International Journal of Wireless and Ad Hoc Communication

♦ ISSN: 2692-4056 Vol: 08, No .02, 2024 ♦ PP. 29–34

Article DOI: https://doi.org/10.54216/IJWAC.080206



FULL LENGTH ARTICLE

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

Received: September 09, 2023 Revised: December 12, 2023 Accepted: May 19, 2024 ⋆ Corresponding author

ABSTRACT

Smart grids (SGs) can ensure continuous power supply, decreased line losses, improved renewable output and storage, user participation in electricity markets, and demand-side responsiveness. The development of cyber-physical SG (CPSG) systems has transformed the standard power grid by allowing bi-directional energy flow among utilities and users. However, increased data exchange among consumers presents a major problem for firewall systems in transmission networks at both cyber and physical planes. Intrusion Detection Systems (IDSs) play an essential role in maintaining SG systems against cyber threats by generating a second wall of defense that complements conventional preventive security procedures such as authorization, encryption, and authentication. Therefore, this article concentrates on the design and development of Hybrid Metaheuristics with Deep Learning Assisted Intrusion Detection in Cyber-Physical Smart Grid (HMDL-IDCPSG) infrastructure. The major objective of the HMDL-IDCPSG system is effective intrusion recognition using feature selection and classification processes in CPSG infrastructure. In the presented HMDL-IDCPSG method, a binary dragonfly algorithm with the hybrid directed differential operator (BDA-DDO) is implemented for feature selection. Besides, an attention-based bi-directional long short-term memory (ABiLSTM) algorithm is carried out for recognizing and classifying intrusions. Finally, the sparrow search algorithm (SSA) is exploited to choose the hyperparameter values of the ABiLSTM algorithm, supporting better solutions. Simulation results report the supremacy of the HMDL-IDCPSG methodology compared with 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 end users [1]. It contains improved measuring and communication technologies and control methods executed at the cyber plane of cyber-physical smart-grid (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 such as phasor measurement units (PMUs) for complex control functions and higher-resolution monitoring [2].

Since network size and attack types continue to grow, communication networks can be susceptible to cyber vulnerabilities. Users now interact directly with the grid through smart appliances, increasing the possibility of cyberattacks in CPSG platforms [3]. Additionally, interventions occurring at cy-

© 2024The Author(s). Published by ASPG. This article is licensed under CC BY 4.0.

ber and physical planes may be caused by manual or natural attacks. Therefore, differentiating power-system interventions is essential for supporting cyberattack identification and control abilities [4].

Intrusion detection systems monitor traffic data flow and identify suspicious activities or attacks by detecting unauthorized access and generating alarms for administrators [5]. IDSs are commonly classified into anomaly-based and signature-based systems. Anomaly-based IDSs detect attacks based on deviations from normal activity, whereas signature-based IDSs compare traffic with known attack models [6]. Depending on location, IDSs can be host-based or network-based. In smart-grid platforms, the chosen IDS architecture must match whether the system is centralized, decentralized, or distributed [7].

As a cyber-physical system, failure to detect interventions in SGs may create physical effects on power systems, including loss of control, major blackouts, and system failure [8]. Machine learning and deep learning are therefore important tools for improving IDS efficiency, but high-dimensional data, feature redundancy, and the requirement for optimized hyperparameters remain key challenges. This work proposes the HMDL-IDCPSG method, combining BDA-DDO feature selection, ABiLSTM intrusion detection, and SSA-based hyperparameter tuning.

2. RELATED WORKS

Several recent studies have investigated IDS techniques for smart grids and industrial cyber-physical systems. Kaur et al. [9] presented a Bayesian technique incorporated with deep CNNs (CNN-Bayesian) to differentiate CPS intrusions from normal activities in binary and multiclass settings. Goyel and Swarup [10] offered optimization methods to build false data injection attacks (FDIA) against state-prediction techniques at the control center. Sakhnini et al. [11] introduced an intelligent attack-identification and localization method based on an ensemble of machine-learning techniques.

