increases a system attacks issue when it will be compared [7]. According to the location of an IDS system, it has been host- (for example, software applications deployed on user computers) and network-based (that is positioned in the network at multi-points as hardware sensors or implemented system software interconnected to network analyzing the flow of data packet). If an SG platform is further centralized or decentralized or allocated, individuals could select a method for optimum exploitation [8].

A standard IDS system studies and analyses network traffic for identifying and detecting attacks and preventing some security breaches by producing alarms for network administrators. Additionally, as a Cyber-Physical System (CPS), the failure for detection like interventions in the SG could present a physical effect on the power system namely loss of control, a main blackout, and system failure [9]. Thus, it is noticeable that the aid of exploiting ML-based IDS for improving the method of self-configuration and self-learning through the computers from data configurations and increasing forecasts depends on the extensive data patterns without human involvement dependent upon the learned behaviours [10].

This article concentrates on the development of Hybrid Metaheuristics with Deep Learning Assisted Intrusion Detection in a CyberPhysical Smart Grid (HMDL-IDCPSG) environment. In the presented HMDL-IDCPSG technique, a binary dragonfly algorithm with the hybrid directed differential operator (BDA-DDO) algorithm could be used for the feature selection procedure. Moreover, attention-based bi-directional long short-term memory (Abi-LSTM) methodology can be executed for classifying and recognizing the intrusions. Eventually, the sparrow search algorithm (SSA) could be exploited for optimal choose the hyperparameter values of the ABiLSTM algorithm that supports realizing better solutions. For demonstrating the excellent outcome of the HMDL-IDCPSG method, a comprehensive result values were achieved.

2. Related Works

Kaur et al. [11] presented a Bayesian technique incorporated with deep-CNNs (CNN-Bayesian). The Bayesian element was employed for differentiating CPS intrusions from the normal activities in the multiclass and binary activities. CNN layers were employed for managing the higher dimensional feature space before the classification of intrusion tasks. Goyel and Swarup [12] offered a new approach to optimization methods to build FDIA against state prediction techniques existing at the control center. The development for producing AC state evaluation attacks with detailed data as well as inadequate data together with DC state prediction attacks is provided. In [13], introduced intelligent attack identification and recognition method dependent upon an ensemble of ML techniques. Additionally, this suggested method finds the attacks or mistakes to features or estimations in the method for supporting cybersecurity experts in alleviating the impact of the attacks in communication networks.

Bitirgen and Filik [14] presented an approach of optimum CNN-LSTM with PSO for detecting FDIA in the SG system. A difficult hyperparameter space of the CNN-LSTM was improved by the PSO and contrasted with employing LSTM, CNN-LSTM, and PSO-LSTM techniques. Mukherjee et al. [15] suggested a new real-time FDIA detection algorithm through a DL-based state prediction method and later a new intrusion detection method utilizing the error covariance matrices. This presented DL algorithm with its optimal classification of hyper-parameters proves an efficient, accessible, real-time, state estimation technique with less error margin. Dairi et al. [16] developed 2-semi-supervised hybrid DL-based anomaly detection techniques for IDS in ICS traffic of SG. The primary method was AE-GRU, and the secondary approach is created by a GAN algorithm with a RNN for discriminator and generator, which can be known as GAN-RNN.

In [17], recommended an Intelligent Loop Based-ANN (IL-ANN) based identification method. This algorithm is compared with the abnormality of a model with the load profile existing under the architecure nodes and some abnormalities from predetermined data produces an alarm. For each 2ms the data acquired by the estimation is transferred through the IDS. Mhmood et al. [18] introduced an intelligent IDS. In the first stage, this developed technique equals the training data with a standard DL algorithm depending on CGAN and Game Theory. In the second stage, the Aquila Optimization (AO) approach chooses features. In the third stage, map the chosen features and code minimum-dimensional data into RGB color images. Lastly, the AO method optimum adapts meta-parameters for decreasing errors.

3. The Proposed Model

In this article, we have concentrated on the presents of the HMDL-IDCPSG algorithm for the SG platform. The major aim of the HMDL-IDCPSG method lies in the effectual recognition of the intrusions using feature selection

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024

and classification processes in the CPSG environment. In the presented HMDL-IDCPSG technique, three processes are involved namely BDA-DDO-based FS, ABiLSTM-based intrusion detection, and SSA-based parameter tuning. Fig. 1 portrays the entire procedure of the HMDL-IDCPSG method.

