Leveraging Digital Twins with Hybrid Deep Learning Model for Robust Intrusion Detection System in Smart City Environment

Nouf Atiahallah Alghanmi[1,*]

[1]Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, P. O. Box 344, Rabigh 21911, Saudi Arabia

Emails: naalganmy@kau.edu.sa

Abstract

Cyber-physical systems (CPSs) unite the computation with physical methods. Embedded networks and computers observe and handle the physical procedures, generally with feedback encircles whereas physical procedures affect computation and conversely. In the last decade, the prompt growth of network-associated services has formed confidential information on the Internet. However, networks are much inclined to intrusions wherever unapproved consumers try to retrieve confidential data and even disturb the systems. Constructing a proficient network intrusion detection system (IDS) can be essential to avert these attacks. Utilizing digital twin technology enhances the IDS of physical devices in CPSs. IDSs normally utilize machine learning (ML) techniques for categorizing the attacks. However, the features employed for classifications are not appropriate or adequate all the time. Moreover, the amount of intrusions can be significantly lower than the amount of non-intrusions. Therefore, simple techniques may fail to deliver satisfactory performances owing to this class imbalance. In this study, we offer a Metaheuristic-Driven Hybrid Deep Learning Model for Robust Intrusion Detection in Secure Cyber-Physical Systems (MHDLM-RIDCPS) model in Smart City Environment. The proposed MHDLM-RIDCPS technique primarily targets the classification and recognition of intrusions using digital twin technology to enhance security within the CPS. Primarily, the proposed MHDLM-RIDCPS approach utilizes min-max normalization for transforming an input data into a standardized format. To alleviate dimensionality issues, the coyote optimization algorithm (COA) can be executed to select a subset of features. In addition, the modified prairie dog optimizer (mPDO) combined with a convolutional neural network and bi-directional long short-term memory with attention mechanism (AM-CNN+BiLSTM) classifier is exploited for the identification of intrusions. The design of the mPDO system primarily concentrates on the parameter optimizer of the AM-CNN+BiLSTM algorithm and so improves the classifier performances. To determine the greater efficiency of the MHDLM-RIDCPS system, a comprehensive set of simulations can be applied and the performances are tested over distinct aspects. The experimental analysis guaranteed the superior results of the MHDLM-RIDCPS methodology with existing methods

Keywords: Intrusion Detection; Smart City Environment; Cyber-Physical System; Metaheuristic Algorithm; Deep Learning; Attack; Feature Selection; Digital Twins

1. Introduction

Cyber-physical systems (CPS) a powerfully united pattern of computing methods, communication devices, and physical systems, are shown to present numerous security difficulties due to their fundamental composite design [1]. The CPS has comprehensive applications contains aviation, civil, transport industry, consumer, and chemical applications, and in the areas of manufacturing and healthcare. The CPS attack might generate a breakdown of the system and miss confidential information from the hackers [2]. This might lead to numerous damages. To prevent losses to users and systems, it is basic to design and deploy secured CPS. It may help in retaining security and privacy for CPS and additionally increase the application's qualities. CPS security is a development of conventional cybersecurity, where the process of the physical method has been additionally considered [3]. The important privacy issue in the conventional cybersecurity field due to the personal data leakage risks can be password cracking which is a password recovery technique for the methods. In CPS security, simpler data leakages cannot

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

harm the CPSs; however, the process of the physical method by prohibited accessibility with a password may affect the movement of the physical system [4]. Digital twins in CPS within a smart city environment enable real-time monitoring and management of urban infrastructure, enhancing efficiency and responsiveness. Fig. 1 depicts the general structure of digital twins in smart city environment.

Intrusion detection is a crucial task to improve securities in CPSs. For performing such a task, an intrusion detection system (IDS) has been required. Adequate research has been devoted to IDS. It is classified into dual major classes of misappropriation and anomaly detection [5]. In the initial situation, features of system vulnerabilities or known attacks are utilized for misuse detection. After executing misuse detection, the audited data are in comparison with the database, and some compliance would be described as an intrusion. Misuse detectors give smaller false positives; nevertheless, these kinds of detectors have their particular limitations as well [6]. For example, upgrading and creating a complete database is a cumbersome task. Additionally, they can only detect formerly identified attacks. Numerous models were presented for intrusion detection.

To overcome the restriction of legacy model-based CPS security, the data-driven anomalies detection approach has been changed in CPS security [7]. Particularly, Deep Learning (DL) and machine learning (ML) display a correlation between input and output by a larger amount of information without modelling-based physical laws, which can be revised in CPS security to satisfy consistency points and high-level safety [8]. Additionally, the ML algorithm allows a model to be completed for the massive and complex relations of each of the CPS components, connecting numerous physical methods in real-time, composite software applications, and various network protocols in the cyber world, the produced model can increase the security levels of the CPSs [9]. In recent times, investigators to make IDS effective in classifying malicious attacks have presented numerous DL- and ML-based solutions. However, the massive growth in the network traffic and the resultant safety threats have posed several challenges for the IDS systems to identify malicious intrusions effectively in cyber-physical environments [10].

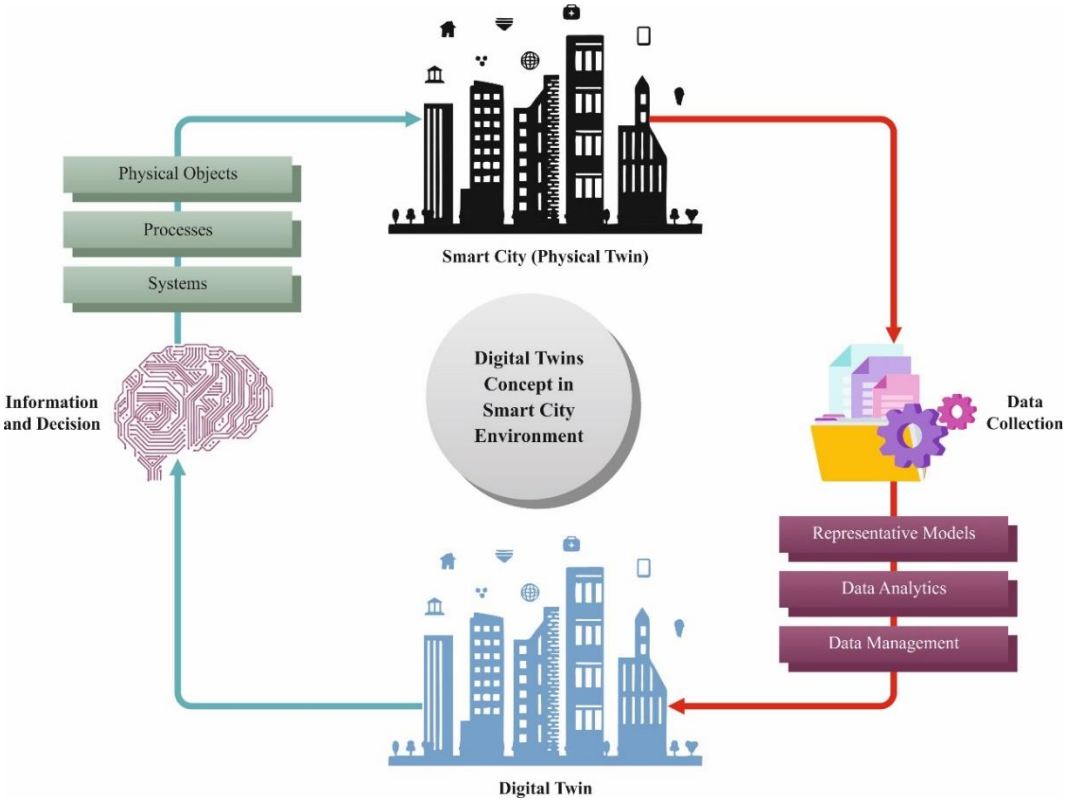

Figure 1. General architecture of Digital Twins in Smart City Environment

This study offers a Metaheuristic-Driven Hybrid Deep Learning Models for Robust Intrusion Detection in Secure Cyber-Physical Systems (MHDLM-RIDCPS) method in Smart City Environment. The proposed MHDLM-RIDCPS technique primarily targets the classification and recognition of intrusions using digital twin technology to enhance security within the CPS. Primarily, the proposed MHDLM-RIDCPS approach utilizes min-max normalization to transform the input data into a standardized format. To alleviate dimensionality issues, the coyote optimization algorithm (COA) can be executed to select a subset of features. In addition, the modified prairie dog

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

optimizer (mPDO) combined with a convolutional neural network and bi-directional long short-term memory with attention mechanism (AM-CNN+BiLSTM) classifier is exploited for the identification of intrusions. The design of the mPDO system primarily concentrates on the parameter optimizer of the AM-CNN+BiLSTM algorithm and so improves the classifier performances. The experimental analysis guaranteed the superior results of the MHDLM-RIDCPS methodology with existing approaches.

2. Literature Review

The authors [11] presented an effectual IDS model, which utilizes either ML-based approaches or rule-based recognition to identify DDoS attacks destructive to the substructure of CPPS. For training and authentication of the method, the research uses actual network traffic extracted from actual industrial circumstances, described as the Farm-to-Fork (F2F) supply chain method. Either, attacks or usual traffic is taken, and bidirectional features are extracted over CIC-FLOWMETER. Alohali et al. [12] present a novel swarm-based feature selection (FS) method to develop attack recognition in an IoT-based CPS atmosphere. An Enhanced Chicken Swarm Optimizer (ECSO) method with self-learning capability-based FS can be executed to choose the related feature from the pre-processed data. Then, the ensemble classifications were implemented with the chosen features on the cloud platform. In [13], a blockchain (BC)-based technique for data security in which blocks were created utilizing the RSA hashing technique has been proposed. Utilizing Differential Evolution (DE), the technique initially chosen for the BC-secured data, and the data can be separated into test and train datasets to utilize for testing and training the method. In addition, it is allowable for the authenticated method to utilize a deep belief network (DBN) to predict attacks.