Bitirgen and Filik [12] presented an optimized CNN-LSTM with particle swarm optimization (PSO) for FDIA detection in SG systems. Mukherjee et al. [13] suggested a real-time FDIA detection algorithm through a deep-learning-based state-prediction method and an intrusion-detection method using error covariance matrices. Dairi et al. [14] developed two semi-supervised hybrid deep-learning anomaly-detection techniques for IDS in ICS traffic of SGs: AE-GRU and GAN-RNN.

Gupta et al. [15] recommended an Intelligent Loop Based ANN (IL-ANN) identification method that compares abnormalities in the model with load profiles under architecture nodes. Mhmood et al. [16] introduced an intelligent IDS that combines CGAN, game theory, Aquila Optimization for feature selection, RGB image encoding of selected features, and optimized meta-parameters.

3. THE PROPOSED MODEL

This article concentrates on the HMDL-IDCPSG algorithm for the SG platform. The major aim is effective recognition of intrusions using feature-selection and classification processes in the CPSG environment. The presented method includes three processes: BDA-DDO-based feature selection, ABiLSTM-based intrusion detection, and SSA-based parameter tuning. Figure 1 portrays the complete procedure.

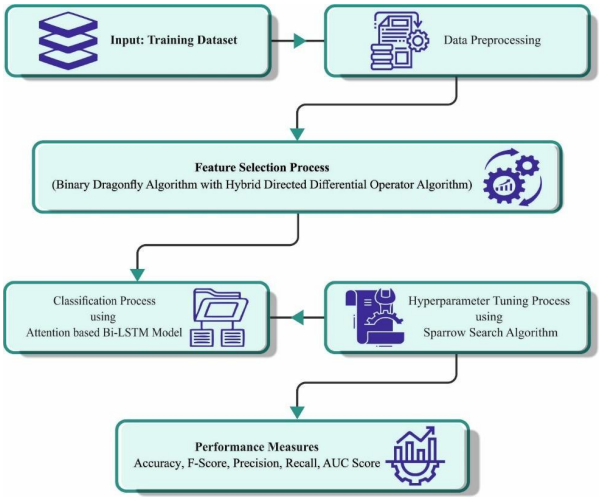


Figure 1. Overall process of the HMDL-IDCPSG method.

3.1 Feature Selection Using BDA-DDO Algorithm

The BDA-DDO method is designed for choosing an optimum feature set. In BDA-DDO, a directed differential operator fuses BDA-generated individuals with a differential operator, leading to fast convergence [17]. The fitness function evaluates solution quality. Mutation of the ith individual generates the mutation vector:

$$V_i = X_i + F \times (X_{Food} - X_{Enemy}). \tag{1}$$

Here, X_{Enemy} is the position of enemies, X_i denotes the updated BDA individual location, X_{Food} characterizes the better position, and F is the scaling factor.

The binomial crossover operator is:

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

Using transfer function T_1, the resultant vector is transformed into a discrete space:

$$T_1 = \frac{1}{1+e^{-U_i^d}}, \tag{3}$$

$$U_{i,j} = \begin{cases} 0, & rand < T_1, \\ 1, & rand > T_1. \end{cases} \tag{4}$$

Selection determines survival in the next generation:

$$X_i = \begin{cases} U_i, & f(U_i) \leq f(X_i), \\ X_i, & \text{otherwise}. \end{cases} \tag{5}$$

The time-varying differential vector is:

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

and the adaptive step update is:

$$\Delta X = F \times \Delta X. \tag{7}$$

Feature selection is modeled as a multiobjective problem balancing minimum subset size and maximum classification accuracy:

$$fitness = \alpha \times ERR + \beta \times \frac{R}{N}. \tag{8}$$

Here, ERR denotes classifier error rate, R is the number of selected features, N is the total number of features, and α and $\beta = 1-\alpha$ balance classification performance and feature subset size.