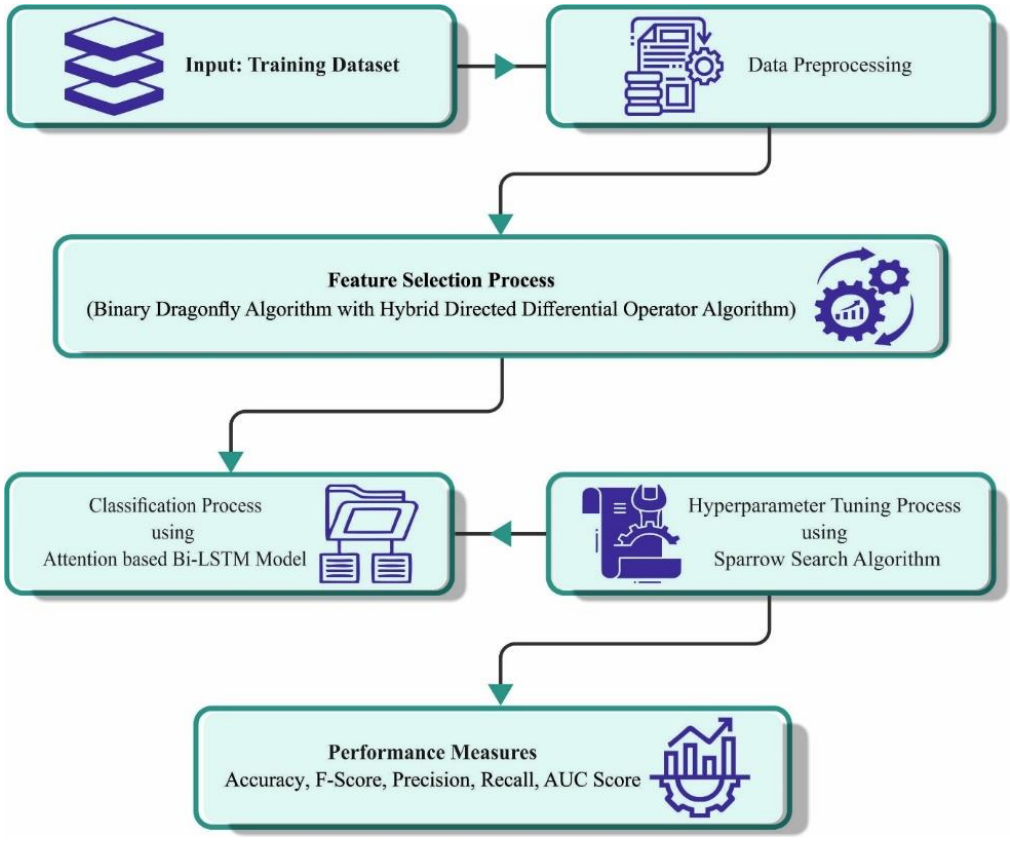

Figure 1: Overall process of the HMDL-IDCPSG method

A. Feature Selection using BDA-DDO Algorithm

The BDA-DDO method can be designed for choosing an optimum set of features. In BDA-DDO, a directed differential operator, which fuses BDA generated individuals with the differential operator, led to fast convergence [19]. BDA shows effective search ability, which addresses the difficulties including a lack of population diversity, limited late exploration, and slow convergence. We present three improvement mechanisms to effectively address this issue. As well, an adaptive approach is used for updating these operators, thus increasing population diversity. The fitness function (FF) evaluates the quality of the solution. The study proposed a new DO based on the DE technique to optimize the convergence rate of BDA. The best and worst solutions of the DF are combined to form a focused differential operator. Thereby, it offers a potential direction from the searching space, which guides individuals nearby the best solution and facilitates fast convergence toward the optimum area. A step-by-step explanation of differential operator.

Mutation: In this step, mutation can be used to i^{th} individual DF for generating mutation vector Storn and Price presented various mutation processes, with "$DE/rand/1$" exist the major standard one:

$$V_i = X_i + F \times \left(X_{Food} - X_{Enemy}\right) \quad (1)$$

Where X_{Enemy} is the position of DF enemies X_i denotes the individual location after updating the BDA, and X_{Food} characterizes the position of DFs food (the better position). F denotes the scaling factor controlling the increase of the variance vector and considerably impacts the convergence rates.

Crossover: crossover process is done by choosing both the original individual $X_{i,j}$ and mutant individual $V_{i,j}$ randomly for generating the experimental individual. Rotation-invariant arithmetic crossover, binomial crossover, and exponential crossover are the 3 traditional crossover operators. The binomial crossover operator can be given as follows:

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024

$$U_{i,j} = \begin{cases} V_{i,j} & rand < CR \text{ or } randi\ (1,d) = j \\ X_{i,j} & rand > CR \text{ or } randi\ (1,d) \neq j \end{cases} \quad (2)$$

In Eq. (2), $rand$ denotes the randomly produced parameter within [0,1] and $jrand$ specifies a random integer in the interval $[1, D]$, which ensures that one or more $U_{i,j}$ comes from $V_{i,j}$. CR refers to the crossover probability, chosen in zero and one, controlling the population diversity. Using the transfer function $T1$, the resultant $U_{i,j}$ vector can be transmuted into a discrete space vector. Next, a selection operation is performed for determining whether it survives to the next generation:

$$T1 = \frac{1}{1 + e^{-(U_i^d)}} \quad (3)$$

$$U_{i,j} = \begin{cases} U_{i,j} = 0\ rand < T1 \\ U_{i,j} = 1\ rand > T1 \end{cases} \quad (4)$$

Selection: selection operation is carried out for determining the survival factors U_i and X_i from the next generation.

$$X_i = \begin{cases} U_i\ f(U_i) \leq f(X_i) \\ X_i\ others \end{cases} \quad (5)$$

In Eq. (5), $f(U_i)$ and $f(X_i)$ denote the FF equivalent to U_i and X_i, correspondingly.

Time-varying differential vector approach was proposed to resolve the problem of population diversity. The value of the differential vector reduces from its initial value as iteration progresses. Initially, a large differential vector provides more valuable data for individual searches. On the other hand, a small differential vector is used to enhance population diversity in the optimum area, thus optimizing the performance of the overall search process.

$$F = \frac{0.5}{1 + (-0.5) \times e^{-0.5 \times iter}} \quad (6)$$

An adaptive step-updating process can used to overcome the issues of fixed step size which causes slower convergence if too small, or oscillation if too large, resulting in local optimal solution. During iteration, this mechanism adjusts the DF step size. The BDA-DDO technique incorporates the DDO and the adaptive step updating mechanism. This integrated method purposes to improve population diversity and enhance exploration in the late stage of an optimizer.

$$\Delta X = F \times \Delta X \quad (7)$$

FS method is a multiobjective problem, where the minimum subset of features and maximum classification accuracy are the goals that need to be accomplished. Both objectives with FF are balanced, by setting weighting factors:

$$fitness = \alpha \times ERR + \beta \times \frac{R}{N} \quad (8)$$

In Eq. (8), ERR denotes the classifier error rate attained by the ABiLSTM classifier, R refers to the number of FS subsets by the searching agent, and N indicates the overall number of features from the dataset. α and β show the weight factor to balance classification performance and feature subset. The ranges of α is [0,1] and the value of β is $(1 - \alpha)$. We set α to 0.99 and β to 0.01 to maximize the classification performance.

B. Intrusion Detection utilizing ABiLSTM Model

The ABiLSTM system could be implemented for the detection and classification of intrusions. LSTM is progressively employed in the network intrusion detection model for resolving the gradient vanishing problems caused by RNNs because of its capability to preserve long-term memory. LSTM is a time cyclic NN [20]. The LSTM unit changes the neurons from the RNN based on the cyclic NN. It contains forget, input and output gates that are introduced whose historical data is to be controlled and allow data to be passed through, preserve the memory capacity of extended data, and resolve the current long-term dependence problems from the RNN model. Fig. 2 depicts the framework of ABiLSTM.