Korium et al. [14] present an IDS based on the ML method. In this research, an approach can be proposed for intrusion detection by a sensitive assessment and choice of the utmost effectual methods for the succeeding stages of the machine ML method: 1) data pre-processing by utilizing Z-score normalization, which maintains the data distributions for the presented technique and controls outliers; 2) FS by utilizing a regression method, which facilitates the difficulty of the model and decreases the implementation time; and 3) method training and selection– Extreme Gradient Boosting, Random Forest(RF), Light Gradient Boosting Machine, Categorical Boosting – with hyperparameter optimizer for handling the behavior in the training stage and to avoid overfittings. Hassler et al. [15] present a new IDS combining UAV physical and cyber features to enhance recognition abilities. Initially, the research advanced a testbed, which contains a controller, UAV, and data-gathering tools to perform cyber-attacks and collect physical and cyber data in attack and normal circumstances. Later, ML-based IDSs combining physical and cyber features are trained to identify cyber-attacks utilizing recurrent neural networks (RNNs), support vector machine (SVM), feedforward neural network (FNN) with CNNs, and LSTM cells.

Saheed et al. [16] presented a novel lightweight transfer learning (TL) technique by executing residual network-50 with CNN one dimension (ResNet50CNN1D) methods for intrusion detection in CPS. In addition, the Adaptive Gradient (Adagrad) optimization has been used in the presented method to reduce the function of loss by the modification of system weight. Ramachandran et al. [17] introduce an Aquila Optimization with Parameter Tuned Machine Learning Anomaly Detection (AOPTML-AD) method in the CPS atmosphere. At first, the pre-processing stage is applied by adapting them into a consistent format. In addition, the enhanced AO algorithm-based FS (AOA-FS) method can be intended to select an optimum feature subset. Apart from this, the Chimp optimizer algorithm (ChOA) with an adaptive neuro-fuzzy inference system (ANFIS) method has been employed for identifying anomalies. In addition, used for optimum fine-tuning of the membership function (MF) delighted in the ANFIS technique. Divya et al. [18] propose an ML-based Smart Intrusion and Fault Identification (SIFI) technique. The SIFI technique uses an ensemble classifier (EC) to integrate the decisions from 3 separate classifications (forest by penalizing attributes (FPA), C4.5 decision tree, and RF). The presented technique utilizes a voting mechanism to localize and identify the unusual proceedings for enhanced precision. The research examines the impacts of cyber threats and physical anomalies initiated by line faults in micro grids.

3. Proposed Methodology

In this article, we offer a new MHDLM-RIDCPS algorithm in Smart City Environment. The proposed MHDLM-RIDCPS technique primarily targets the classification and recognition of intrusions using digital twin technology to enhance security within the CPS. To accomplish that, the MHDLM-RIDCPS algorithm has data normalization, COA using feature subset selection, a hybrid DL model for the classification process, and mPDO using parameter optimizer. Fig. 2 exemplifies the complete workflow process of MHDLM-RIDCPS algorithm.

A. Data Normalization: Min-Max Normalization

Primarily, the proposed MHDLM-RIDCPS system utilizes min-max normalization for transforming an input data into a standardized format. Min-max data normalization can be a critical pre-processing method in intrusion detection for CPS [19]. It transmutes feature values to a particular range, generally [0,1], assuring that all points of data subsidize similarly to the method execution. By measuring features, it inhibits main features with greater

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

values from slanting the recognition method, increasing the precision of ML methods. In CPS, whereas varied sensors create data with variable measures, min-max normalization helps in reliable data demonstration. This enhances the effectiveness and precision of anomaly detection in intricate CPS atmospheres.

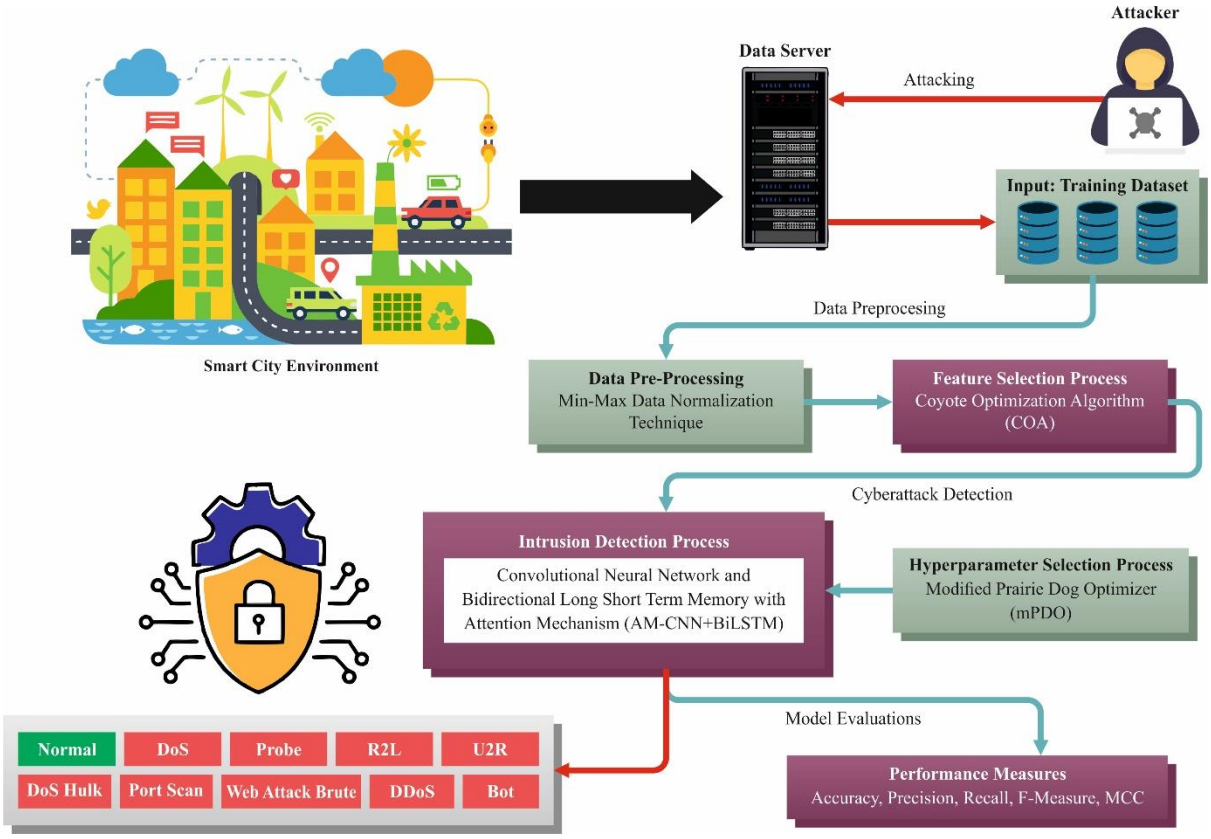

Figure 2. Overall flow of MHDLM-RIDCPS algorithm

B. Feature Subset Selection: COA Model

To alleviate dimensionality issues, the COA can be executed for selecting a sub-set of feature. The COA is a metaheuristic optimizer model inspired by the hunting behavior of coyotes [20]. It imitates a combined hunting tactic, whereas individuals cooperate in groups to hunt for prey. As with each other metaheuristic model, the COA attempts to increase the population of solutions across pre-defined iteration counts. The COA provides various benefits in comparison with other metaheuristic optimizer models. Initially, it incorporates pack behavior, stimulating information-sharing and collaboration between individuals, which helps in the detailed exploration of the searching space. It attacks a balance between exploitation and exploration, avoiding early convergence and guaranteeing stronger performance through different types of problems. Furthermore, the COA is adaptable and flexible to various tasks of optimization, with the capability to manage composite, higher-dimensional difficulties efficiently. Even though its efficacy, COA keeps a simpler performance, making it available and easier to comprehend for experts, who can quickly modify it to ensemble particular requirements.

The population has been designated by $N_p \varepsilon \mathbb{N}$ and contains groups that have $N_c \varepsilon \mathbb{N}$ solutions from them. The social condition (soc) for the c^{th} individual of the p^{th} group at t^{th} time is noted as:

$$soc_{c,j}^{p,t} = \vec{x} = (x_1, x_2, \ldots, x_D) \quad (1)$$

The behavior of reproduction, or else discoverable as the ratio of survival, population size, however, the population has been initialized based on Eq. (2):

$$soc_{c,j}^{p,t} = lb_j + r_j * (ub_j - lb_j) \quad (2)$$

Whereas the lb_j and ub_j represent the lower and upper limit, D denotes the searching space dimension, and r_j signifies a randomly generated number from the range of zero and one. Eq. (3) calculates the adaptation to the presentsoc.