3.2 Intrusion Detection Utilizing ABiLSTM Model

The ABiLSTM model is implemented for detection and classification of intrusions. LSTM is widely employed in network intrusion detection to resolve gradient-vanishing problems caused by recurrent neural networks [18]. It contains forget, input, and output gates that preserve long-term memory. Figure 2 depicts the ABiLSTM framework.

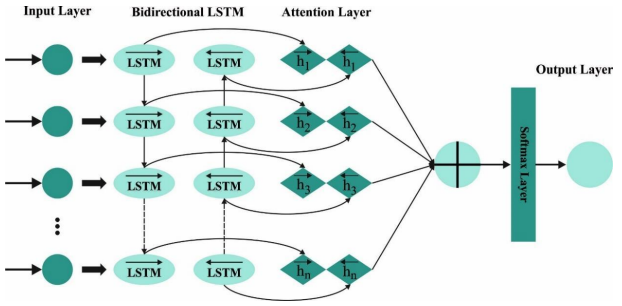


Figure 2. Architecture of ABiLSTM model.

The forget gate computation is:

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

The input gate and candidate cell state are:

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

$$\widetilde{C}_t = \tanh\left(W_c \cdot [h_{t-1}, x_t] + b_c\right). \tag{11}$$

The final cell state is:

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

The output gate and hidden state are:

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

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

Assuming the final hidden layer of the ith BLSTM is h_{it}, the attention mechanism is computed as follows [19]:

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

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

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

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

3.3 Parameter Tuning Utilizing SSA

SSA is implemented to choose the hyperparameter values of the ABiLSTM method. It is a population optimizer that updates the positions of discoverers, followers, and vigilantes during foraging, where the position of optimal food corresponds to the optimal solution [20]. When there are n sparrows in the population, the population matrix and fitness vector are:

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

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

The discoverer position is renewed by:

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

The follower position is updated by:

$$x_{ij}^{t+1} = \begin{cases} Q \cdot \exp\left(\dfrac{x_{worst}^t - x_{ij}^t}{i^2}\right), & i > n/2, \\ x_p^{t+1} + |x_{ij} - x_p^{t+1}| \cdot Z^+ \cdot L, & i \leq n/2. \end{cases} \tag{22}$$

The vigilante position is updated as:

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

The optimized fitness is defined by classifier error rate:

$$fitness(x_i) = ClassifierErrorRate(x_i) \tag{24}$$

$$= \frac{\text{No. of misclassified instances}}{\text{Total no. of instances}} \times 100. \tag{25}$$

4. RESULTS AND DISCUSSION

This section explains the intrusion-detection outcome of the HMDL-IDCPSG system on the ICS dataset [21]. Experiments are examined using binary-class and multiclass datasets. From the available 129 features, the HMDL-IDCPSG system selected 76 features for the binary-class experiment.

Table 1. Details on binary class database.

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

Figure 3 illustrates classifier performance on the binary-class database, including confusion matrices, PR curve, and ROC curve.

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

Class	Accuy	Precn	Recal	FScore	AUCScore
Training Phase (70%)					
Normal	94.32	53.85	94.59	68.63	94.45
Attacks	94.32	99.35	94.29	96.75	94.45
Average	94.32	96.60	94.32	95.43	94.32
Testing Phase (30%)					
Normal	89.92	39.13	93.10	55.10	91.22
Attacks	89.92	99.25	89.68	94.22	91.22
Average	89.92	95.87	89.92	92.62	89.92

The training and validation accuracy/loss behavior of the HMDL-IDCPSG algorithm on the binary dataset is shown in