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024

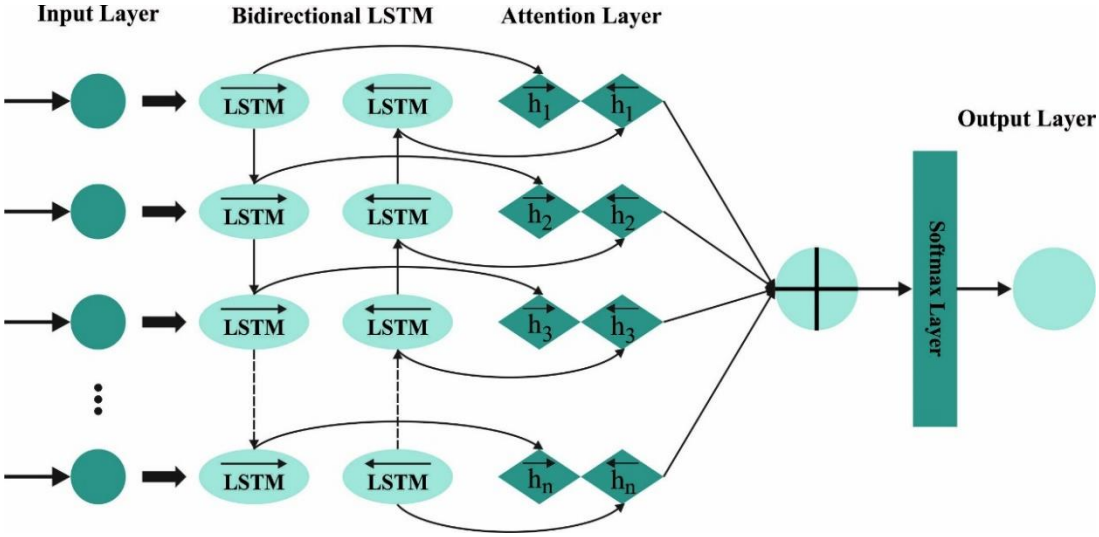

Figure 2: Architecture of ABiLSTM Model

The forget gate forgets the data that need to be forgotten and changes with the context. The outcome of forget gate is a sigmoid function, the value ranges from 0 to 1, and the latter is multiplied by the cell layer, where 0 signifies the data of this bit is all forgotten, and 1 signifies bit was retained entirely. The computation equation can be given as follows:

$$f_t = \sigma\left(W_f \cdot [h_{t-1}, x_t] + b_f\right) \tag{9}$$

The input gate additions the data. The outcome of the input gate is a sigmoid function within zero and one, which can be multiplied by the existing cell layer. The computation equation can be given as follows.

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \tag{10}$$

$$\tilde{C}_t = Tanh(W_c \cdot [h_{t-1}, x_t] + b_c) \tag{11}$$

Next, the older and newer state information are combined to form the last cell state.

$$C_t = f_t \times C_{t-1} + i_t \times \tilde{C}_t \tag{12}$$

The $Tanh$ function and the last cell state are the output. The outcome of the output gate is a sigmoid function within [0,1]. Select which data can be output. The computation equations are given below.

$$O_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \tag{13}$$

$$h_t = O_t \times Tanh(C_t) \tag{14}$$

Where the resultant signal of the output gate is i_t, whose values define the data to be inputted into the memory cell c, the resultant signal of forget gate is f_t, and its value defines the forget ratio of memory cell c, and shows whose values define the quantity of memory cell c to be outputted to the existing state h, C_t refers to the preparatory data to be inputted into the memory cell c, whose values are multiplied by i_t to acquire the data in the memory cell c, C_t indicates the preparatory data to be outputted to the HL h, where it multiplied by 0_t to acquire the data in h, the memory cell c_t at t time was screened by the input and forget gates, and after the hidden layer h_t is attained by the screening of output gate [21]. A NN infrastructure with an attention module chooses when to investigate data by automatically providing greater attention to feature vectors with the most important data than the feature vector with less important data. Assume that the final hidden layer of i^{th} BLSTM as h_{it}, is computed as follows:

$$h_{it} = \left[h_t^f, h_t^b\right] \tag{15}$$

$$e_{it} = tanh(W_a h_{it} + b_a) \tag{16}$$

$$a_{it} = \frac{exp(e_{it})}{\sum_{j=1}^{T} e\ xp(e)} \tag{17}$$

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024

$$v_t = \sum_{t=1}^{T} a_{it} \cdot h_{it} \tag{18}$$

The attention module allows attention to weight a_{it} to the i^{th} BLiSTM resultant vector at t time. W_a and b_a show the weight and bias in the attention layers. At last, the outcome in the attention layer creates an attention vector v_t is estimated as a weighted sum of the multiplication between i^{th} BiLSTM output vector and attention weight a_{it} at t time.

C. Parameter Tuning utilizing SSA

The SSA will be implemented for optimum choosing the hyperparameter values of the ABiLSTM method. SSA describes population optimizer technique that concludes the food acquisition by incessantly upgrading the location of discoverers, followers, and vigilantes during foraging, and the position of the optimum food will be the optimal solution acquired [22]. When there are n sparrows in the population, the count of vigilante account for $10\% \sim 20\%$ of the species groups, and amount followers and discoverers are changing dynamically.

$$X = [x_1, x_2, \dots, x_n] \tag{19}$$

The suitable function of individual correspondence is

$$F = [f(x_1), f(x_2), \dots, f(x_n)] \tag{20}$$

The renewal position of the discoverers is given below:

$$x_{ij}^{t+1} = \begin{cases} x_{ij}^{t} \cdot exp.\left(\dfrac{-i}{\alpha \times iter_{\max}}\right) & R_2 < ST \\ x_{ij}^{t} + Q \cdot L & R_2 \geq ST \end{cases} \tag{21}$$

Where t means the amount of existing iterations, x_{ij}^{t} indicates the location of i^{th} sparrow in the j^{th} decision parameter at t^{th} generation, and $\alpha \in (0,1)$, the safety threshold is ST, $iter_{\max}$ indicates the maximum iteration count, R_2 characterizes the alarm value, Q describes the random integer that follows the uniform distribution, dim means the dimension, and L signifies the identity matrix of $1 \times dim$.

The renewal position of the follower is given below:

$$x_{ij}^{t+1} = \begin{cases} Q \cdot \exp + \left(\dfrac{x_{worst}^{t} - x_{i.j}^{t}}{ij^{-X}prr + 11i^2}\right) & i \in (n/2, +\infty) \\ x_p^{t+1} + \left|x_{ij} - x_p^{t+1}\right| \cdot Z^{+} \cdot i \in [0, n/2] \end{cases} \tag{22}$$

Where x_p^{t+1} shows the individual location with better alteration in t+1, Z refers to the matrix of $1 \times dim$ and every component from the matrix is fixed to -1 or 1, $Z^{+} = Z^{T}(ZZ^{T})^{-1}x_{worst}^{t}$ indicates the individual location with a worse adaptation of t. If $i > n/2$, it implies that the i^{th} entrant is hungry extremely condition and has not got food. The existing fitness value (FV) is lower, and it must fly to another place to feed for more energy.

The renewal location of the vigilante is given below:

$$x_{ij}^{t+1} = \begin{cases} x_{best}^{t} + \beta \cdot \left|x_{ij} - x_{best}^{t}\right| & f_i \neq f_g \\ x_{best}^{t} + k \cdot \left(\dfrac{x_{ij}^{t} - x_{best}^{t}}{|f_i - f_w| + \varepsilon}\right) & f_i = f_g \end{cases} \tag{23}$$

Where the control step is β, x_{best}^{t} denotes the position of global optima at t generation, k ε is constant,$\in$ [1, 1], follows the uniform distribution of mean 0 and standard deviation of 1, f_w and f_i shows the FV of the present and existing global worst individual, and f_g shows the FV of the present global optimum.