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

$$fit_c^{p,t} = f\left(sol_{c,j}^{p,t}\right) \quad (3)$$

The probability of solutions eviction from the group is given by Eq. (4).

$$P_e = 0.005 * N_c^2 \quad (4)$$

The p^{th} group's alpha (optimal solution) within the t^{th} sample of time can be described for each, but the social trend can be designated by Eq. (6).

$$alpha^{p,t} = soc_{c,j}^{p,t} \left| arg_{c=\{1,2,\ldots,N_C\}} minf\left(soc_c^{p,t}\right)\right\} \quad (5)$$

Here, the $O^{p,t}$ displays the hierarchical social situations for every solution. Original solutions are natural with a mixture of the soc of each parent based on

$$cult_j^{p,t} = \begin{cases} O^{p,t}_{\frac{(N_C+1)}{2}}, & N_c isodd \\ \frac{o^{p,t}_{\frac{N_c}{2}},j + \left(\frac{N_C t}{2}+1\right),j}{2}, & otherwise \end{cases} \quad (6)$$

Now, the randomly generated solution of the p^{th} the group has been provided as r_1 and r_2, the dual randomly formed dimensions are j_1 and j_2, and the scatter chance is assumed as P_s, explained in Eq. (8), however, the relationship likelihood is P_a, designated in Eq. (7), a randomly generated numbers within the boundaries of the j^{th} dimension is R_j, but a randomly generated within the interval (0 and 1) is specified as rnd_j.

$$pup_j^{p,t} = 1 \begin{cases} soc_{r_1,j}^{p,t} & rnd_j < P_s \; or \; j = j_1 \\ soc_{r_2,j}^{p,t} & rnd_j < P_s + P_a \; or \; j = j_2 \\ \mathrm{R}_j, & otherwise \end{cases} \quad (7)$$

$$P_s = \frac{1}{D} \quad (8)$$

$$P_a = \frac{1-P_s}{2} \quad (9)$$

The alpha influence has been designated by δ_1 in Eq. (10), and the effect of a group by δ_2 in Eq. (11). Using this dual parameter, the effect of both parameters can be proven in

$$\delta_1 = alpha^{p,t} - soc_{cr_1}^{p,t} \quad (10)$$

$$\delta_2 = cult^{p,t} - soc_{cr_2}^{p,t} \quad (11)$$

$$new_s oc_c^{p,t} = soc_c^{p,t} + r_1 * \delta_1 + e_2 * \delta_2, \quad (12)$$

Here, the weights of the pack influence and alpha are correspondingly r_1 and r_2. The original social state can result in Eq. (13), whereas Eq. (14) refers to the adaptation mechanism.

$$new_f it_c^{p,t} = f\left(new_{soc_c^{p,t}}\right) \quad (13)$$

$$soc_c^{p,t+1} = \begin{cases} new_{soc_c^{p,t}}, new_f it_c^{p,t} < fit_c^{p,t} \\ soc_c^{p,t}, \quad otherwise \end{cases} \quad (14)$$

In the COA system, the objects were united into a particular objective formulation that a present weight recognizes each objective significance. Here, we implement a fitness function (FF) that integrates both FS objectives as displayed in (15).

$$Fitness(X) = \alpha \cdot E(X) + \beta * \left(1 - \frac{|R|}{|N|}\right) \quad (15)$$

whereas Fitness(X) denotes the subset fitness value, X, $E(X)$ signifies the classifier rate of error by employing the selected features in the X sub-set, $|R|$ and $|N|$ denotes an amount of chosen feature and the number of original features in the dataset respectively, α and β epitomizes classification error weights and the decrease ratio, $\alpha \in [0,1]$ and $\beta = (1-\alpha)$.

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

C. Hybrid Deep Learning: AM-CNN+BiLSTM Classifier

For the classification process, the hybrid of DL models using the AM-CNN+BiLSTM algorithm can be employed. The CNN is an extensively identified DL architecture by the natural visual perception mechanism noted in human life [21]. The CNN method is generally applied for extracting and processing features from organized grid-like data. Unlike conventional neural networks, CNN, with particular layers, is aimed to take spatial hierarchies and decrease the calculation load. CNN structure normally includes three major portions: pooling, convolutional, and fully connected (FC) layers. Rather than using two-dimensional convolutional layers like image data, this work accepts one-dimensional CNN (1D-CNN) to remove local spatial features of time series data. Nearly the process of the 1D-CNN method, the data is initially started and controlled within the input layer. Formerly, the convolutional layer utilizes filters, otherwise named kernels, to pass over the input data to identify spatial hierarchies of features. The feature mapping output of the convolution layer at the position i is designed by:

Whereas $ReLU(\cdot)$ represents the Rectifer Linear Unit activation function, M denotes filter size, X stands for input series, and W_{co} and b_{co} represent bias and weight matrices, correspondingly. Then, the pooling layer decreases the time-based dimension, reducing the parameter counts. Max pooling has been applied in this work, which chooses the maximal value from a local input area owing to robustness improvement and feature retention. The mathematical equation is stated in the following:

$$P_i = \max\{H_{i.s}, H_{i.s+1}, \dots, H_{i.s+s-1}\} \quad (16)$$

Here P_i signifies pooled value, and s denotes pooling size. Once the pooling and convolutional layer, the attained features fatten up into a solitary prolonged vector and pass through a dense layer or FC layer before attaining the output layer. Moreover, the dropout has been utilized for the prevention of overfitting.

$$F = [P_1, P_2, \dots, P_N] \quad (17)$$

$$Y = ReLU\left(W_f \times F + b_f\right) \quad (18)$$

Now, F represents a fattened vector, Y denotes FC layer output and W_f, and b_f stands for bias and weight matrices of the FC layer, correspondingly.

LSTM was initially presented, it is a development in the domain of neural networks, mainly compared to its precursor, RNN. Unlike conventional RNNs, LSTM components comprise methods like input, output, and forget gates, letting them take time-based dependencies well and process time-series data. The process of the LSTM cell is mathematically designated in the following:

Forget gate f_t: utilizes an activation function of the sigmoid to select which portions of the present cell state will be maintained and which must be forgotten.

$$f_t = \sigma\left(W_{fx} \times x_t + W_{fh} \times h_{t-1} + b_f\right) \quad (19)$$

Here, W_f and b_f refer to the bias and weight matrices of the forgetting gate, x_t signifies present input data, and h_{t-1} characterizes the earlier hidden layer (HL).

Input gate i_t: works by applying an activation function of the sigmoid to choose which values of the input must be upgraded. At the same time, a tanh activation function offers a novel candidate cell state. $\tilde{C}_t$ that might be included in the original cell state C_t.

$$i_t = \sigma(W_{ix} \times x_t + W_{ih} \times h_{t-1} + b_i) \quad (20)$$

$$\tilde{C}_t = \tanh(W_{cx} \times x_t + W_{ch} \times h_{t-1} + b_c) \quad (21)$$

$$C_t = f_t \times C_{t-1} + i_t \times \tilde{C}_t \quad (22)$$

Whereas W_i, b_i, W_c, and b_c symbolize the bias and weight matrices of the memory cell and input gate, correspondingly, and C_{t-1} denotes the earlier cell state.

Output state o_t: controls the information outputs from the memory cell. The o_t equation and the novel HL h_t show up as:

$$o_t = \sigma(W_{ox} \times x_t + W_{oh} \times h_{t-1} + b_o) \quad (23)$$

$$h_t = o_t * \tanh(C_t) \quad (24)$$

Now, W_o and b_o signify the bias and weight matrices of the outputted gate, and $*$ refers to the product of Hadamard. However, LSTM is effective for tasks with unidimensional dependences; Bi-LSTM provides a complete model to

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

take bi-directional dependences. Hence, Bi-LSTM includes dual LSTM layers with opposed directions and the h'_t Bi-LSTM network output is the outcome of a process of combination stated in the following:

$$h_f = LSTM(x_t, h_{f-1}) \quad (25)$$

$$h_b = LSTM(x_t, h_{b-1}) \quad (26)$$

$$h'_t = W_{hf} \times h_f + W_{hb} \times h_b + b_h \quad (27)$$

Here, h_f and h_b represent the forward and backward LSTM layer's output, correspondingly; W_{hf} and W_{hb} signifies weight matrices equivalent to every layer, but b_h means the biased matrix. The Attention Mechanism (AM) describes stimulus from the manner physiological systems in humans focus on different modules once control wide information. In DL, AM is a core notion that permits methods to concentrate on specific portions of input series selectively. After being applied to time-series data, AM permits methods to dynamically balance the significance of different time-based points, increasing the capability of the models to illustrate longer-term interconnection. Hence, important information is concentrated on rather than irrelevant particulars. In this work, AM uses the HL output vector of the Bi-LSTM network h'_t stated above as inputs, followed by the AM should be mathematically designated as demonstrated:

The e_{ij} correlation score between the i^{th} and j^{th} output (h'_i and h'_j) of the Bi-LSTM network has been designed below:

$$e_{ij} = f\left(W_i \times h'_i + W_j \times h'_j + b_{ij}\right) \quad (28)$$

Here, W_i and W_j represent weight matrices equivalent to h'_i and h'_j, correspondingly, and b_{ij} describes the biased matrix.

After this, the attention score α_{ij} must be calculated depending on the Softmax function and correlation score e_{ij} by the subsequent Eq. (29):

$$\alpha_{ij} = \frac{\exp(e_{ij})}{\sum_{k=1}^{T} \exp(e_{ij})}, \sum a_{ij} = 1 \quad (29)$$

Thus, the AM layer output or the contribution of every input is measured in the following. Fig. 3 illustrates the structure of AM-CNN+BiLSTM.

$$H_k = \sum_j \alpha_{ij} \times h'_j \quad (30)$$

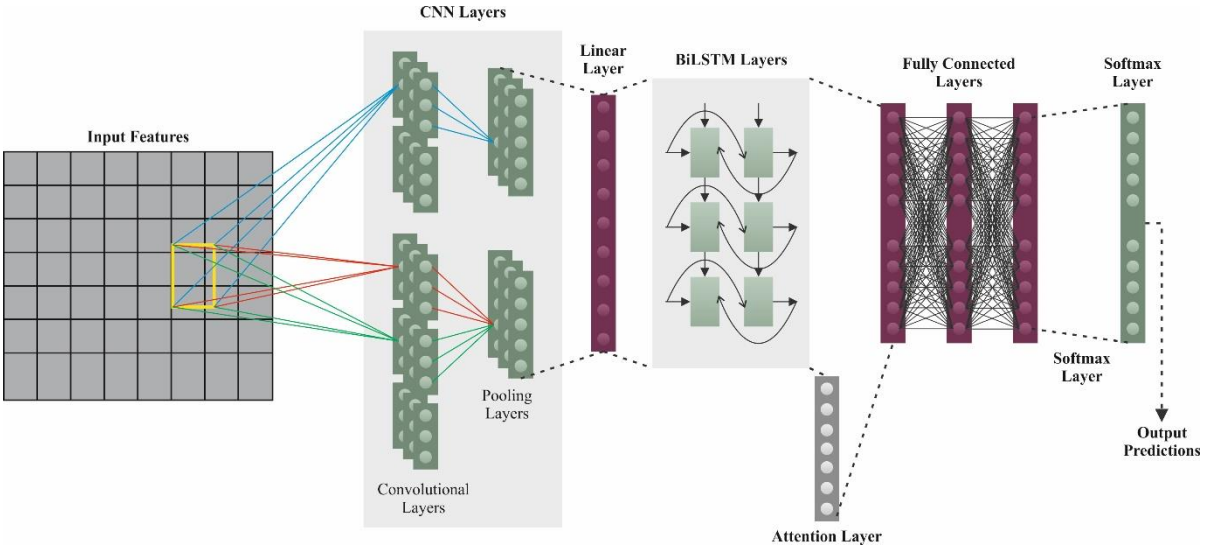

Figure 3. Architecture of AM-CNN+BiLSTM

D. Parameter Optimizer: mPDO Algorithm

Finally, the design of the mPDO system primarily concentrates on the parameter optimizer of the AM-CNN+BiLSTM algorithm and so improves the classifier performances. PDO is a metaheuristic model that is stimulated by the prairie dogs' behavior [22]. This kind of dog takes numerous actions throughout the day like

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

avoiding predators, eating, generating and preserving holes, and food hunting. They display attention when hunting to evade predators and utilize sound and signs to convey with another entity. These gestures send data regarding the existence of hunters, food accessibility, and much more. Particularly prairie dogs can identify dissimilar hunters and their searching forms.