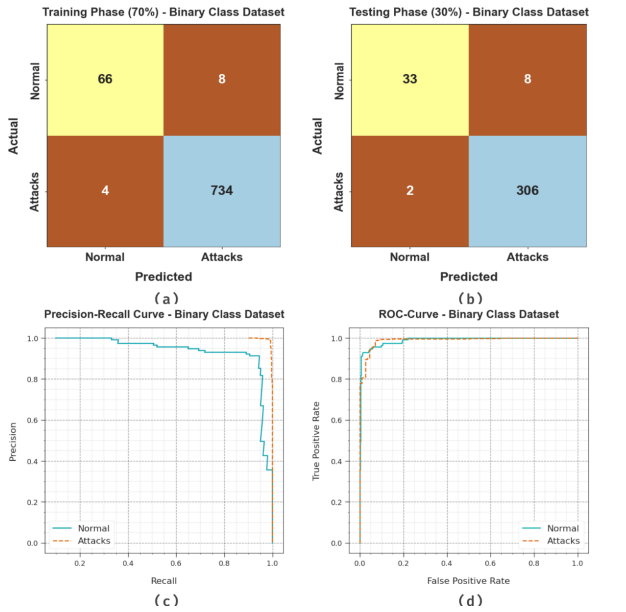


Figure 3. Binary class dataset of (a–b) confusion matrices, (c) PR curve, and (d) ROC.

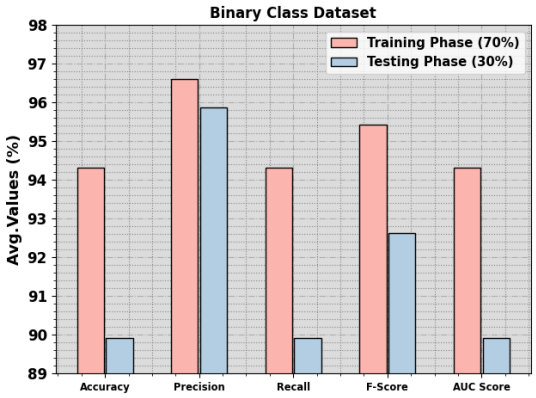


Figure 4. Average of HMDL-IDCPSG algorithm on a binary class dataset.

Figures 5 and 6. The curves show improvement in training and validation accuracy with increased epochs, while loss tends to decrease.

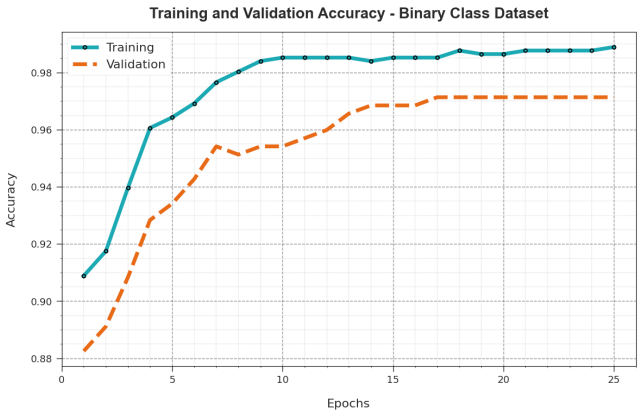


Figure 5. Accuracy curve of HMDL-IDCPSG algorithm on a binary class dataset.

For the multiclass database, the dataset includes natural, attack, and no-event samples, as shown in Table 4. Figure 8 presents the multiclass confusion matrices, PR curve, and ROC curve.

Figures 10 and 11 show the training and validation behavior for the multiclass dataset. Accuracy improves with epochs,

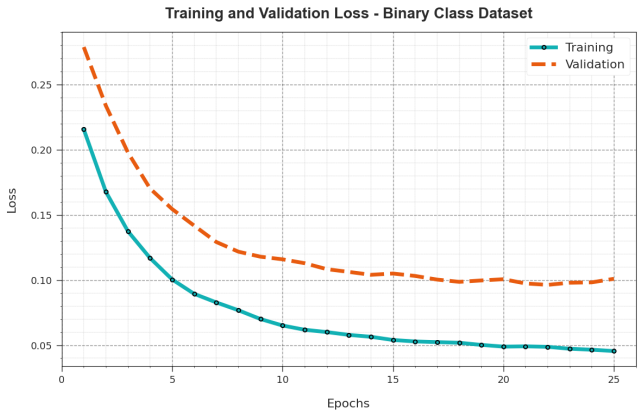


Figure 6. Loss curve of HMDL-IDCPSG algorithm on a binary class dataset.