The LOA system improves a FF to accomplish better classifier solutions. This defines a positive integer for depicting the higher outcome for candidate effectiveness. The decrease in classifier errors is supposed to be FF.

$$fitness(x_i) = ClassifierErrorRate(x_i)$$
$$= \frac{No.of\ misclassified\ instances}{Total\ no.of\ instances} * 100 \tag{24}$$

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024

4. Results and Discussion

This section briefly explains the intrusion detection outcome of the HMDL-IDCPSG system [23]. These accomplished outcomes of the HMDL-IDCPSG method are examined with the binary class dataset, which holds 115 normal samples and 1046 attack samples as demonstrated in Table 1. The available 129 features, the HMDL-IDCPSG system has chosen a total of 76 features.

Table 1: Details on binary class database

Binary Class Dataset	
Class	No. of Instances
Normal	115
Attacks	1046
Total Instances	1161

Fig. 3 illustrates the classifier performances of the HMDL-IDCPSG method at the binary class database. Figs. 3a-3b exemplifies the confusion matrices attained by the HMDL-IDCPSG algorithm on 70:30 of the TRAPH/TESPH. These experimental values defined that the HMDL-IDCPSG method can be recognized and categorized with 2 classes exactly. Then, Fig. 3c illustrates the PR effectiveness of the HMDL-IDCPSG method. This demonstrated that the HMDL-IDCPSG methodology provides the higher values of PR in 2 classes. However, Fig. 3d defines the ROC of the HMDL-IDCPSG approach. These results are represented that the HMDL-IDCPSG technique provides for performances with increased ROC values under 2 classes.

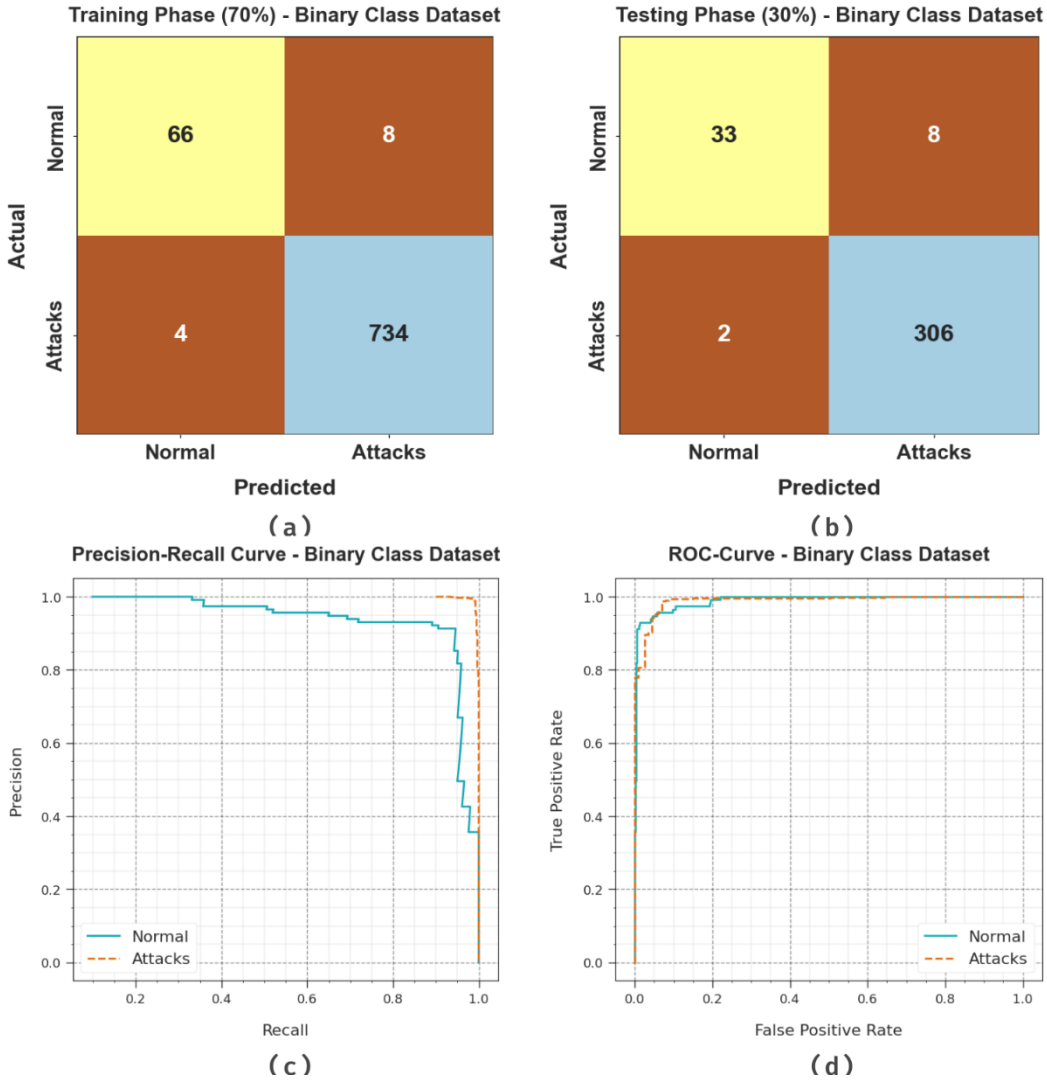

Figure 3: Binary class dataset of (a-b) Confusion matrices, (c) PR_curve, and (d) ROC

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024

The binary class detection results of the HMDL-IDCPSG approach can be inspected in Table 2 and Fig. 4. These achieved outcomes implies that the HMDL-IDCPSG system appropriately recognized the normal and attack instances. According to a 70% TRAPH, the HMDL-IDCPSG system provides average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 94.32%, 96.60%, 94.32%, 95.43%, and 94.32% respectively. Meanwhile, with 30% TESPH, the HMDL-IDCPSG algorithm offers average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 89.92%, 95.87%, 89.92%, 92.62%, and 89.92% correspondingly.

Table 2: Detection outcome of HMDL-IDCPSG model at binary class dataset

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	AUC_{Score}
TRAPH (70%)					
Normal	89.19	94.29	89.19	91.67	94.32
Attacks	99.46	98.92	99.46	99.19	94.32
Average	94.32	96.60	94.32	95.43	94.32
TESPH (30%)					
Normal	80.49	94.29	80.49	86.84	89.92
Attacks	99.35	97.45	99.35	98.39	89.92
Average	89.92	95.87	89.92	92.62	89.92