The exploration and exploitation processes are repetitive for groups present. The PDO algorithm begins with an arbitrary population and is parallel to every other meta-heuristics technique. Let the number of dogs be denoted by n_p, the position of i^{th} in each coterie has a total amount of m. The formulation is expressed below.

$$CT = \begin{pmatrix} CT_{1,1} & CT_{1,2} & \dots & CT_{1,d-1} & CT_{1,d} \\ CT_{2,1} & CT_{2,2} & \dots & CT_{2,d-1} & CT_{2,d} \\ . & . & \dots & . & . \\ CT_{m,1} & CT_{m,2} & \dots & CT_{m,d-1} & CT_{m,d} \end{pmatrix}, \quad (31)$$

Whereas, CT_{ij} denotes dimension number j of ith individual. The following calculation provides the position of dogs in a similar coterie.

$$PD = \begin{pmatrix} PD_{1,1} & PD_{1,2} & \dots & PD_{1,d-1} & PD_{1,d} \\ PD_{2,1} & PD_{2,2} & \dots & PD_{2,d-1} & PD_{2,d} \\ . & . & \dots & . & . \\ PD_{n_p,1} & PD_{n_p,2} & \dots & PD_{n_p,d-1} & PD_{n_p,d} \end{pmatrix}. \quad (32)$$

The below-mentioned dual equations are the positions for each coterie and dog utilizing uniform distribution.

$$CT_{ij} = U(0,1) \times \left(UB_j - LB_j\right) + LB_j, \quad (33)$$

$$PD_{ij} = U(0,1) \times \left(UB_j - LB_j\right) + LB_j, \quad (34)$$

Here, UB_j and LB_j denote upper and lower bounds correspondingly. U refers to an evenly distributed value with the range of $[0,1]$. Eq. (35) is employed for computing the fitness function for every individual and protecting them in a range.

$$f(PD) = \begin{bmatrix} f_1\left(\left[PD_{1,1}PD_{1,2} \dots PD_{1,d-1}PD_{1,d-1}\right]\right) \\ f_2\left(\left[PD_{2,1}PD_{2,2} \dots PD_{2,d-1}PD_{2,d-1}\right]\right) \\ f.\left([\dots\dots]\right) \\ f_{n_p}\left(\left[PD_{n_p,1}PD_{n_p,2} \dots PD_{n_p,d-1}PD_{1,d-1}\right]\right) \end{bmatrix}. \quad (35)$$

1. Exploration phase

This phase plays an essential part in each optimizer technique, and the PDO includes exploration of the actions of whole building and food seeking. When prairie dogs meet a shortage of food in their present position, they automatically travel to novel positions, completely discovering the whole search space of food sources or enhanced solutions. The whole's creation is similarly vital for their existence, delivering defense against predators and subsidizing a good atmosphere.

Prairie dogs naturally exist in groups, which are separated into different regions. The exploration procedure arises together, and they move to novel positions only when there is a danger from predators. The total amount of iterations was divided into 4 clusters, where the first dual classes utilize exploration and the remaining two classes use exploitation. When $iter$ is less than $\frac{\text{Max}_{iter}}{4}$ or when $\frac{ax_{iter}}{4}$ is lesser than $\frac{\text{Max}_{iter}}{4}$ but lesser than $\frac{\text{Max}_{iter}}{2}$. The modification in location for hunting food and building novel holes can be defined by the below-mentioned formulations:

$$PD_{i+1j+1} = GBest_{ij} - eCBest_{ij} \times \rho - CPD_{ij} \times Levy\left(n_p\right) \forall iter < \frac{\text{Max}_{iter}}{4} \quad (36)$$

$$PD_{i+1j+1} = GBest_{ij} \times rPD \times DS \times Levy\left(n_p\right) \forall \frac{\text{Max}_{iter}}{4} \leq iter < \frac{\text{Max}_{iter}}{2} \quad (37)$$

Here, $GBest_{ij}$ denotes the finest individual, $eCBest_{ij}$ refers to an attained finest individual effects as exposed in Eq. (38), CPD_{ij} represents the result of randomized cumulative as stated in Eq. (48), DS indicates the power of coterie's tunneling, rPD means the position of randomly generated individual, the food resource attentive (ρ) has a fixed rate of 0.1 kHz, $Levy$ refers to $leavy$ distribution.

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

$$eCBest1j+1 = GBest_{ij} \times \triangle + \frac{PD_{ij} \times mean\left(PD_{n_p,m}\right)}{GBest_{ij} \times \left(UB_j - LB_j\right) + \triangle}, \quad (38)$$

$$CPD_{ij} = \frac{GBest_{ij} - rPD_{ij}}{GBest_{ij} + \triangle}, \quad (39)$$

$$DS = 1.5 \times r \times \left(1 - \frac{iter}{\mathrm{Max}_{iter}}\right)^{\left(2\frac{iter}{\mathrm{Max}_{iter}}\right)} \quad (40)$$

Here, r denotes randomly produced properties for assuring exploration and $\triangle$ states to a lesser value.

2. Exploitation phase

This segment mainly concentrates on the exploitation behaviours in PDO. Prairie dogs utilize dissimilar noises to connect in numerous states like gesturing the accessibility of food. These interaction and communication skills were vital for gathering the nutritious dogs' desires and enhancing their protective abilities against hunters. These behaviours were pretended in the mathematical formulation of Eqs. (41) and (42).

$$PD_{i+1j+1} = GBest_{ij} - eCBest_{ij} \times \tau - CPD_{ij} \times rand \; \forall \frac{\mathrm{Max}_{iter}}{2} \leq iter < 3\frac{\mathrm{Max}_{iter}}{4} \quad (41)$$

$$PD_{i+1j+1} = GBest_{ij} \times PE \times rand \; \forall 3\frac{\mathrm{Max}_{iter}}{4} \leq iter < \mathrm{Max}_{iter} \quad (42)$$

Here, PE denotes an impact of the hunter and τ refers to a smaller number of food quality supply.

$$PE = 1.5 \times \left(1 - \frac{iter}{\mathrm{Max}_{iter}}\right)^{\left(2\frac{iter}{\mathrm{Max}_{iter}}\right)} \quad (43)$$

The original PDO has restrictions such as extreme exploitation and exploration, liability to local sub-optimal areas, and early convergence. To beat these disadvantages, a novel form of the prairie optimizer is developed. The projected optimizer includes a new phase of exploration stimulated by the food method of slime mold algorithm (SMA). The explorative ability of mPDO is enhanced by the smell index parameter from SMA. The mathematical formulation of smell index weight is given below:

$$\overrightarrow{W\left(SmellIndex(\iota)\right)} = \begin{cases} 1 + r.\log\left(\frac{GBest - SO(i)}{GBest - wf} + 1\right) & condition \\ 1 - r.\log\left(\frac{GBest - SO(i)}{GBest - wf} + 1\right) & others \end{cases} \quad (44)$$

While $GBest$ denotes the best solution; wf refers to the worst solution; SO indicates smell order of organized fitness function. A non-linear operator named A is introduced and computed below:

$$A = arctanh\left(-\left(\frac{iter}{\mathrm{max}_{iter}}\right) + 1\right). \quad (45)$$

The new exploration upgrading formulation is expressed as :

$$PD_i = \begin{cases} GBest_{i,j} + vb.(W * PD_A - PD_B)r < rand \\ PD_A + F. \propto . |PD_A - PD_i| \; otherwis \end{cases} e \quad (46)$$

The fitness selection is a significant factor controlling the performances of mPDO model. The hyperparameter range technique contains the solution-encoded technique to evaluate the efficacy of the candidate solutions. The mPDO method studies accuracy as the main measure to model the FF that is expressed as.

$$Fitness \; = \; \max\left(P\right) \quad (47)$$

$$P = \frac{TP}{TP + FP} \quad (48)$$

From the formulation, TP and FP represent the true and false positive values.

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

4. Performance Validation

The performance evaluation of MHDLM-RIDCPS algorithm can be examined under two databases. Initially, the NSLKDD database [23] had 148517 samples with five class labels. Then, the CICIDIS 2017 database [24] contains 13000 samples with six class labels. Table 1 denotes the NSLKDD database. Table 2 indicates the CICIDIS 2017 database.

Table 1: Details of NSLKDD dataset

NSLKDD Dataset	
Class	No. of Samples
Normal	77054
DoS	53385
Probe	14410
R2L	3416
U2R	252
Total Samples	148517

Table 2: Details of CICIDIS 2017 dataset

CICIDIS 2017 Dataset	
Class	No. of Samples
Normal	2500
DDoS	2500
Bot	1500
Port Scan	2500
DoS Hulk	2500
Web Attack-Brute	1500
Total Samples	13000

Table 3 and Fig. 4 represent the best cost of the MHDLM-RIDCPS system under two datasets. Based on NSLKDD2015 dataset, the MHDLM-RIDCPS technique has best cost of 0.042613 whereas the GJO-FS, GTO-FS, HBA-FS, and PIO-FS approaches have obtained the best cost of 0.05822, 0.07007, 0.11117, and 0.13188, respectively. Based on the CICIDIS 2017 dataset, the MHDLM-RIDCPS technique has best cost of 0.04318 whereas the GJO-FS, GTO-FS, HBA-FS, and PIO-FS models have obtained the best cost of 0.05645, 0.09829, 0.12854, and 0.13874, respectively.