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

Classifier	Accuy	Precn	Recal	FScore
Vanilla-ANN	78.64	50.00	50.00	50.00
GRU	81.79	72.28	63.34	66.86
RNN	86.68	78.84	75.12	76.57
LSTM	88.39	81.95	78.70	80.08
CNN	88.68	83.44	75.79	78.63
CNN-Bayesian	89.42	87.50	73.55	77.93
HMDL-IDCPSG	89.92	95.87	89.92	92.62

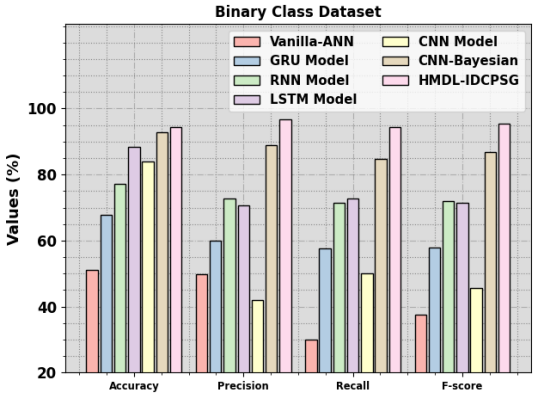


Figure 7. Comparative result of HMDL-IDCPSG model on a binary class dataset.

Table 4. Details on multi-class database.

Class	No. of Instances
Natural	115
Attack	556
No Events	490
Total Instances	1161

Table 5. Detection outcome of HMDL-IDCPSG model on multi-class dataset.

Class	Accuy	Precn	Recal	FScore	AUCScore
Training Phase (70%)					
Natural	96.70	84.15	93.24	88.46	96.36
Attack	96.70	96.15	97.66	96.90	96.91
No Events	96.70	99.12	96.30	97.69	96.93
Average	96.70	96.77	96.70	96.72	96.70
Testing Phase (30%)					
Natural	94.49	67.50	93.10	78.26	94.74
Attack	94.49	95.04	91.62	93.30	93.61
No Events	94.49	96.88	98.58	97.72	96.32
Average	94.49	89.16	81.48	84.48	87.66

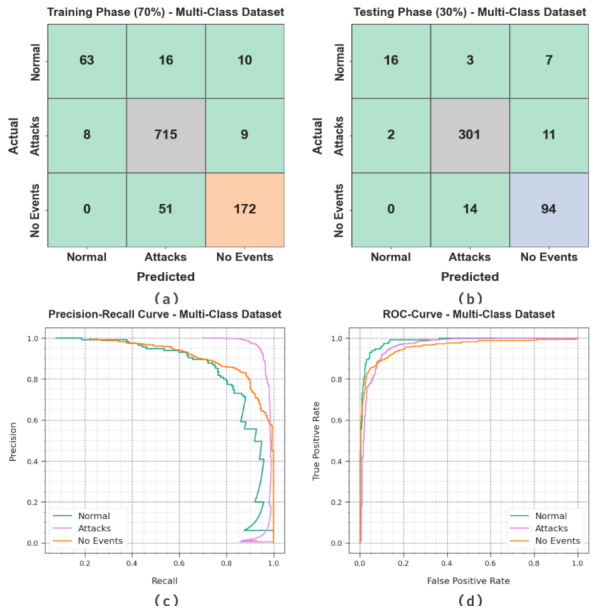


Figure 8. Multi-class dataset of (a–b) confusion matrices, (c) PR curve, and (d) ROC.