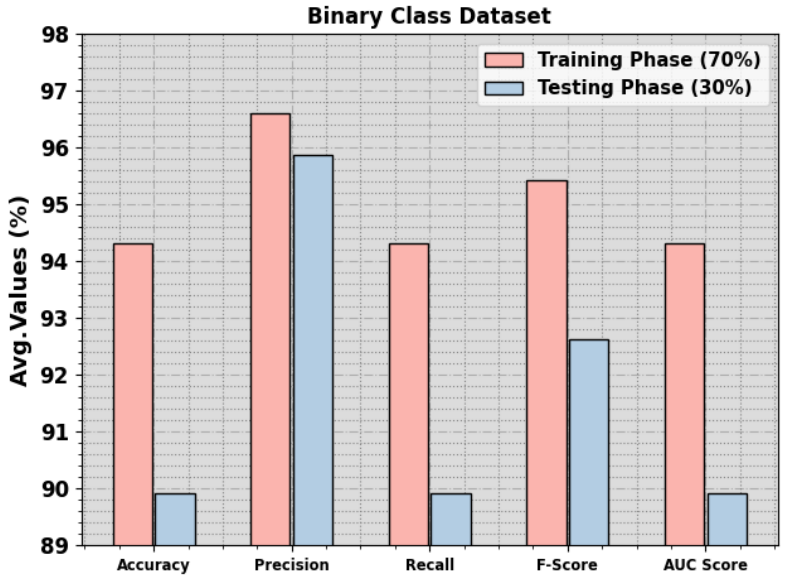

Figure 4: Average of HMDL-IDCPSG algorithm on a binary class dataset

Fig. 5 represents the training accuracy TR_accu_y and VL_accu_y of the HMDL-IDCPSG method at binary class dataset. The TR_accu_y will be determined by the assessment of the HMDL-IDCPSG method at the TRA dataset while the VL_accu_y can be calculated to evaluate the efficacy under a TRA dataset. These results highlighted that TR_accu_y and VL_accu_y raise with increased epochs. Subsequently, the effectiveness of the HMDL-IDCPSG method obtains increased under the TRA and TES dataset with an improvement of the varying epochs.

In Fig. 6, the TR_loss and VR_loss curve of the HMDL-IDCPSG system at binary class dataset is shown. The TR_loss determines the error amongst the predictable and actual values in the TRA data. The VR_loss signify the calculation of the effectiveness of the HMDL-IDCPSG method under validation data. These accomplished findings are denoted that the TR_loss and VR_loss tends to decrease with improving epochs. This portrayed the enhanced efficiency of the HMDL-IDCPSG technique and the capabilities to produce a precise classification. The minimized value of TR_loss and VR_loss demonstrates the improved effectiveness of the HMDL-IDCPSG method for capturing relationships and patterns.

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024

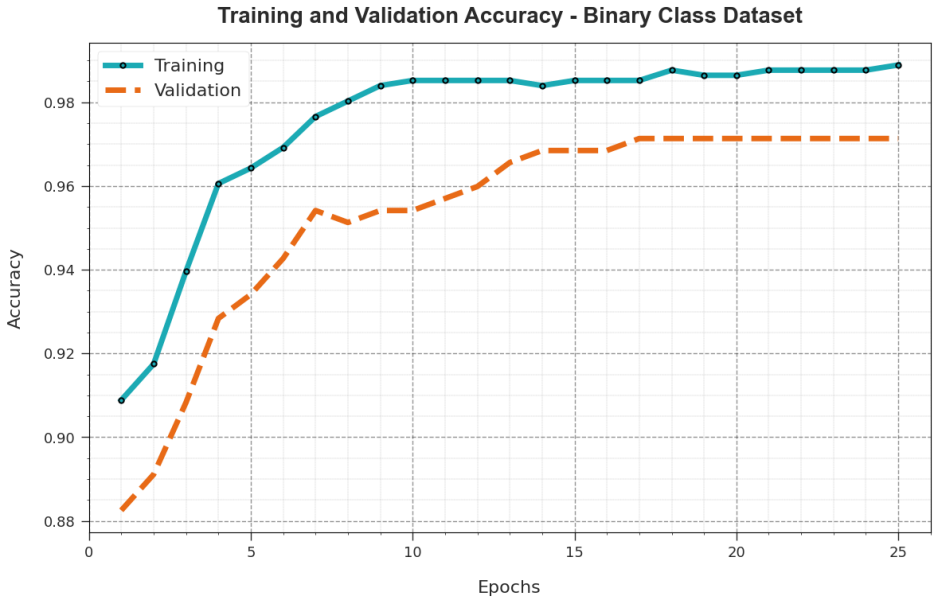

Figure 5: $Accu_y$ curve of HMDL-IDCPSG algorithm on a binary class dataset

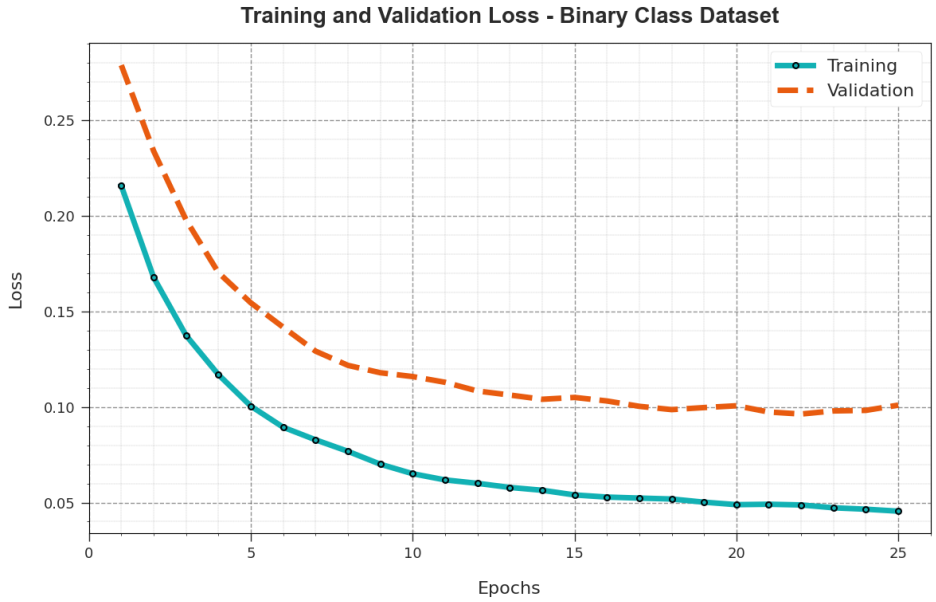

Figure 6: Loss curve of HMDL-IDCPSG algorithm on a binary class dataset

The comparative analysis of the HMDL-IDCPSG technique is determined under the binary class dataset, as demonstrated in Table 3 and Fig. 7 [11]. These experimental values notified that the vanilla-ANN, GRU, and RNN models have shown the least outcomes. Similarly, the LSTM and CNN algorithms have reported moderately improved results. Although the CNN-Bayesian algorithm reaches reasonable performance, the HMDL-IDCPSG technique outperforms the other recent approaches with maximum $accu_y$, $prec_n$, $reca_l$, and F_{score} of 94.32%, 96.60%, 94.32%, and 95.43%.