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

Table 3: Best cost of the MHDLM-RIDCPS method under two datasets

Methods	Best cost	No. of selected features
NSLKDD dataset		
MHDLM-RIDCPS	0.042613	15
GJO-FS	0.05822	18
GTO-FS	0.07007	19
HBA-FS	0.11117	24
PIO-FS	0.13188	28
CICIDS-2017 dataset		
MHDLM-RIDCPS	0.04318	36
GJO-FS	0.05645	43
GTO-FS	0.09829	60
HBA-FS	0.12854	63
PIO-FS	0.13874	67

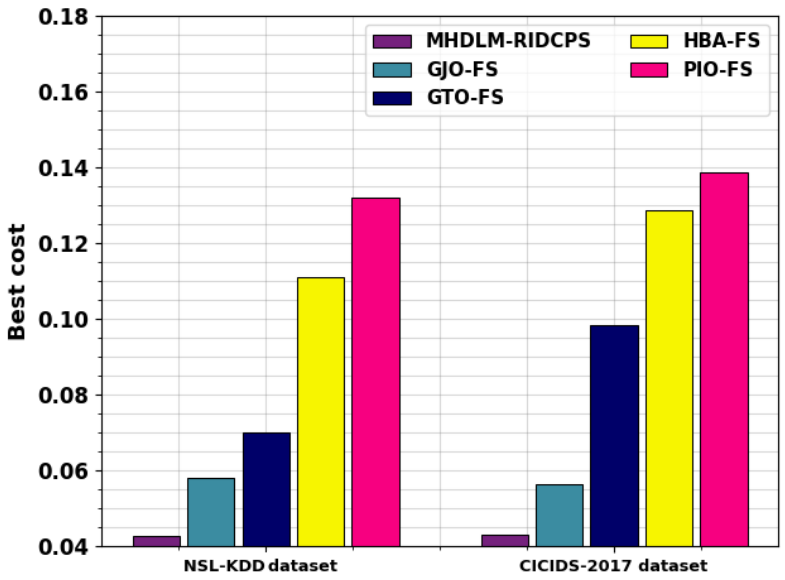

Figure 4. Best cost of the MHDLM-RIDCPS method under two datasets

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

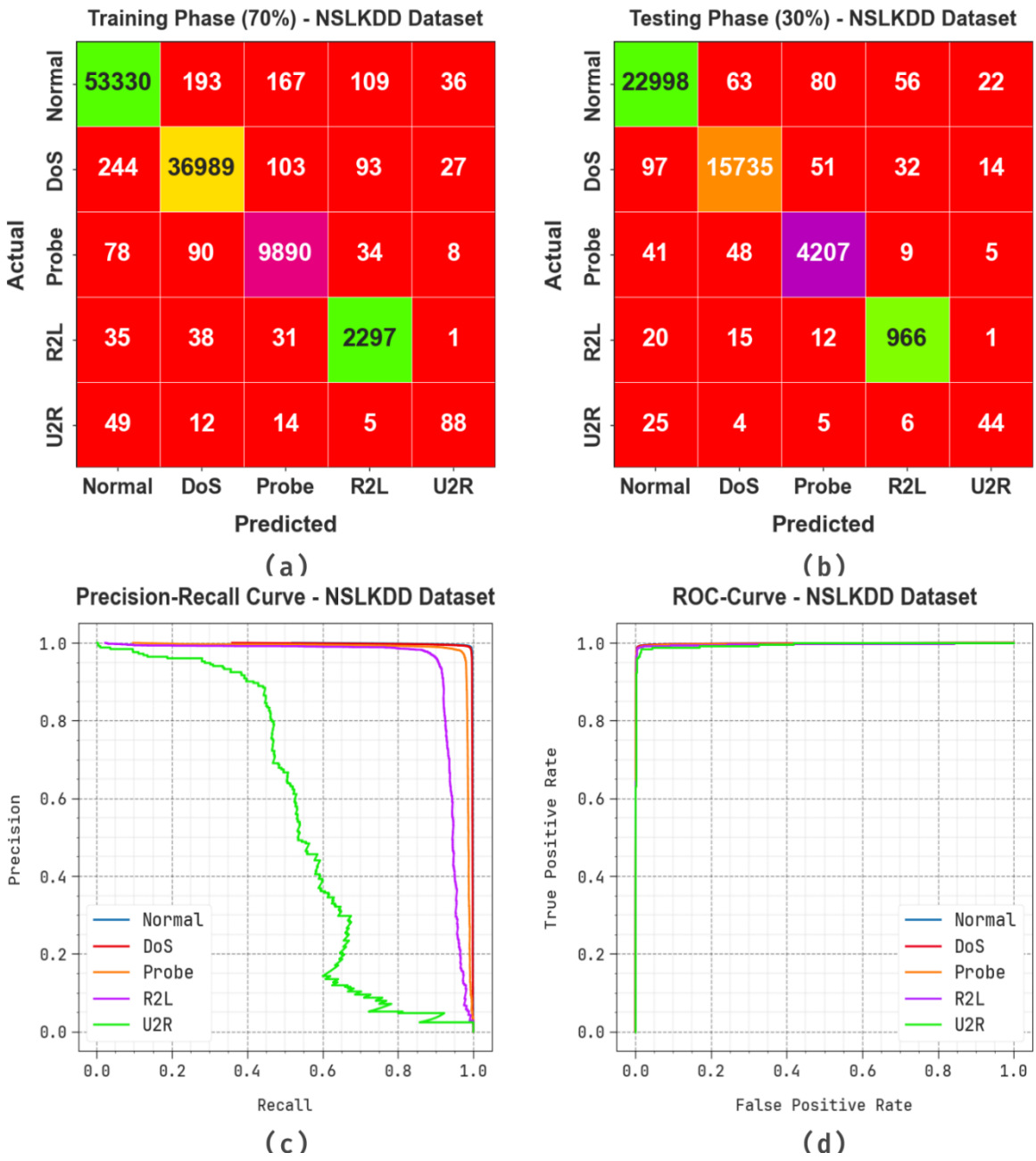

Figure 5. NSLKDD dataset (a-b) Confusion matrices and (c) curve of PR and (d) curve of ROC

Fig. 5 represents the classification outcomes of the MHDLM-RIDCPS model on the NSLKDD dataset. Figs. 5a-5b demonstrates the confusion matrices with accurate recognition and classification of all 5 classes below 70 %TRAPH and 30%TESPH. Fig. 5c displays the analysis of PR, demonstrating the greatest performances across every 5 classes. Ultimately, Fig. 5d shows the analysis of ROC, representing efficient outcomes with better values of ROC for distinct classes.

Table 4 and Fig. 6 offer intrusion detection of MHDLM-RIDCPS system on NSLKDD database. The results denote that the MHDLM-RIDCPS technique properly recognized the samples. With 70%TRAPH, the MHDLM-RIDCPS system delivers average $accu_y$, $prec_n$, $reca_l$, $F_{measure}$, and MCC of 99.47%, 88.15%, 88.75%, 88.43%, and 88.04%, respectively. Furthermore, with 30%TESPH, the MHDLM-RIDCPS system provides average $accu_y$, $prec_n$, $reca_l$, $F_{measure}$, and MCC of 99.46%, 87.30%, 88.62%, 87.95%, and 87.54%, respectively.

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

Table 4: Intrusion detection of MHDLM-RIDCPS technique on the NSLKDD dataset

Class	$Accu_y$	$Prec_n$	$Reca_l$	$F_{measure}$	MCC
70% TRAPH					
Normal	99.12	99.24	99.06	99.15	98.25
DoS	99.23	99.11	98.75	98.93	98.33
Probe	99.50	96.91	97.92	97.41	97.14
R2L	99.67	90.50	95.63	93.00	92.86
U2R	99.85	55.00	52.38	53.66	53.60
Average	99.47	88.15	88.75	88.43	88.04
30% TESPH					
Normal	99.09	99.21	99.05	99.13	98.18
DoS	99.27	99.18	98.78	98.98	98.42
Probe	99.44	96.60	97.61	97.10	96.79
R2L	99.66	90.36	95.27	92.75	92.61
U2R	99.82	51.16	52.38	51.76	51.68
Average	99.46	87.30	88.62	87.95	87.54