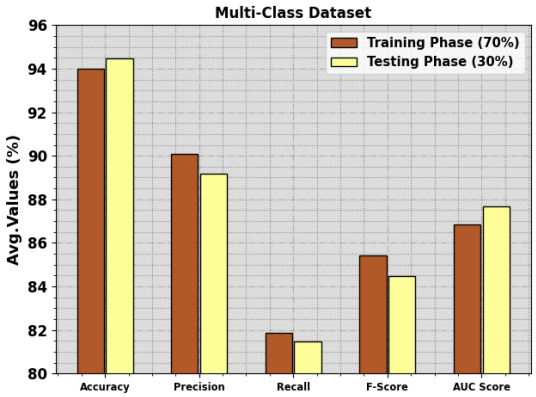


Figure 9. Average of HMDL-IDCPSG algorithm on multi-class dataset.

and loss values decrease, indicating the ability of HMDL-IDCPSG to model relationships and generate correct classifications.

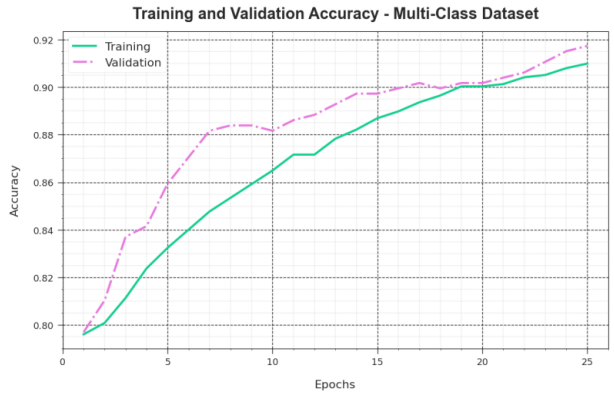


Figure 10. Accuracy curve of HMDL-IDCPSG algorithm on multi-class dataset.

These outcomes confirm the stronger solution of the HMDL-IDCPSG technique for the intrusion-detection procedure. For the binary dataset, the method provides average accuracy, precision, recall, F-score, and AUC score of 89.92%, 95.87%, 89.92%, 92.62%, and 89.92%, respectively, in testing. For the multiclass dataset, the HMDL-IDCPSG method outperforms

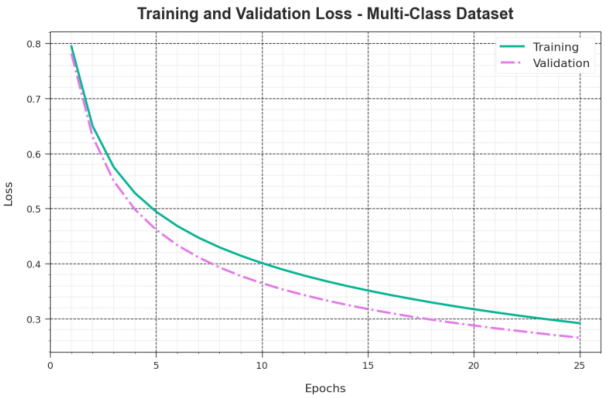


Figure 11. Loss curve of HMDL-IDCPSG algorithm on multi-class dataset.

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

Classifier	Accuy	Precn	Recal	FScore
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

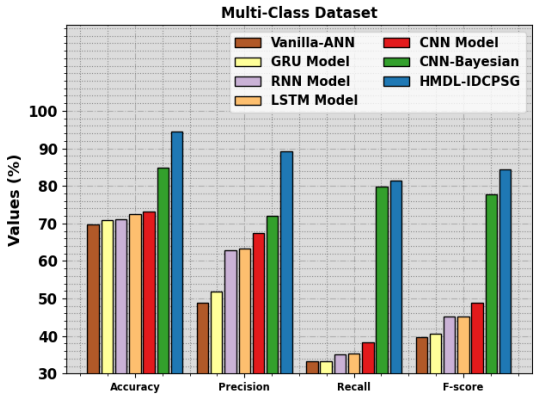


Figure 12. Comparative result of HMDL-IDCPSG algorithm on multi-class dataset.

other recent systems with accuracy, precision, recall, and F-score of 94.49%, 89.16%, 81.48%, and 84.48%, respectively.