Table 3: Comparative result of HMDL-IDCPSG model with other techniques at binary class database

Binary Class Dataset				
Classifier	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
Vanilla-ANN	51.06	49.89	30.10	37.54
GRU	67.66	59.88	57.70	57.92
RNN	77.20	72.73	71.43	71.99

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024

LSTM	88.38	70.58	72.77	71.55
CNN	83.84	41.92	50.00	45.60
CNN-Bayesian	92.76	88.97	84.74	86.83
HMDL-IDCPSG	94.32	96.60	94.32	95.43

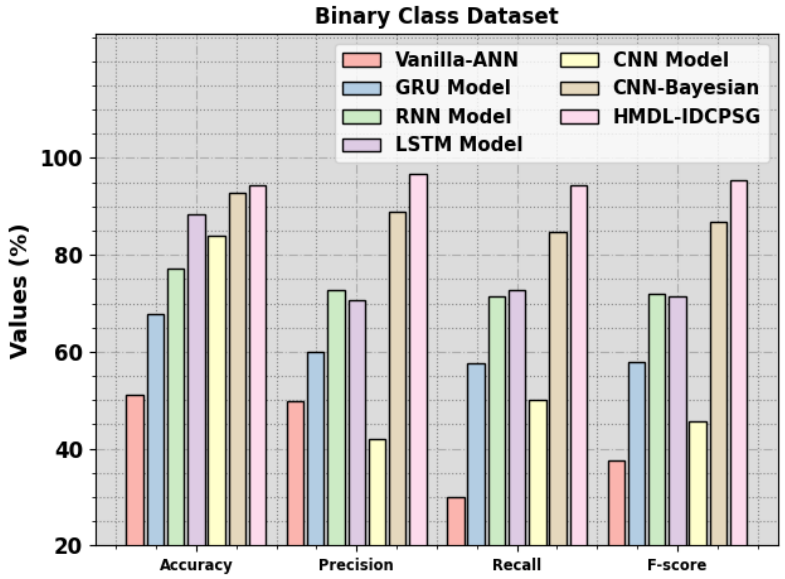

Figure 7: Comparative result of HMDL-IDCPSG model on a binary class dataset

The performance outcomes of the HMDL-IDCPSG approach can be examined at the multi-class dataset, which holds 115 normal samples, 1046 attack samples and 331 no-events samples as demonstrated in Table 4. The available 131 features, the HMDL-IDCPSG approach comprised to a total of 82 features.

Fig. 8 determines the classifier result of the HMDL-IDCPSG methodology at a multi-class database. Figs. 8a-8b signifies the confusion matrices achieved by the HMDL-IDCPSG system on 70:30 of the TRAPH/TESPH. These acquired results displayed that the HMDL-IDCPSG system has identified and categorized 3 classes accurately. Subsequently, Fig. 8c signifies the PR study of the HMDL-IDCPSG method. These obtained result values outperformed that the HMDL-IDCPSG algorithm has gained higher values of PR on 3 classes. But Fig. 8d reveals the ROC result of the HMDL-IDCPSG algorithm. This defined that the HMDL-IDCPSG algorithm gives a proficient solution with superior values of ROC on 3 classes.

The Multi-class detection outcome of the HMDL-IDCPSG method can be investigated in Table 5 and Fig. 9. These obtained outcomes show that the HMDL-IDCPSG system properly recognized the normal, attack, and no events samples. With a 70% TRAPH, the HMDL-IDCPSG system attains average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 94%, 90.07%, 81.86%, 85.43%, and 86.83% correspondingly. Then, with a 30% TESPH, the HMDL-IDCPSG algorithm achieves average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 94.49%, 89.16%, 81.48%, 84.48%, and 87.66% respectively.

Table 4 Details on Multi-class database

Multi-Class Dataset	
Class	No. of Samples
Normal	115
Attacks	1046
No Events	331
Total Samples	331

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024

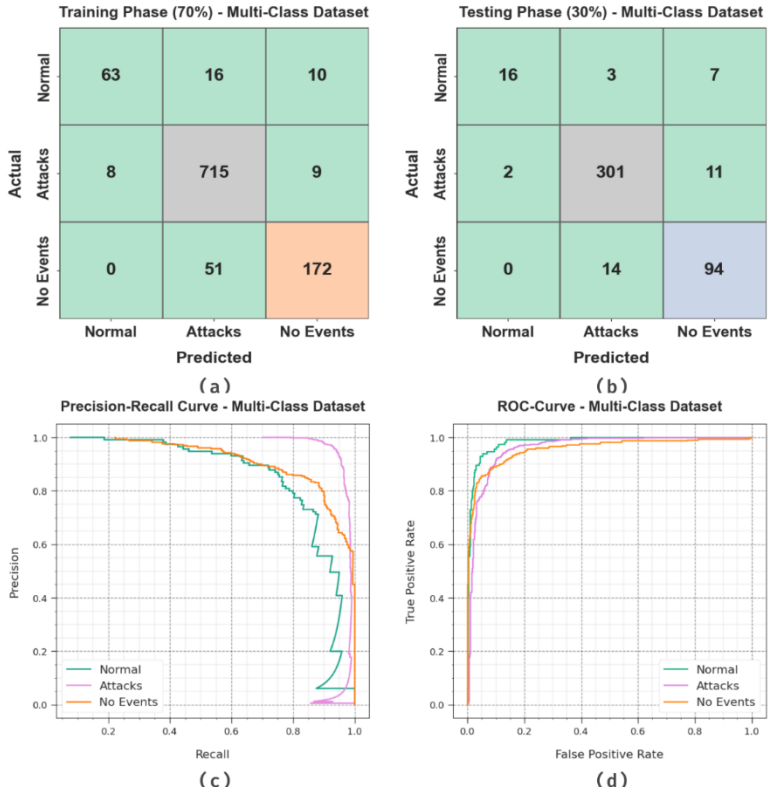

Figure 8: Multi-class dataset of (a-b) Confusion matrices, (c) PR_curve, and (d) ROC

Table 5: Detection outcome of HMDL-IDCPSG model on Multi-class dataset

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	AUC_{Score}
TRAPH (70%)					
Normal	96.74	88.73	70.79	78.75	84.97
Attacks	91.95	91.43	97.68	94.45	88.10
No Events	93.30	90.05	77.13	83.09	87.41
Average	94.00	90.07	81.86	85.43	86.83
TESPH (30%)					
Normal	97.32	88.89	61.54	72.73	80.53
Attacks	93.30	94.65	95.86	95.25	91.59
No Events	92.86	83.93	87.04	85.45	90.87
Average	94.49	89.16	81.48	84.48	87.66

Fig. 10 portrays the training accuracy TR_accu_y and VL_accu_y of the HMDL-IDCPSG approach on a multi-class dataset. The TR_accu_y can be measured by the estimation of the HMDL-IDCPSG method under the TRA dataset however, the VL_accu_y was measured by assessing the outcome on a TRA dataset. These results will be display that TR_accu_y and VL_accu_y improvement with raised epochs. Thus, the effectiveness of the HMDL-IDCPSG method offers raise on the TRA and TES dataset with improve the epochs count.

In Fig. 11, the TR_loss and VR_loss results of the HMDL-IDCPSG technique at the multi-class dataset are exposed. The TR_loss found out the error amongst the predicted and actual values under TRA data. The VR_loss represent the calculation of the efficacy of the HMDL-IDCPSG method under validation data. These achieved results indicates that the TR_loss and VR_loss tends for reducing with raised epochs. This can be represented the improved efficiency of the HMDL-IDCPSG algorithm and the capability for producing the correct classification. The lesser value of TR_loss and VR_loss determines the better solution of the HMDL-IDCPSG algorithm for taking patterns and relationships.

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024

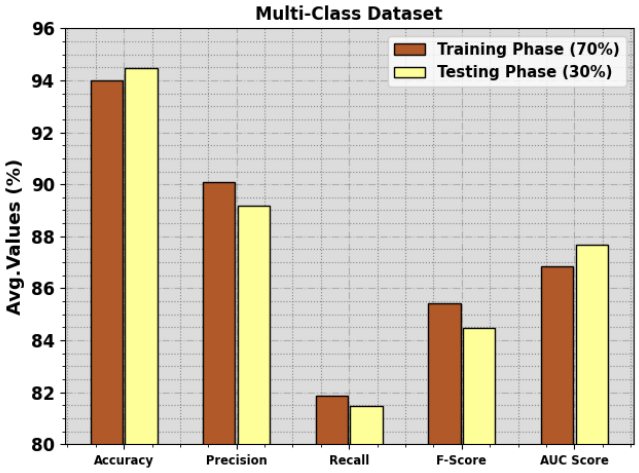

Figure 9: Average of HMDL-IDCPSG algorithm on Multi-class dataset

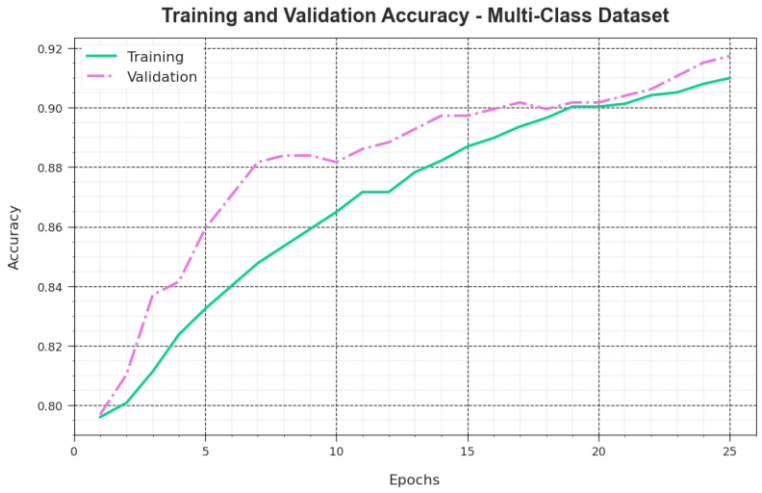

Figure 10: $Accu_y$ curve of HMDL-IDCPSG algorithm on Multi-class dataset

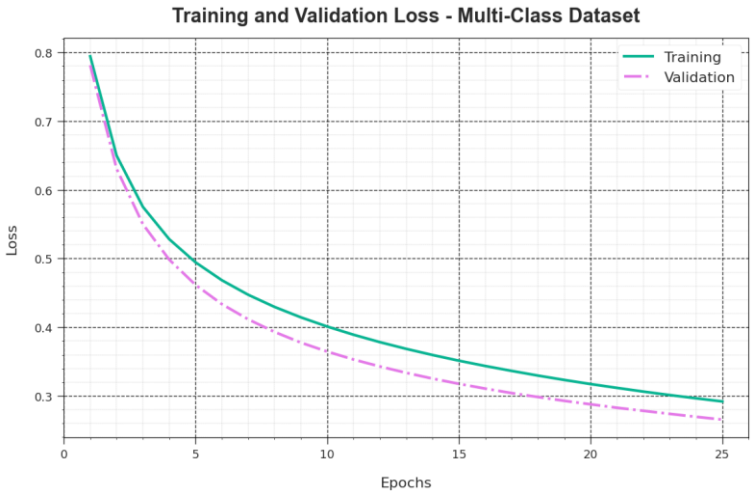

Figure 11: Loss curve of HMDL-IDCPSG algorithm on Multi-class dataset

An extensive comparative investigation of the HMDL-IDCPSG approach is tested at the multi-class dataset, as revealed in Table 6 and Fig. 12. These simulation values implied that the vanilla-ANN, GRU, and RNN methods have revealed the least outcomes. Besides, the LSTM and CNN models have reported somewhat better performances. But, the CNN-Bayesian algorithm reaches reasonable performance, the HMDL-IDCPSG method

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024

outperforms the other recent systems with maximal $accu_y$, $prec_n$, $reca_l$, and F_{score} of 94.49%, 89.16%, 81.48%, and 84.48%.

Table 6: Comparative result of HMDL-IDCPSG model with another algorithm under multi-class database

Multi-Class Dataset				
Classifier	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
Vanilla-ANN	69.62	48.77	33.33	39.59
GRU	70.96	51.78	33.33	40.55
RNN	71.02	62.87	35.15	45.09
LSTM	72.56	63.23	35.29	45.29
CNN	73.23	67.43	38.33	48.87
CNN-Bayesian	84.76	71.97	79.74	77.84
HMDL-IDCPSG	94.49	89.16	81.48	84.48

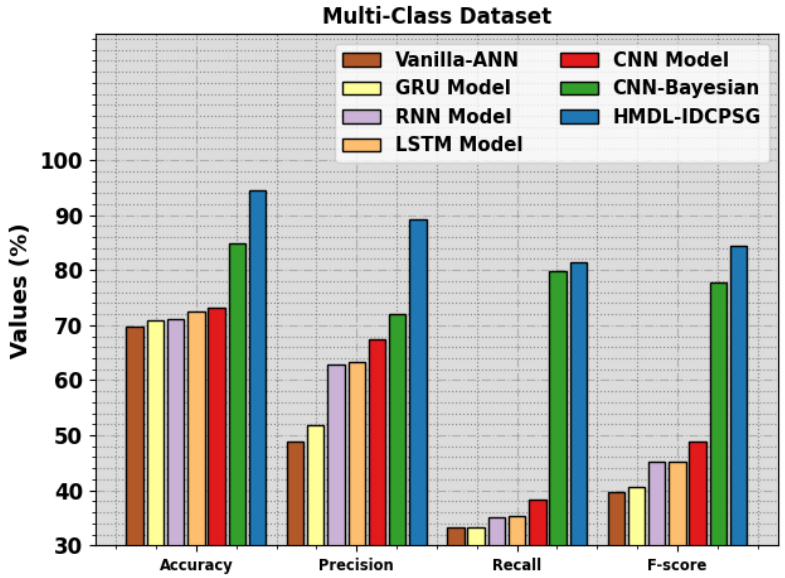

Figure 12: Comparative result of HMDL-IDCPSG algorithm on multi-class dataset

These outcomes confirmed the greater solution of the HMDL-IDCPSG technique on the intrusion detection procedure.

5. Conclusion

In this article, we have presented and developed of the HMDL-IDCPSG algorithm for the SG platform. The primary aim of the HMDL-IDCPSG technique gains the efficient recognition of the intrusions using feature selection (FS) and classification processes in the CPSG environment. In the presented HMDL-IDCPSG technique, three processes are involved namely BDA-DDO-based FS, ABiLSTM-based intrusion detection, and SSA-based parameter tuning. In this work, the HMDL-IDCPSG method includes the ABiLSTM method for the detection and classification of intrusions. Ultimately, the SSA could be utilized for optimum choosing the hyperparameter values of the ABiLSTM system that supports accomplishing enhanced performance. For demonstrating the greater solution of the HMDL-IDCPSG technique, a comprehensive simulation value is executed. The obtained results reported the supremacy of the HMDL-IDCPSG system with other existing approaches.

Funding: "This research received no external funding"

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

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024

References

[1] Li, X.J., Ma, M. and Sun, Y., 2023. An Adaptive Deep Learning Neural Network Model to Enhance Machine-Learning-Based Classifiers for Intrusion Detection in Smart Grids. Algorithms, 16(6), p.288.

[2] Mohanty, D., Sethi, K., Prasath, S., Rout, R.R. and Bera, P., 2021, June. Intelligent intrusion detection system for smart grid applications. In 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (pp. 1-8). IEEE.

[3] Ossama H. Embarak, Raed Abu Zitar, Securing Wireless Sensor Networks Against DoS attacks in Industrial 4.0, Journal of Intelligent Systems and Internet of Things, Vol. 8 , No. 1 , (2023) : 66-74 (Doi : https://doi.org/10.54216/JISIoT.080106)

[4] Khder Alakkari, Alhumaima Ali Subhi, Hussein Alkattan, Ammar Kadi, Artem Malinin, Irina Potoroko, Mostafa Abotaleb, El-Sayed M El-kenawy, A Comprehensive Approach to Cyberattack Detection in Edge Computing Environments, Journal of Cybersecurity and Information Management, Vol. 13 , No. 1 , (2024) : 69-75 (Doi : https://doi.org/10.54216/JCIM.130107)

[5] Gao, Y., Chen, J., Miao, H., Song, B., Lu, Y. and Pan, W., 2022. Self-learning spatial distribution-based intrusion detection for industrial cyber-physical systems. IEEE Transactions on Computational Social Systems, 9(6), pp.1693-1702.

[6] Althobaiti, M.M., Kumar, K.P.M., Gupta, D., Kumar, S. and Mansour, R.F., 2021. An intelligent cognitive computing-based intrusion detection for industrial cyber-physical systems. Measurement, 186, p.110145.

[7] Santoso, F. and Finn, A., 2022. A Data-Driven Cyber–Physical System Using Deep-Learning Convolutional Neural Networks: Study on False-Data Injection Attacks in an Unmanned Ground Vehicle Under Fault-Tolerant Conditions. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 53(1), pp.346-356.

[8] Li, Y., Xue, W., Wu, T., Wang, H., Zhou, B., Aziz, S. and He, Y., 2021. Intrusion detection of cyber physical energy system based on multivariate ensemble classification. Energy, 218, p.119505.

[9] Faya Safar, Raddad Al King, Data Security in Cloud Computing, International Journal of Wireless and Ad Hoc Communication, Vol. 7 , No. 1 , (2023) : 50-61 (Doi : https://doi.org/10.54216/IJWAC.070105)

[10] Song, C., Sun, Y., Han, G. and Rodrigues, J.J., 2021. Intrusion detection based on hybrid classifiers for smart grid. Computers & Electrical Engineering, 93, p.107212.

[11] Kaur, D., Anwar, A., Kamwa, I., Islam, S., Muyeen, S.M. and Hosseinzadeh, N., 2023. A Bayesian Deep Learning Approach With Convolutional Feature Engineering to Discriminate Cyber-Physical Intrusions in Smart Grid Systems. IEEE Access, 11, pp.18910-18920.

[12] Goyel, H. and Swarup, K.S., 2022. Data Integrity Attack Detection Using Ensemble-Based Learning for Cyber–Physical Power Systems. IEEE Transactions on Smart Grid, 14(2), pp.1198-1209.

[13] Sakhnini, J., Karimipour, H., Dehghantanha, A. and Parizi, R.M., 2021. Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach. Physical Communication, 47, p.101394.

[14] Bitirgen, K. and Filik, Ü.B., 2023. A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid. International Journal of Critical Infrastructure Protection, 40, p.100582.

[15] Mukherjee, D., Chakraborty, S., Abdelaziz, A.Y. and El-Shahat, A., 2022. Deep learning-based identification of false data injection attacks on modern smart grids. Energy Reports, 8, pp.919-930.

[16] Dairi, A., Harrou, F., Bouyeddou, B., Senouci, S.M. and Sun, Y., 2023. Semi-supervised deep learning-driven anomaly detection schemes for cyber-attack detection in smart grids. In Power Systems Cybersecurity: Methods, Concepts, and Best Practices (pp. 265-295). Cham: Springer International Publishing.

[17] Gupta, P.K., Singh, N.K. and Mahajan, V., 2021. Intrusion detection in cyber-physical layer of smart grid using intelligent loop based artificial neural network technique. International Journal of Engineering, 34(5), pp.1250-1256.

[18] Mhmood, A.A., Ergül, Ö. and Rahebi, J., 2023. Detection of Cyber Attacks on Smart Grids Using Improved VGG19 Deep Neural Network Architecture and Aquila Optimizer Algorithm.

[19] Chen, Y., Gao, B., Lu, T., Li, H., Wu, Y., Zhang, D. and Liao, X., 2023. A Hybrid Binary Dragonfly Algorithm with an Adaptive Directed Differential Operator for Feature Selection. Remote Sensing, 15(16), p.3980.

[20] Yousaf, K. and Nawaz, T., 2022. A deep learning-based approach for inappropriate content detection and classification of youtube videos. IEEE Access, 10, pp.16283-16298.

[21] Du, J., Yang, K., Hu, Y. and Jiang, L., 2023. Nids-cnnlstm: Network intrusion detection classification model based on deep learning. IEEE Access, 11, pp.24808-24821.

[22] Du, Y., Yuan, H., Jia, K. and Li, F., 2023. Research on Threshold Segmentation Method of Two-dimensional Otsu Image Based on Improved Sparrow Search Algorithm. IEEE Access.

[23] https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets

DOI: https://doi.org/10.54216/IJWAC.080206
Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024