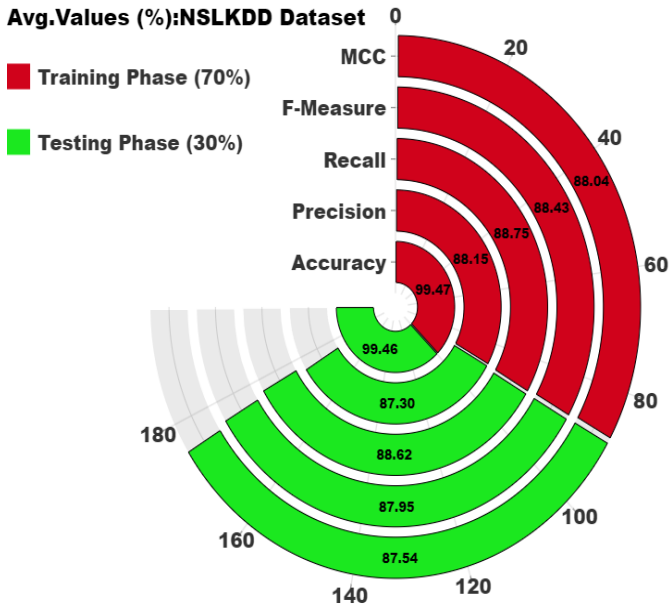

Figure 6. Average of MHDLM-RIDCPS technique on NSLKDD dataset

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

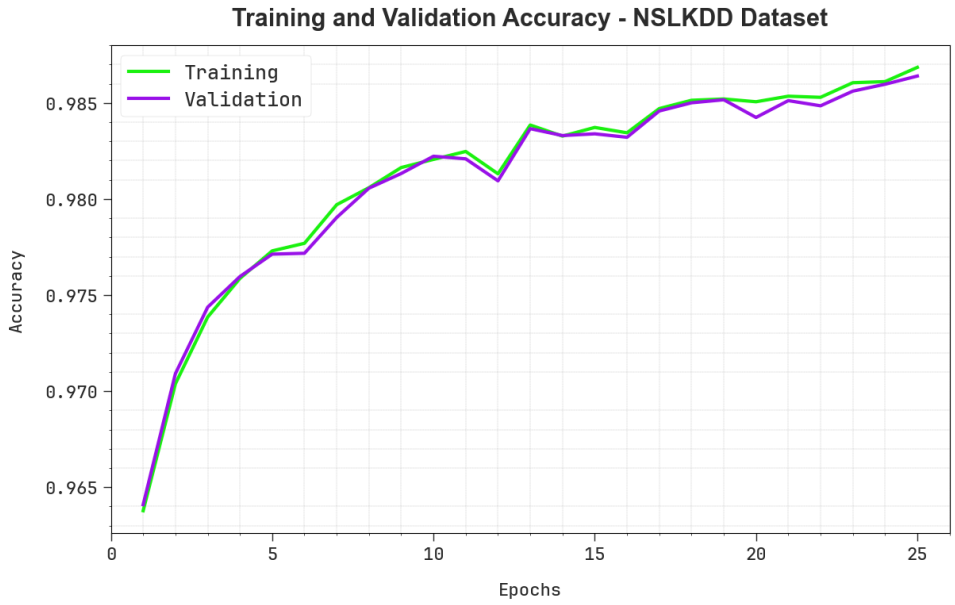

Figure 7. $Accu_y$ The curve of the MHDLM-RIDCPS model on the NSLKDD dataset

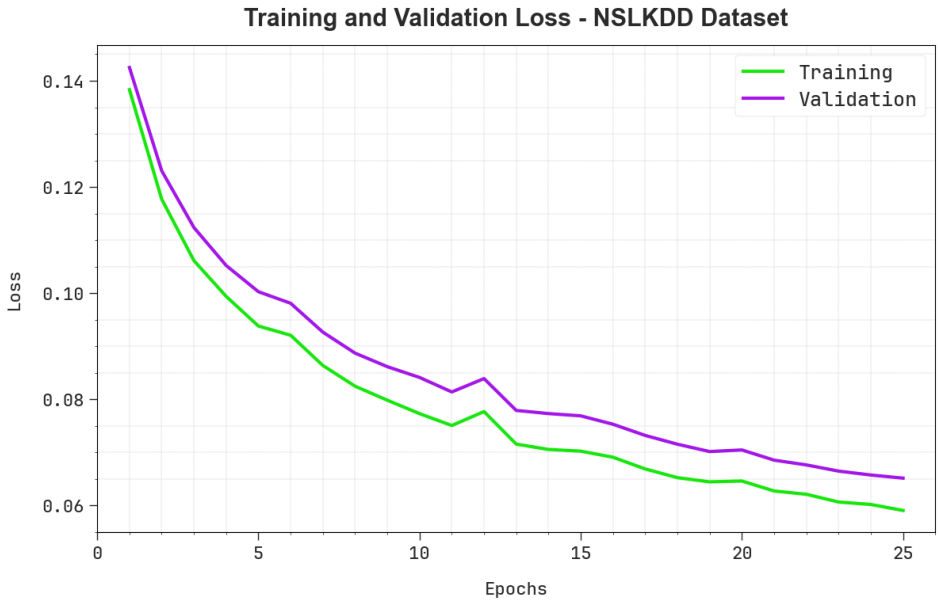

Figure 8. Loss curve of MHDLM-RIDCPS model on NSLKDD dataset

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

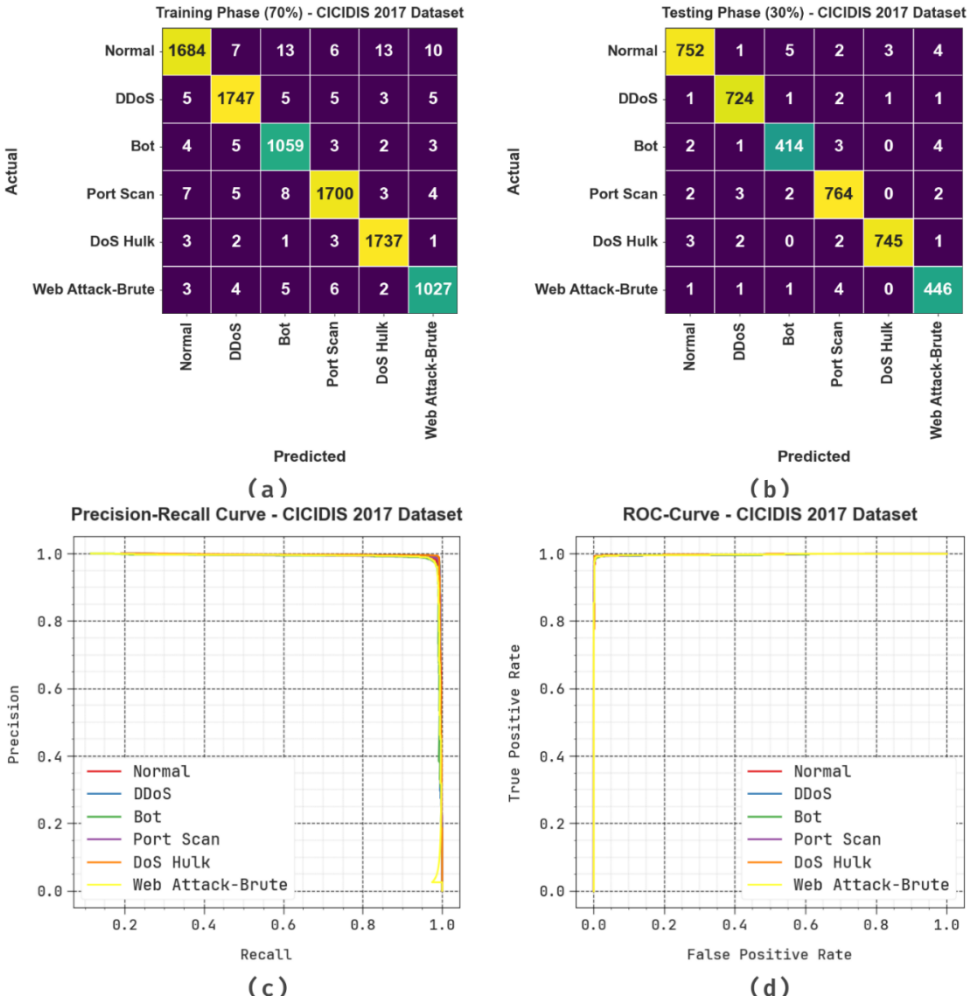

Figure 9. CICIDIS 2017 dataset (a-b) Confusion matrices and (c) curve of PR and (d) curve of ROC

In Fig. 7, the training $accu_y$(TRAAUC) and validation $accu_y$(VLAAUC) outcomes of the MHDLM-RIDCPS system on the NSLKDD database can be exhibited. The $accu_y$values are estimated for 0-25 epochs. The figure highlighted that the TRAAUC and VLAAUC values exhibit a rising trend, which described the ability of MHDLM-RIDCPS algorithm with superior performances over various iterations. Moreover, the TRAAUC and VLAAUC remain adjacent over the epochs, which displays lower least overfitting and shows greater performance of MHDLM-RIDCPS technique, promising constant forecast on unseen samples.

In Fig. 8, the TRA loss (TRALOS) and VLA loss (VLALOS) graph of the MHDLM-RIDCPS technique on the NSLKDD database can be shown. The loss values are estimated for 0-25 epochs. It is indicated that the TRALOS and VLALOS values show a decreasing tendency, notifying the capability of the MHDLM-RIDCPS model to balance a trade-off. The incessant decrease in values of loss besides guarantees the better performances of the MHDLM-RIDCPS algorithm and tunes the forecast outcomes over time.

Fig. 9 signifies the classification outcomes of MHDLM-RIDCPS system on the CICIDIS 2017 dataset. Figs. 9a-9b demonstrates the confusion matrices with precise identification of all 6 class labels under 70%TRAPH and 30%TESPH. Fig. 9c shows the PR analysis, demonstrating the greatest performances across all 6-class labels. Eventually, Fig. 9d shows the ROC analysis, signifying proficient outcomes with better values of ROC for various class labels.

Table 5 and Fig. 10 offer intrusion detection of the MHDLM-RIDCPS method on the CICIDIS 2017 database. The outcomes specify that the MHDLM-RIDCPS technique properly identified the samples. With 70%TRAPH, the MHDLM-RIDCPS system delivers average $accu_y$, $prec_n$, $reca_l$, $F_{measure}$, and MCC of 99.47%, 98.27%, 98.37%, 98.32%, and 98.00%, respectively. Furthermore, with 30%TESPH, the MHDLM-RIDCPS methodology provides average $accu_y$, $prec_n$, $reca_l$, $F_{measure}$ and MCC of 99.53%, 98.46%, 98.52%, 98.49%, and 98.21%, respectively.

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

Table 5: Intrusion detection of MHDLM-RIDCPS technique on the CICIDIS 2017 dataset

Class	$Accu_y$	$Prec_n$	$Reca_l$	$F_{measure}$	MCC
70% TRAPH					
Normal	99.22	98.71	97.17	97.94	97.46
DDoS	99.49	98.70	98.70	98.70	98.39
Bot	99.46	97.07	98.42	97.74	97.44
Port Scan	99.45	98.67	98.44	98.55	98.21
DoS Hulk	99.64	98.69	99.43	99.06	98.84
Web Attack-Brute	99.53	97.81	98.09	97.95	97.68
Average	99.47	98.27	98.37	98.32	98.00
30% TESPH					
Normal	99.38	98.82	98.04	98.43	98.05
DDoS	99.64	98.91	99.18	99.04	98.82
Bot	99.51	97.87	97.64	97.76	97.48
Port Scan	99.44	98.33	98.84	98.58	98.23
DoS Hulk	99.69	99.47	98.94	99.20	99.01
Web Attack-Brute	99.51	97.38	98.45	97.91	97.64
Average	99.53	98.46	98.52	98.49	98.21

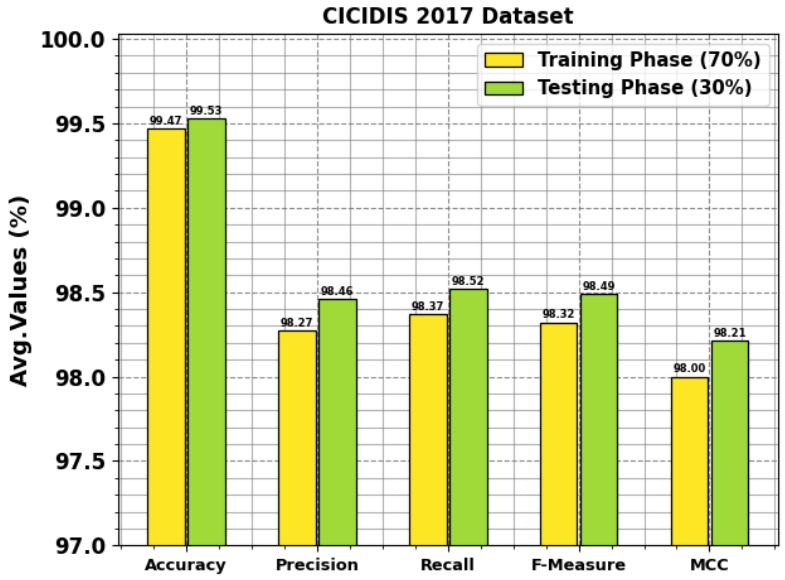

Figure 10. Average of MHDLM-RIDCPS system on CICIDIS 2017 dataset

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

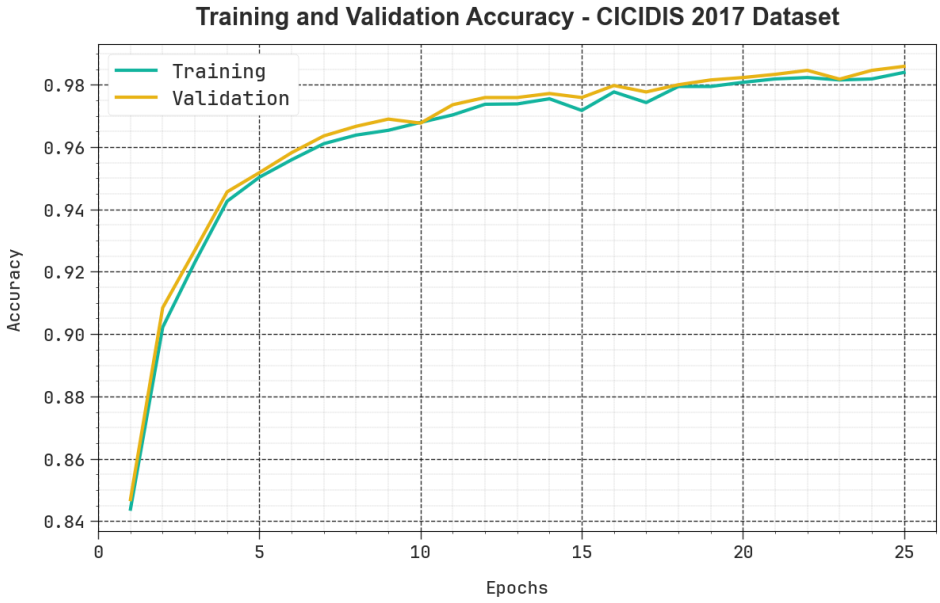

Figure 11. $Accu_y$ Curve of MHDLM-RIDCPS system on CICIDIS 2017 dataset

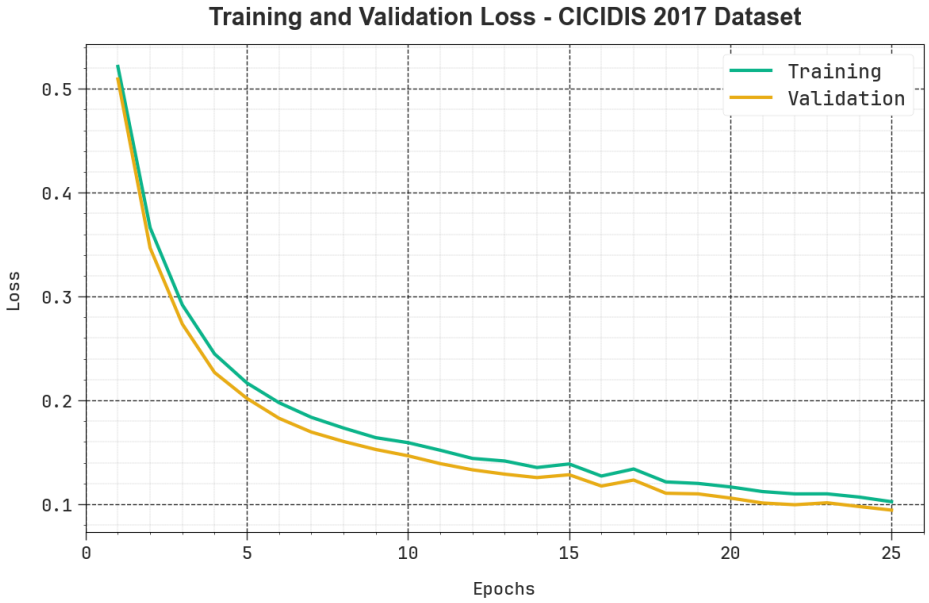

Figure 12. Loss curve of MHDLM-RIDCPS technique on CICIDIS 2017 dataset

In Fig. 11, the TRAAUC and VLAAUC results of the MHDLM-RIDCPS model on CICIDIS 2017 database can be exhibited. The $accu_y$values are estimated for 0-25 epochs. The figure underlined that the TRAAUC and VLAAUC values display an enhancing trend that stated the ability of MHDLM-RIDCPS algorithm with better performances over numerous iterations. Furthermore, the TRAAUC and VLAAUC remain adjacent over the epochs, which specifies lower smallest overfitting and displays greater performances of the MHDLM-RIDCPS methodology, promising continuous forecast on unseen samples.

In Fig. 12, the TRALOS and VLALOS graph of the MHDLM-RIDCPS methodology on the CICIDIS 2017 database is shown. The values of loss are estimated for 0-25 epochs. It is signified that the TRALOS and VLALOS values show a decreasing tendency, reporting the capability of the MHDLM-RIDCPS algorithm to balance a trade-off between generalization and data fitting. The constant decrease in values of loss moreover guarantees the greater performances of MHDLM-RIDCPS technique and alters the forecast results.

Table 6 and Fig. 13 signify the comparison analysis of MHDLM-RIDCPS model with current methods [25]. The results emphasized that the MHDLM-RIDCPS technique has attained superior performances. The DVAE, PT-

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

DSAE, DT, RF, FID-GAN, MAD-GAN, and ALAD systems have designated poorer performance. In the meantime, the XAIIDS-FSDVAE technique has attained closer outcomes. Furthermore, the MHDLM-RIDCPS technique designated greater performance with higher $prec_n$, $reca_l$, $F_{measure}$, and $accu_y$, of 98.46%, 98.52%, 98.49%, and 99.53% respectively.

Table 6: Comparative analysis of MHDLM-RIDCPS system with existing models

Methods	$Prec_n$	$Reca_l$	$F_{measure}$	$Accu_y$
MHDLM-RIDCPS	98.46	98.52	98.49	99.53
XAIIDS-FSDVAE	98.32	98.23	98.27	99.27
DVAE Model	97.75	98.01	97.72	99.02
PT-DSAE Method	97.91	97.65	97.60	98.49
DT Algorithm	96.59	92.84	95.42	93.65
RF Classifier	97.56	93.84	95.92	95.98
FID-GAN Technique	97.72	97.80	97.44	96.07
MAD-GAN Model	96.98	97.11	96.25	96.80
ALAD	97.12	97.84	95.89	94.10

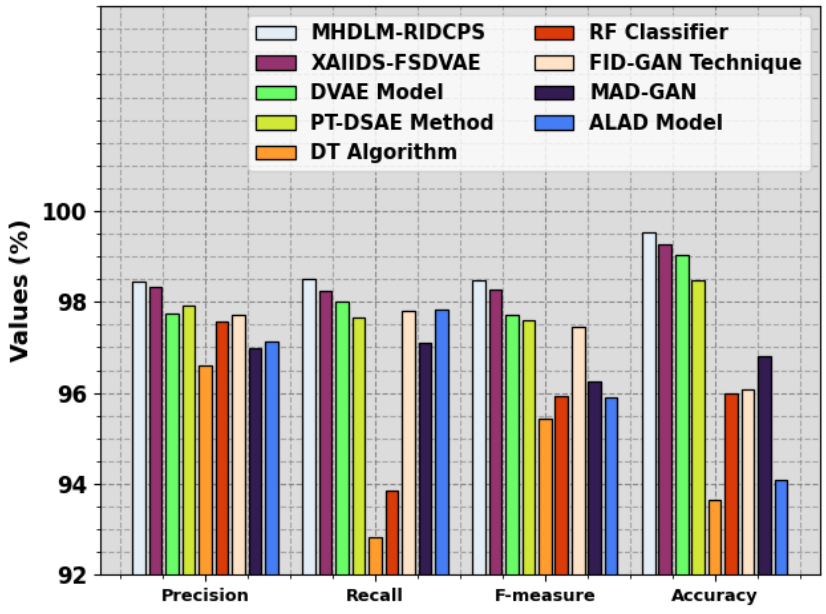

Figure 13. Comparative analysis of MHDLM-RIDCPS system with existing techniques

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

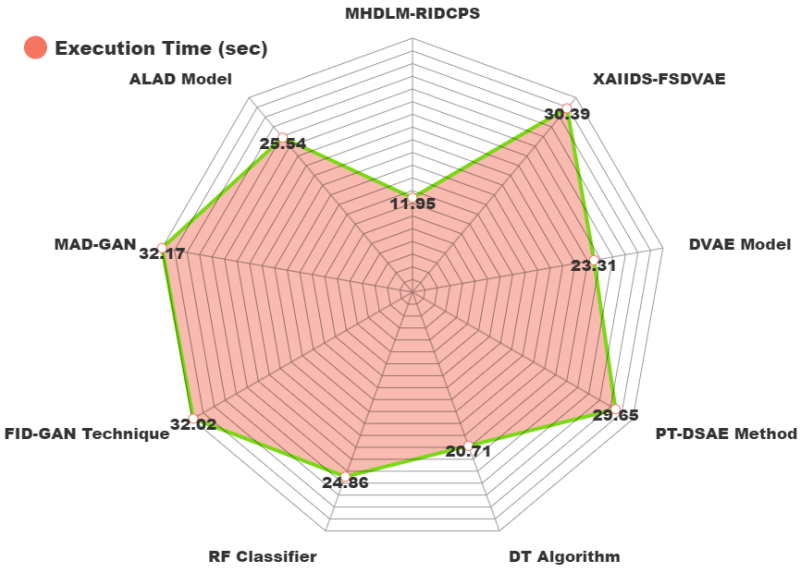

Figure 14. ET outcome of MHDLM-RIDCPS algorithm with existing models

In Table 7 and Fig. 14, the comparison results of the MHDLM-RIDCPS model can be indicated based on execution time (ET). The results indicate that the MHDLM-RIDCPS model got superior performance. For ET, the MHDLM-RIDCPS methodology offers lower ET of 11.93s while the XAIIDS-FSDVAE, DVAE, PT-DSAE, DT, RF, FID-GAN, MAD-GAN and ALAD models get better ET values of 30.39s, 23.31s, 29.65s, 20.71s, 24.86s, 32.02s, 32.17s, and 25.54s, respectively.

Table 7: ET outcome of MHDLM-RIDCPS technique with existing models

Methods	Execution Time (sec)
MHDLM-RIDCPS	11.95
XAIIDS-FSDVAE	30.39
DVAE Model	23.31
PT-DSAE Method	29.65
DT Algorithm	20.71
RF Classifier	24.86
FID-GAN Technique	32.02
MAD-GAN	32.17
ALAD Model	25.54

5. Conclusion

In this study, we offer a new MHDLM-RIDCPS method in Smart City Environment. The proposed MHDLM-RIDCPS technique primarily targets the classification and recognition of intrusions using digital twin technology to enhance security within the CPS. To accomplish that, the MHDLM-RIDCPS algorithm has data normalization, COA using feature subset selection, a hybrid DL model for the classification process, and mPDO using parameter optimizer. Primarily, the proposed MHDLM-RIDCPS approach utilizes min-max normalization for transforming

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

an input data into a standardized format. To alleviate dimensionality issues, the COA can be executed to select a subset of features. In addition, the mPDO combined with the AM-CNN+BiLSTM classifier is exploited for the identification of intrusions. The design of the mPDO system primarily concentrates on the parameter optimizer of the AM-CNN+BiLSTM algorithm and so improves the classifier performances. To determine the greater efficiency of the MHDLM-RIDCPS system, a comprehensive set of simulations can be applied and the performances are tested over distinct aspects. The experimental analysis guaranteed the superior results of the MHDLM-RIDCPS methodology with existing methods.

Funding: "This research received no external funding"

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

References

[1] D. Ding, Q. L. Han, Y. Xiang, X. Ge, and X. M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018.

[2] C. Liang, B. Shanmugam, S. Azam, A. Karim, and A. Islam, "Intrusion detection system for the internet of things based on blockchain and multi-agent systems," *Electronics*, vol. 9, no. 7, p. 1120, 2020.

[3] D. Midi, A. Rullo, A. Mudgerikar, and E. Bertino, "Kalis—A system for knowledge-driven adaptable intrusion detection for the internet of things," in *Proc. IEEE 37th Int. Conf. Distributed Comput. Syst. (ICDCS)*, Atlanta, GA, USA, 2017, pp. 656–666.

[4] A. Hussain, E. M. Tordera, X. Masip-Bruin, and H. C. Leligou, "Rule-based with machine learning IDS for DDoS attack detection in cyber-physical production systems (CPPS)," *IEEE Access*, vol. 12, pp. 12345–12356, 2024.

[5] S. Krishnamurthy, S. Sarkar, and A. Tewari, "Scalable anomaly detection and isolation in cyber-physical systems using Bayesian networks," in *Proc. ASME 2014 Dynamic Syst. Control Conf.*, San Antonio, TX, USA, 2014, pp. V002T26A006.

[6] A. Jones, Z. Kong, and C. Belta, "Anomaly detection in cyber-physical systems: A formal methods approach," in *Proc. IEEE 53rd Annu. Conf. Decision Control (CDC)*, Los Angeles, CA, USA, 2014, pp. 848–853.

[7] C. Zimmer, B. Bhat, F. Mueller, and S. Mohan, "Time-based intrusion detection in cyber-physical systems," in *Proc. 1st ACM/IEEE Int. Conf. Cyber-Physical Syst.*, 2010, pp. 109–118.

[8] R. Mitchell and I. R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surveys (CSUR)*, vol. 46, no. 4, pp. 1–29, 2014.

[9] K. N. Junejo and D. Yau, "Data-driven physical modelling for intrusion detection in cyber-physical systems," in *Proc. Singapore Cyber-Secur. Conf. (SG-CRC)*, 2016, pp. 43–57.

[10] H. Sadreazami, A. Mohammadi, A. Asif, and K. N. Plataniotis, "Distributed-graph-based statistical approach for intrusion detection in cyber-physical systems," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 4, no. 1, pp. 137–147, 2017.

[11] A. Hussain, E. M. Tordera, X. Masip-Bruin, and H. C. Leligou, "Rule-based with machine learning IDS for DDoS attack detection in cyber-physical production systems (CPPS)," *IEEE Access*, vol. 12, pp. 12345–12356, 2024.

[12] M. A. Alohali et al., "Swarm intelligence for IoT attack detection in a fog-enabled cyber-physical system," *Comput. Electr. Eng.*, vol. 108, p. 108676, 2023.

[13] A. Aljabri, F. Jemili, and O. Korbaa, "Intrusion detection in cyber-physical system using RSA blockchain technology," *Multimedia Tools Appl.*, vol. 83, no. 16, pp. 48119–48140, 2024.

[14] M. S. Korium et al., "Intrusion detection system for cyberattacks in the Internet of Vehicles environment," *Ad Hoc Netw.*, vol. 153, p. 103330, 2024.

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025

[15] S. C. Hassler, U. A. Mughal, and M. Ismail, "Cyber-physical intrusion detection system for unmanned aerial vehicles," *IEEE Trans. Intell. Transp. Syst.*, 2023.

[16] Y. K. Saheed et al., "ResNet50-1D-CNN: A new lightweight resNet50-One-dimensional convolution neural network transfer learning-based approach for improved intrusion detection in cyber-physical systems," *Int. J. Crit. Infrastruct. Protect.*, vol. 45, p. 100674, 2024.

[17] A. Ramachandran, K. Gayathri, A. Alkhayyat, and R. Q. Malik, "Aquila optimization with machine learning-based anomaly detection technique in cyber-physical systems," *Comput. Syst. Sci. Eng.*, vol. 46, no. 2, 2023.

[18] R. Divya, S. Umamaheswari, and A. A. Stonier, "Machine learning-based smart intrusion and fault identification (SIFI) in inverter-based cyber-physical microgrids," *Expert Syst. Appl.*, vol. 238, p. 122291, 2024.

[19] L. R. Ramadhan and Y. A. Mudya, "A comparative study of Z-score and Min-Max normalization for rainfall classification in Pekanbaru," *J. Data Sci.*, vol. 2024, no. 04, pp. 1–8, 2024.

[20] Q. Hai, L. Zhang, G. Li, M. Khayatnezhad, and S. Abdolhosseinzadeh, "Water resource management using remote sensing and coyote optimization algorithms," *Irrig. Drain.*, vol. 73, no. 3, pp. 1010–1029, 2024.

[21] Z. Ji, W. Tao, and J. Ren, "Boiler furnace temperature and oxygen content prediction based on hybrid CNN, biLSTM, and SE-Net models," *Appl. Intell.*, vol. 54, no. 17, pp. 8241–8261, 2024.

[22] M. A. Elseify et al., "Boosting prairie dog optimizer for optimal planning of multiple wind turbine and photovoltaic distributed generators in distribution networks considering different dynamic load models," *Sci. Rep.*, vol. 14, no. 1, pp. 1–33, 2024.

[23] [Online]. Available: https://www.kaggle.com/datasets/hassan06/nslkdd

[24] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. Int. Conf. Inf. Syst. Secur. Privacy*, Funchal, Portugal, 2018, pp. 108–116.

[25] B. A. Alqaralleh, F. Aldhaban, E. A. AlQaralleh, and A. H. Al-Omari, "Optimal machine learning enabled intrusion detection in cyber-physical system environment," *Comput. Mater. Continua*, vol. 72, no. 3, pp. 4691–4707, 2022.

DOI: https://doi.org/10.54216/FPA.190116
Received: October 28, 2024 Revised: January 12, 2025 Accepted: February 07, 2025