5. CONCLUSION

In this article, the HMDL-IDCPSG algorithm for the smart-grid platform has been presented and developed. The primary aim is efficient intrusion recognition using feature selection and classification processes in the CPSG environment. The presented technique includes BDA-DDO-based feature selection, ABiLSTM-based intrusion detection, and SSA-based parameter tuning. The SSA is utilized to choose optimal hyperparameter values of the ABiLSTM system, supporting enhanced performance. Comprehensive simulation results report the supremacy of the HMDL-IDCPSG system compared with existing approaches.

Funding: This research received no external funding.

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

REFERENCES

[1] X. J. Li, M. Ma, and Y. Sun, "An adaptive deep learning neural network model to enhance machine-learning-based classifiers for intrusion detection in smart grids," *Algorithms*, vol. 16, no. 6, p. 288, 2023.

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

[3] O. H. Embarak and R. A. Zitar, "Securing wireless sensor networks against dos attacks in industrial 4.0," *Journal of Intelligent Systems and Internet of Things*, vol. 8, no. 1, pp. 66–74, 2023.

[4] K. Alakkari, A. A. Subhi, H. Alkattan, A. Kadi, A. Malinin, I. Potoroko, M. Abotaleb, and E.-S. M. El-kenawy, "A comprehensive approach to cyberattack detection in edge computing environments," *Journal of Cybersecurity and Information Management*, vol. 13, no. 1, pp. 69–75, 2024.

[5] Y. Gao, J. Chen, H. Miao, B. Song, Y. Lu, and W. Pan, "Self-learning spatial distribution-based intrusion detection for industrial cyber-physical systems," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 6, pp. 1693–1702, 2022.

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

[7] F. Santoso and A. Finn, "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*, vol. 53, no. 1, pp. 346–356, 2022.

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

[9] D. Kaur, A. Anwar, I. Kamwa, S. Islam, S. M. Muyeen, and N. Hosseinzadeh, "A bayesian deep learning approach with convolutional feature engineering to discriminate cyber-physical intrusions in smart grid systems," *IEEE Access*, vol. 11, pp. 18 910–18 920, 2023.

[10] H. Goyel and K. S. Swarup, "Data integrity attack detection using ensemble-based learning for cyber–physical power systems," *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1198–1209, 2022.

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

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

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

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

[15] P. K. Gupta, N. K. Singh, and V. Mahajan, "Intrusion detection in cyber-physical layer of smart grid using intelligent loop based artificial neural network technique," *International Journal of Engineering*, vol. 34, no. 5, pp. 1250–1256, 2021.

[16] A. A. Mhmood, Ö. Ergül, and J. Rahebi, "Detection of cyber attacks on smart grids using improved vgg19 deep neural network architecture and aquila optimizer algorithm," 2023.

[17] Y. Chen, B. Gao, T. Lu, H. Li, Y. Wu, D. Zhang, and X. Liao, "A hybrid binary dragonfly algorithm with an adaptive directed differential operator for feature selection," *Remote Sensing*, vol. 15, no. 16, p. 3980, 2023.

[18] K. Yousaf and T. Nawaz, "A deep learning-based approach for inappropriate content detection and classification of youtube videos," *IEEE Access*, vol. 10, pp. 16 283–16 298, 2022.

[19] J. Du, K. Yang, Y. Hu, and L. Jiang, "Nids-cnnlstm: Network intrusion detection classification model based on deep learning," *IEEE Access*, vol. 11, pp. 24 808–24 821, 2023.

[20] Y. Du, H. Yuan, K. Jia, and F. Li, "Research on threshold segmentation method of two-dimensional otsu image based on improved sparrow search algorithm," *IEEE Access*, 2023.

[21] "Ics data sets," https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets.