AIMS Mathematics, 9(5): 11718–11734.
DOI: 10.3934/math.2024574
Received: 23 January 2024
Revised: 08 March 2024
Accepted: 12 March 2024
Published: 26 March 2024

http://www.aimspress.com/journal/Math

Research article

An equilibrium optimizer with deep recurrent neural networks enabled intrusion detection in secure cyber-physical systems

E Laxmi Lydia[1], Chukka Santhaiah[2], Mohammed Altaf Ahmed[3], K. Vijaya Kumar[4], Gyanendra Prasad Joshi[5,*] and Woong Cho[6,*]

[1] Department of Computer Science and Engineering, GMR Institute of Technology, Andhra Pradesh, Rajam 532127, India
[2] Professor Department of CSE, SV College of Engineering, Karakambadi, Tirupati, India
[3] Department of Computer Engineering, College of Computer Engineering & Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[4] Department of Computer Science and Engineering, GITAM School of Technology, GITAM (Deemed to be University), Visakhapatnam, India
[5] Department of Computer Science and Engineering, Sejong University, Seoul 05006, Republic of Korea
[6] Department of Electronics, Information and Communication Engineering, Kangwon National University, Samcheok 25913, Gangwon State, Republic of Korea

* **Correspondence:** Email: joshi@sejong.ac.kr; wcho@kangwon.ac.kr.

Abstract: Cyber-physical systems (CPSs) are characterized by their integration of physical processes with computational and communication components. These systems are utilized in various critical infrastructure sectors, including energy, healthcare, transportation, and manufacturing, making them attractive targets for cyberattacks. Intrusion detection system (IDS) has played a pivotal role in identifying and mitigating cyber threats in CPS environments. Intrusion detection in secure CPSs is a critical component of ensuring the integrity, availability, and safety of these systems. The deep learning (DL) algorithm is extremely applicable for detecting cyberattacks on IDS in CPS systems. As a core element of network security defense, cyberattacks can change and breach the security of network systems, and then an objective of IDS is to identify anomalous behaviors and act properly to defend the network from outside attacks. Deep learning (DL) and Machine learning (ML) algorithms are crucial for the present IDS. We introduced an Equilibrium Optimizer with a Deep Recurrent Neural Networks Enabled Intrusion Detection (EODRNN-ID) technique in the Secure CPS platform. The

main objective of the EODRNN-ID method concentrates mostly on the detection and classification of intrusive actions from the platform of CPS. During the proposed EODRNN-ID method, a min-max normalization algorithm takes place to scale the input dataset. Besides, the EODRNN-ID method involves EO-based feature selection approach to choose the feature and lessen high dimensionality problem. For intrusion detection, the EODRNN-ID technique exploits the DRNN model. Finally, the hyperparameter related to the DRNN model can be tuned by the chimp optimization algorithm (COA). The simulation study of the EODRNN-ID methodology is verified on a benchmark data. Extensive results display the significant performance of the EODRNN-ID algorithm when compared to existing techniques.

Keywords: smart environment; cyber-physical system; security; intrusion detection; deep learning
Mathematics Subject Classification: 11T71, 68P25, 94A60

1. Introduction

Cyber physical system (CPS) is commonly utilized to observe and secure a physical environment using a set of components namely control units, physical objects, actuators, and sensors [1]. As the result of dreadful consequences of a CPS failure, it is more important than anything else to protect a CPS from dangerous attacks. In this paper, we speak about the reliability problem of a CPS aimed at enduring hazardous attacks over a long time without energy replacement [2]. CPS often works in a rough environment where energy renewal is not possible, and nodes may be captured or compromised at periods. As a result, the intrusion detection system (IDS) is needed to detect harmful nodes without unnecessarily wasting energy to extend the network lifetime. IDS designed for CPSs has attracted significant interest [3]. IDS were used to identify security attacks and to monitor computer systems. Usually, IDS were of two major types: Signature-based and Behavior-based. Signature-based IDS deals with the comparison of the real-time performance of the computer system in contradiction of identified security attacks [4]. They cannot detect unknown attacks (signatures) as they depend on known attack models. This is notably important for CPS as they are operating independently for a longer time, and therefore it is difficult to interrupt the common upgrading or patching in the field [5].

Contrastingly, Behavior-based systems identify intrusions by observing a system's active implementation to identify suspect behavior and can identify both known and unknown attacks [6]. IDS, an initial layer is needed to fast assess, identify, and reply to dangerous cyber traffic. Network intrusion detection is vital for identifying and monitoring possible risks. Besides, there are key extreme data in public datasets for intrusion finding. In complex network infrastructure, managing a huge amount of data is another problem that these methods usually fail to solve [7]. For such reasons, classical IDSs based on predictable machine learning (ML) methods commonly have a few limitations, like poor real-time presentation and low regularization capability. In the past years, many researchers have been developed variations of IDS using deep learning (DL), ML, and other arithmetical approaches [8]. Over the years, DL methods have quickly been designed and it is largely used across various industries due to the continuous growth of computational capacity and much information. Both traditional and DL models were examined using familiar classification metrics. In multiple areas, involving image recognition and natural language processing (NLP), DL has created excellent outcomes [9]. Many researcher workers have used convolutional neural networks (CNN) effectively

to find cyberattacks to raise the intelligence and correctness of network intrusion detection. The major cause of the failure is that network traffic is not in an image data format [10].

We introduce an Equilibrium Optimizer with Deep Recurrent Neural Networks Enabled Intrusion Detection (EODRNN-ID) technique in a Secure CPS environment. In the presented EODRNN-ID technique, a min-max normalization algorithm takes place to scale the input dataset. Besides, the EODRNN-ID technique involves an EO-based feature selection approach to choose the feature and diminish high dimensionality problem. For intrusion detection, the EODRNN-ID technique exploits the DRNN model. Finally, the hyperparameter related to the DRNN model can be tuned by the Chimp optimization algorithm (COA). The simulation study of the EODRNN-ID model is verified on a benchmark ID dataset.

2. Related works

Almuqren et al. [11] proposed an Explainable AI Enabled Intrusion Detection Approach for Secured CPSs (XAIID-SCPS). This developed method especially focuses on the classification and intrusion detection in the CPS. In this study, a Hybrid Enhanced GSO (HEGSO) method was employed for the FS. In the IDS, the Improved ENN (IENN) algorithm has been applied with the Enhanced Fruitfly Optimizer (EFFO) method for parameter optimization. Hilal et al. [12] presented an imbalanced GAN (IGAN) with optimum kernel ELM (OKELM), named the IGAN-OKELM method for IDS in the CPS platform. Furthermore, the OKELM framework was implemented as a classification and an optimum parameter tuning of KELM architecture was executed through the applications of the sandpiper optimization (SPO) method and thus, devises the effectiveness of IDS.

The authors [13] implemented FID-GAN, an innovative fog-based, unsupervised ID for CPSs employing GANs. The IDS was introduced for the fog model that makes computation efficiency nearer to the terminal nodes and aids in gathering low-latency necessities. Almutairi et al. [14] employed a Quantum Dwarf Mongoose Optimizer with an Ensemble DL Intrusion Detection (QDMO-EDLID) method in CPS. This algorithm is targeted for identifying the survival of intrusions by employing ensemble learning and FS methods. Furthermore, a Deep Autoencoder (DAE), ensemble of Convolution Residual Network (CRN), and Deep Belief Networks (DBNs) techniques have been implemented for classifying intrusion methods.

The authors [15] presented an Optimum DBN-based distributed IDS (ODBN-IDS) for secured CPS platforms. The Binary Flower Pollination Algorithm (BFPA) was utilized for the FS algorithm. The achieved features have been employed for optimally DBNs for detecting the occurrence of intrusion in cloud information and generating alarms if there is an existence of intrusions. In DBN architecture, the Equilibrium Optimizer Algorithm (EOA) could be employed for finetuning the hyperparameter. Xiao et al. [16] implemented the software-defined network (SDN) model into the CPS framework for easily managing CPS and providing a solution against network security issues. The authors also developed an identification method that depends on ELM to secure CPS.

Duhayyim et al. [17] designed an original Stochastic Fractal Search Algorithm with DL Driven IDS (SFSA-DLIDS) for cloud-based CPS platform. This introduced method mainly implements a min-max data normalization algorithm for converting an input dataset into well-suited formats. For decreasing a process of dimensionality, the SFSA method was implemented for choosing a feature subset. Moreover, a chicken swarm optimizer (CSO) with deep stacked-AE (DSAE) technique is exploited for discovering and organizing intrusion. Dutta et al. [18] developed a robust anomaly

detection mechanism according to semi-supervised ML techniques authorizing the nearby real-time location. A deep neural network (DNN) framework could be employed for identifying anomalies – relying on regeneration errors.

3. The proposed model

In this work, a new EODRNN-ID method has been developed for cyberattack recognition in the CPS platform. The foremost goal of the EODRNN-ID model is to classify as well as identify of intrusive actions in the CPS platform. During the proposed EODRNN-ID method, four sets of operations are involved, namely data normalization, COA-based parameter tuning, DRNN-based classification, and EO-based feature subset selection. Figure 1 portrays the workflow of the EODRNN-ID procedure.

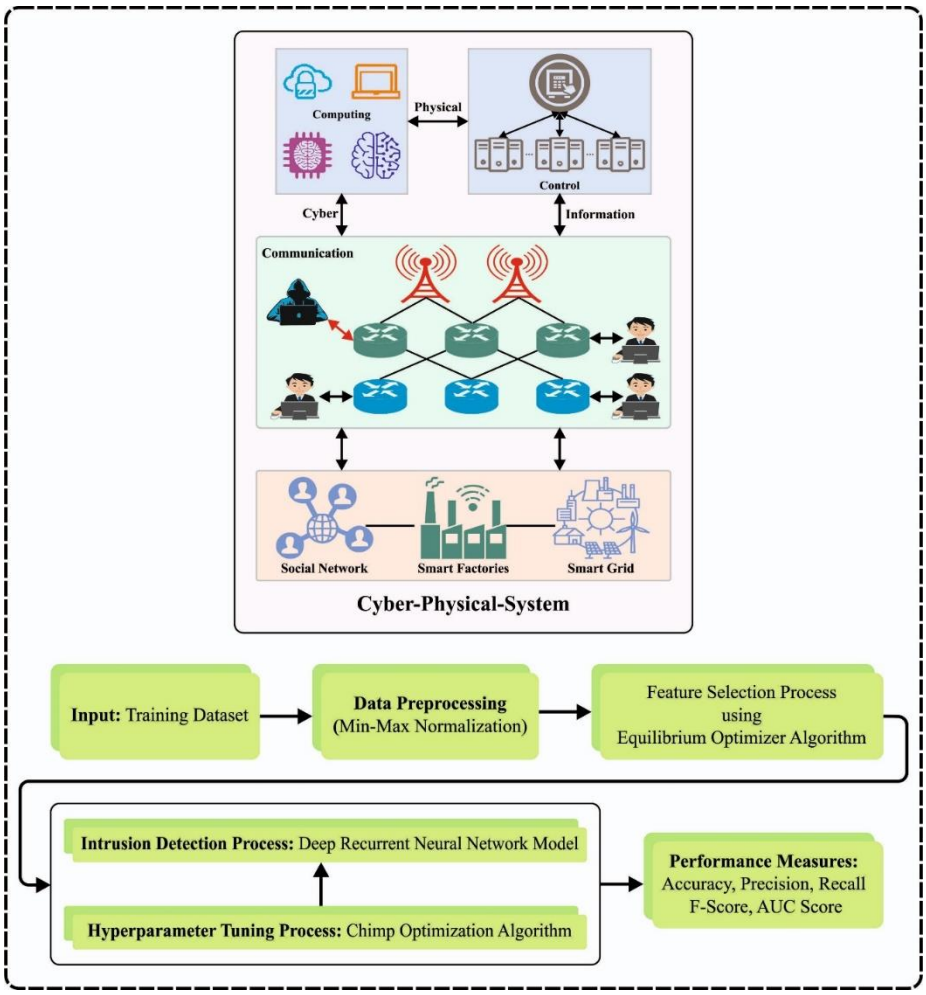

Figure 1. Workflow of EODRNN-ID algorithm.

3.1. Data normalization

Normalization can be done by processing the variably extended data into a reliable range, thereby removing the dimension variation among logging data while preserving relationships amongst the

datasets [19]. This method maps the dataset between 0 and 1:

$$x^* = \frac{x - x_{\min}}{x_{\max} - x_{\min}}, \tag{1}$$

where $x_{\min}$ denotes the minimum value, $x_{\max}$ signifies the maximum value of a certain feature in the dataset, x^* refers to the normalized data, and x denotes an original data.

3.2. Feature selection using EO algorithm

For electing the feature subsets, the EO model is used. The EO method is a new optimizer that draws on approximating equilibrium and dynamic states that establish control volume mass balance [20]. The particle with respective concentration plays the role of the searching agent. After generating a random population, the initial concentration of j^{th} particles can be formulated as:

$$Cn_j^{Initial} = D_{\min^+}(D_{\max} - D_{\min}) \times rand_j \quad j = 0,1, \dots, s. \tag{2}$$

In Eq (2), $rand_j$ is an arbitrarily produced value that lies in [0,1], s refers to the number of particles, and $D_{\max}$ and $D_{\min}$ indicate the maximal and minimal values of the dimension.

The EO creates an equilibrium pool. Initially, the equilibrium candidate is defined (without their knowledge concerning the equilibrium state) to obtain a search pattern for the agent. This can be performed by the four better candidates (viz., large fitness value), along with other particles where the fitness equals the average of four different particles.

$$C_{eq,pool} = \left[C_{eq,1}, C_{eq,2}, C_{eq,3}, C_{eq,4}, C_{eq,mean}\right]. \tag{3}$$

An exponential term (F) is used for the concentration updating:

$$F = e^{-\beta(t - t_0)}, \tag{4}$$

$$\tau = \left(1 - \frac{iTer}{iTer_{max}}\right)^{\left(\frac{\mu \times iTer}{iter_{max}}\right)}. \tag{5}$$

In Eq (5), β indicates the random integer ranges between [0,1], μ shows the constant number to control the exploitation potential. As well, α is a constant number to control the exploration potential, T_0 is evaluated using Eq (6) to ensure the convergence:

$$t_0 = \frac{1}{\beta}\ln\left(-\alpha sign(rand - 0.5)\left[1 - e^{-\beta T}\right]\right) + t. \tag{6}$$

In the equation, sign $(rand - 0.5)$ is used to control the exploitation and exploration direction. Thus, Eq (4), is formulated by:

$$F = \alpha\, sign(rand - 0.5)\left(e^{-\beta t} - 1\right). \tag{7}$$

A parameter used to enhance the exploitation is named generation rate (Gr) and is shown as follows:

$$Gr = Gr_0 e^{-n(t-t_0)}, \tag{8}$$

$$Gr_0 = GrP\left(C_{eq} - \beta C\right), \tag{9}$$

$$P_G = \begin{cases} 0.5\, rand_1 & rand_2 > RP \\ 0 & otherwise \end{cases}. \tag{10}$$

Let GrP and P_G be the generation rate parameter and the likelihood generation, correspondingly.

Eq (11) is used as an updating rule (W is defined as a unit).

$$C = C_{eq} + \left(C - C_{eq}\right).F + \frac{Gr}{\beta W}(1 - F). \tag{11}$$

In the EO, the FF is used to balance the classifier outcome (higher) attained and the amount of features elected in the solution (lower), The fitness function to evaluate solutions is given in Eq (12).

$$Fitness = \alpha\gamma_R(D) + \beta\frac{|R|}{|C|}. \tag{12}$$

Now, α and β are parameters respective to the significance of classification quality and subset length. $\in$ [1,0] and $\beta = 1 - \alpha$. $|R|$ implies the cardinality of the nominated sub-set. $\gamma_R(D)$ implies an error rate of classification. $|C|$ shows the overall feature count in the database.

3.3. *Optimal DRNN based intrusion detection*

The DRNN model is used for the intrusion detection process. RNN is a special type of dense connection NN which is diametrically opposed to the typical FFNN for the introduction of "time" [21]. Especially, the output of the latent layer in the RNN is fed into the input, since the input is a composite of the recent and the present past. RNN exploits the peculiar structure to determine the relationship between events divided by the temporal instant. This means a kind of long-term dependency since a specific event is often a function of a past event. Figure 2 illustrates the framework of RNN.

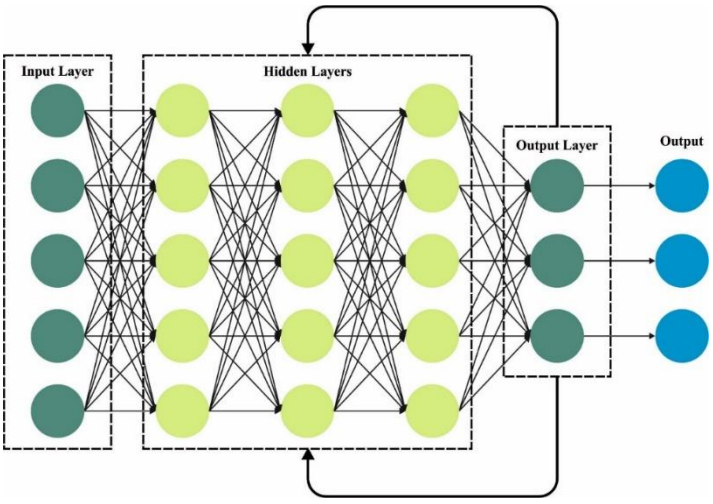

Figure 2. Architecture of RNN.

The RNN has a problem that degrades the performance. During the learning, the gradient tends to vanish similar to other NN models. In this network, the gradient expresses the changes in each weight regarding the change in error. Moreover, the computation gradient passes over several phases of multiplication, and when the quantity multiplied is lesser than one, then the gradient becomes smaller (vanishing), if the quantity multiplied is slightly greater than one, then the gradient becomes larger (exploding). We could not adjust the weight and train the network without accurate knowledge of the gradient. A variant of the RNN is the optimum solution for the gradient vanishing problems that exploit the LSTM unit. LSTM unit helps to retain the error information that can be backpropagated by the time and layers. LSTM unit can able to learn long-term dependency problems on the gradient. LSTM presents a new structure named a memory cell that encompasses of four major components of gate such as a forget, an input, an output and a neuron with a self-recurrent link. The LSTM one has three gating models as new elements in relation to the typical RNN.

The proposed architecture encompassed two recurrent layers with LSTM cells along with the softmax activation function and dense layer for the last classification. The entire network was trained by reducing the categorical cross-entropy as a loss function:

$$\mathcal{L}(y, \hat{y}) = -\sum_{i=1}^{N} y_i \log \hat{y}_i. \tag{13}$$

In Eq (13), y and $\hat{y}$ denote the target and the predicted classes correspondingly.

The Adam algorithm is the chosen optimizer, a gradient-based optimization technique that uses first and second-order moments to attain a fast and smooth convergence.

The COA is used for the optimal parameters tuning of the DRNN. Unlike the other social predators, COA is based on the sexual motivation and intelligence of chimps during group hunting [22]. The four dissimilar stages of hunting in COA are pushing, chasing, blocking, and assaulting. Initially, Chimpanzees are generated randomly to start the COA. The mathematical model of COA's hunting is given below:

$$p_{chimp}^{t+1} = p_{prey}^{t} - \kappa \cdot \left| J \cdot p_{prey}^{t} - \zeta \cdot p_{chimp}^{t} \right|, \tag{14}$$

$$\kappa = 2 \cdot \beta \cdot r_1 - \beta, \tag{15}$$

$$J = 2 \cdot (r_2), \tag{16}$$

$$\zeta = according\ to\ chaotic\ maps, \tag{17}$$

where t indicates the iteration number, $\kappa, J,$ and ζ represent the coefficient vector, p_{prey} shows the optimum solution attained r, and p_{chimp} denotes the optimum location of the chimp. ζ refers to the chaotic mapping vector. Furthermore, β is a nonlinearly dropped constant value that ranges from 2.5 to 0, r_1 and r2 are randomly generated values within [0,1]. Note that the reference gives a comprehensive analysis of these mappings and coefficients.

The most effective and primary strategy for statistically duplicating the chimpanzee behavior is using prey assumed as the initial position of the target. The COA is accountable for housing four of the topmost chimpanzees. Consequently, based on the selected position of best chimpanzees, other individuals would be compelled to relocate as follows:

$$p^{t+1} = \frac{1}{4} \times (p_1 + p_2 + p_3 + p_4), \tag{18}$$

where

$$p_1 = p_A - a_1 \cdot |c_1 p_A - m_1 x|,$$
$$p_2 = p_B - a_2 \cdot |c_2 p_B - m_2 x|,$$
$$p_3 = p_C - a_3 \cdot |c_3 p_c - m_3 P|,$$
$$p_4 = p_D - a_4 \cdot |c_4 p_D - m_4 P|. \quad (19)$$

Moreover, chaotic value mimics social motivation activity in classical COA, as follows:

$$p^{t+1} = \begin{cases} \zeta & \eta_m \geq \frac{1}{2} \\ Eq(5) & \eta_m < \frac{1}{2} \end{cases}. \quad (20)$$

Where, η_m refers to a stochastic value within [0,1]; however, this may result in a moderate or premature convergence.

The COA method derives an FF in order to get high efficacy of classification. It defines an optimistic integer to signify the optimal outcome of the solution candidate. The decay of classification error rate is expected as FF.

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{No.of\ misclassified\ samples}{Total\ no.of\ samples} * 100. \quad (21)$$

4. Results and discussion

The intrusion detection outcomes of EODRNN-ID technique are verified on 2 benchmark databases: NSLKDD2015 and CICIDS2017 datasets as defined in Table 1.

Table 1. Details of two datasets.

Classes	No. of Instances	
	NSLKDD2015	CICIDS2017
Normal	67343	50000
Anomaly	58630	50000
Total No. of Instances	125973	100000

The confusion matrices achieved by the EODRNN-ID approach on the NSLKDD2015 dataset is shown in Figure 3. The results show an effective recognition of the normal as well as anomaly samples under all classes.

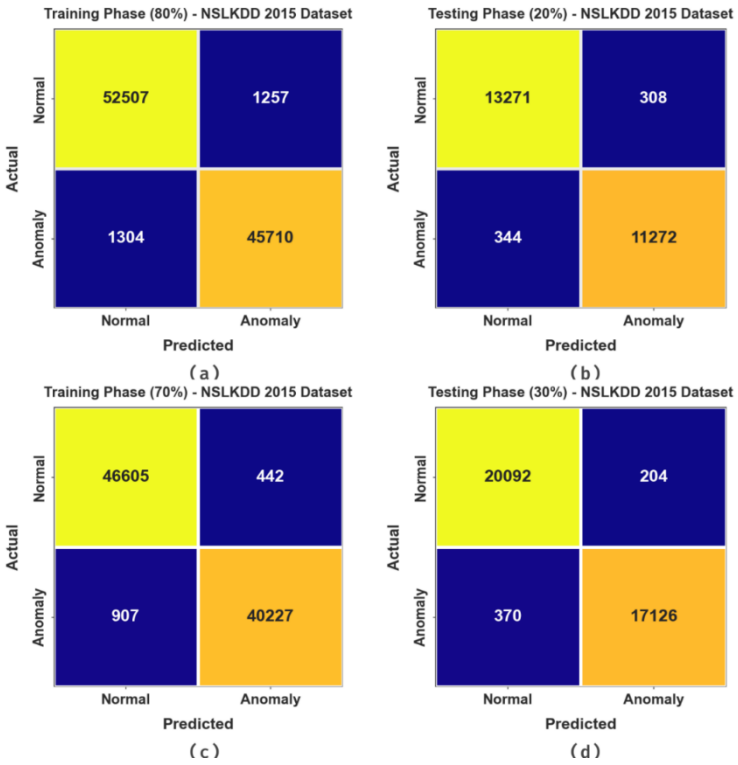

Figure 3. Confusion matrices on NSLKDD2015 dataset (a and b) 80:20 of TRAP/TESP and (c and d) 70:30 of TRAP/TESP.

The recognition outcome of the EODRNN-ID methodology can be inspected on the NSLKDD2015 dataset is given in Table 2 and Figure 4. The outcome implies the effectual recognition of the normal as well as anomaly samples by the EODRNN-ID technique. With 80% of the TRAP, the EODRNN-ID method obtains average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} values of 97.44%, 97.45%, 97.44%, 97.45%, and 97.44%, respectively. Moreover, with 20% of the TESP, the EODRNN-ID method obtains average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} values of 97.39%, 97.41%, 97.39%, 97.40%, and 97.39%, respectively.

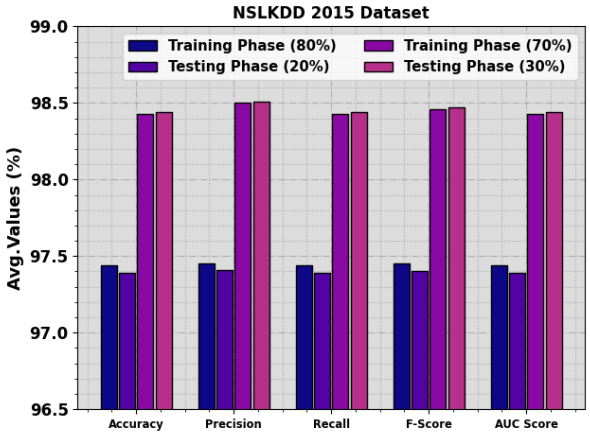

Figure 4. Average of EODRNN-ID algorithm on NSLKDD2015 dataset.

Table 2. Detection outcome of the EODRNN-ID method on the NSLKDD2015 database.

NSLKDD2015 Database					
Classes	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{score}$	AUC_{score}
80% of TRAP					
Normal	97.66	97.58	97.66	97.62	97.44
Anomaly	97.23	97.32	97.23	97.27	97.44
Average	97.44	97.45	97.44	97.45	97.44
20% of TESP					
Normal	97.73	97.47	97.73	97.60	97.39
Anomaly	97.04	97.34	97.04	97.19	97.39
Average	97.39	97.41	97.39	97.40	97.39
70% of TRAP					
Normal	99.06	98.09	99.06	98.57	98.43
Anomaly	97.80	98.91	97.80	98.35	98.43
Average	98.43	98.50	98.43	98.46	98.43
30% of TESP					
Normal	98.99	98.19	98.99	98.59	98.44
Anomaly	97.89	98.82	97.89	98.35	98.44
Average	98.44	98.51	98.44	98.47	98.44

To evaluate the performance of EODRNN-ID method on the NSLKDD2015 dataset, TRA and TES $accu_y$ curves are defined, as presented in Figure 5. The TRA and TES $accu_y$ curves display the performance of EODRNN-ID method over some epochs. The outcome shows significant facts about learning task and generalization capacities of EODRNN-ID model. It is practical that the TRA and TES $accu_y$ curves get improved with an increased epoch count. It is well-known that the EODRNN-ID technique attains superior testing results, which has high ability in detecting the pattern in TRA and TES data.

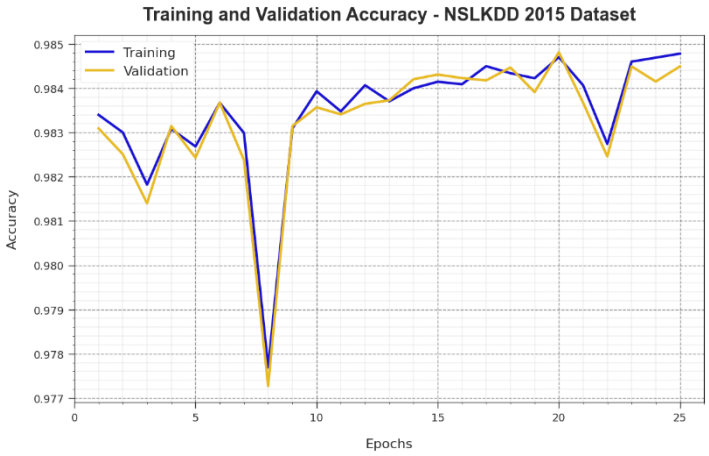

Figure 5. $Accu_y$ curve of EODRNN-ID algorithm on NSLKDD2015 dataset.

Figure 6 demonstrates the complete TRA and TES loss performances of the EODRNN-ID model on the NSLKDD2015 dataset over epochs. The TRA loss shows the model loss acquires reduced over

epochs. Primarily, the loss value gets minimized as the model adapts the load to reduce the prediction error on TRA and TES datasets. The loss curves illustrate the level to which the model fit the TRA dataset. The TRA and TES loss is gradually reduced and showed that the EODRNN-ID technique efficiently learns the pattern revealed in the TRA and TES data. Also, the EODRNN-ID method adjusts the parameters to reduce the divergence among the forecast as well as original TRA labels.

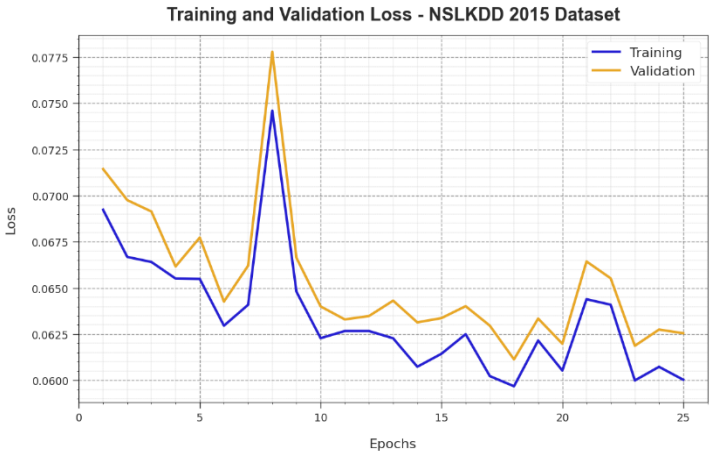

Figure 6. Loss curve of EODRNN-ID algorithm on NSLKDD2015 dataset.

The detection performance of the EODRNN-ID method can be inspected on the CICIDS2017 dataset as delivered in Table 3 and Figure 7. The outcomes indicate the effective detection of the normal and anomaly samples by the EODRNN-ID methodology. With 80% of the TRAP, the EODRNN-ID method accomplished average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} values of 99.20%, 99.20%, 99.20%, 99.20%, and 99.20%, respectively. Besides, with 20% of the TESP, the EODRNN-ID model obtains average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} values of 99.28%, 99.27%, 99.28%, 99.27%, and 99.28%, correspondingly.

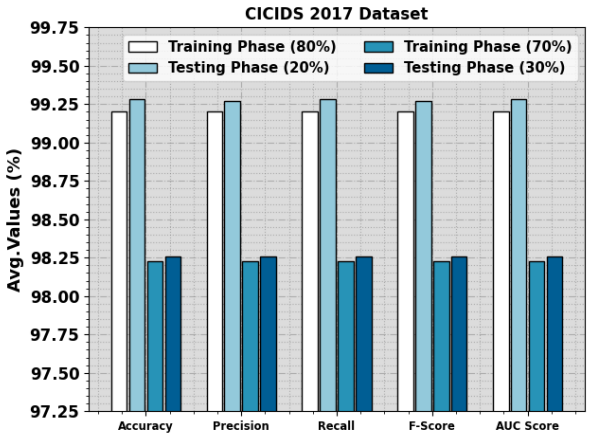

Figure 7. Average of EODRNN-ID algorithm on the CICIDS2017 dataset.

Table 3. Detection outcome of the EODRNN-ID algorithm under CICIDS2017 dataset.

CICIDS 2017 Dataset					
Classes	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{score}$	AUC_{score}
80% of TRAP					
Normal	99.05	99.35	99.05	99.20	99.20
Anomaly	99.36	99.05	99.36	99.20	99.20
Average	99.20	99.20	99.20	99.20	99.20
20% of TESP					
Normal	99.15	99.40	99.15	99.28	99.28
Anomaly	99.40	99.15	99.40	99.27	99.28
Average	99.28	99.27	99.28	99.27	99.28
70% of TRAP					
Normal	98.20	98.25	98.20	98.23	98.23
Anomaly	98.26	98.20	98.26	98.23	98.23
Average	98.23	98.23	98.23	98.23	98.23
30% of TESP					
Normal	98.28	98.24	98.28	98.26	98.26
Anomaly	98.23	98.28	98.23	98.25	98.26
Average	98.26	98.26	98.26	98.26	98.26

To estimate the performance of the EODRNN-ID methodology on the dataset of CICIDS2017, TRA and TS $accu_y$ curves are well-defined, as given in Figure 8. The TRA and TES $accu_y$ curves illustrate the performance of EODRNN-ID model over numerous epochs. The figure delivers significant details concerning the learning task and generalization capabilities of EODRNN-ID technique. It is perceived that the TRA and TES $accu_y$ curves get improved with an increased epoch count. The EODRNN-ID methodology attains improved testing accurateness which has the skill to detect the pattern in TRA and TES datasets.

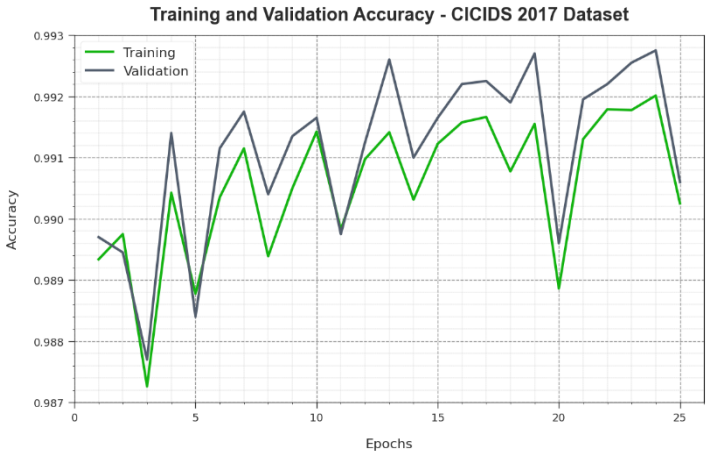

Figure 8. $Accu_y$ curve of EODRNN-ID algorithm on CICIDS2017 dataset.

Figure 9 shows the complete TRA and TES loss performances of the EODRNN-ID model on the CICIDS2017 dataset over epochs. The TRA loss demonstrates the model loss gets reduced over epochs.

Primarily, the loss value gets minimized as the model adapts the weight to diminish the predictive error on the TRA and TES datasets. The loss curves illustrate the range to which the model fits the TRA dataset. It is perceived that the TRA and TES loss is steadily reduced and depicted that the EODRNN-ID technique learns the pattern presented in the TRA and TES datasets. Also, the EODRNN-ID technique adjusts the parameter to minimize the dissimilarity among the prediction and original TRA label.

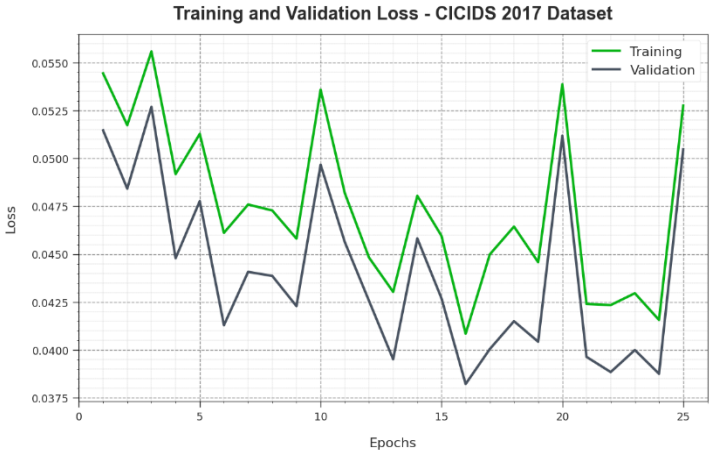

Figure 9. Loss curve of EODRNN-ID algorithm on CICIDS2017 dataset.

The PR curve of the EODRNN-ID method on the CICIDS2017 dataset is established by plotting precision against recall as defined in Figure 10. The outcomes confirm that the EODRNN-ID technique achieves enlarged precision-recall values below all classes. The figure shows that the method learns to identify many classes. The EODRNN-ID method reaches upgraded outcomes in the detection of positive samples through a least false positives.

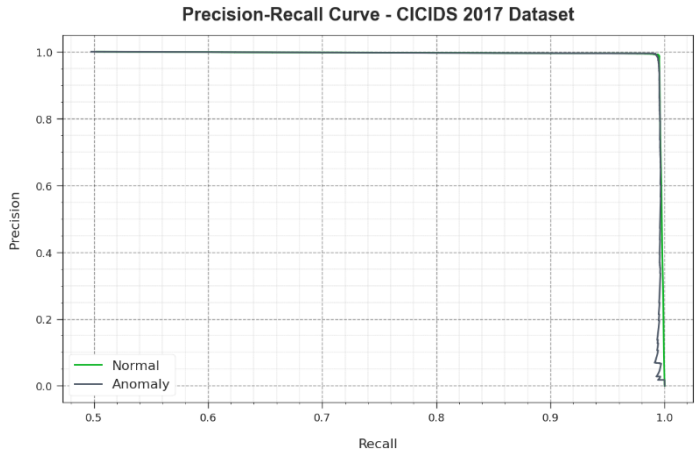

Figure 10. PR curve of EODRNN-ID algorithm on CICIDS2017 dataset.

The ROC curves delivered by the EODRNN-ID methodology on the CICIDS2017 dataset are demonstrated in Figure 11, which has the ability to distinguish the classes. The figure shows valuable insights into the tradeoff amongst the TPR and FPR rates over different detection thresholds and

variable numbers of epochs. It projects an accurate predictive performance of the EODRNN-ID model on the detection of different classes.

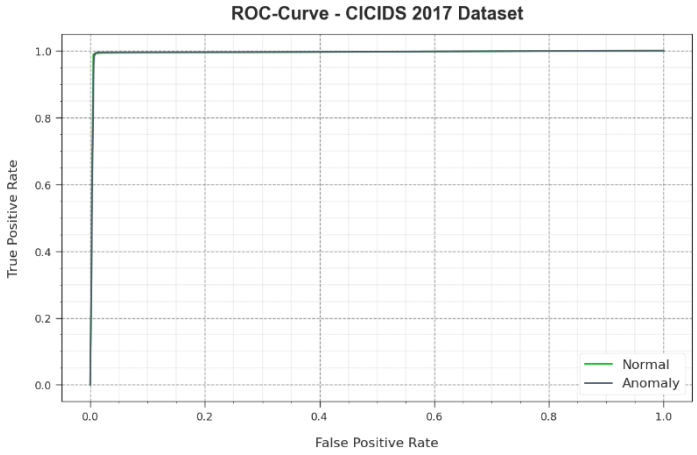

Figure 11. ROC curve of EODRNN-ID method on CICIDS2017 dataset.

The intrusion detection results of the EODRNN-ID system are compared with the present methods in Table 4 and Figure 12 [11]. The outcomes established that the EODRNN-ID technique reaches improved performance over other models. It is stated that the LIB-SVM, WISARD, and Forest-PA models have resulted in worse results whereas the XAIID-SCPS, FURIA, AE-RF, and GSAE models have tried to accomplish manageable performance. However, the EODRNN-ID technique resulted in better performance with maximum $accu_y$, $prec_n$, $reca_l$, and $F1_{score}$ of 99.28%, 99.27%, 99.28%, and 99.27% respectively. Thus, the EODRNN-ID technique can be applied to achieve security from the CPS platform.

Table 4. Comparative outcome of EODRNN-ID algorithm with existing approaches**.**

Methods	$\boldsymbol{Accu_y}$	$\boldsymbol{Prec_n}$	$\boldsymbol{Reca_l}$	$\boldsymbol{F1_{score}}$
EODRNN-ID	99.28	99.27	99.28	99.27
XAIID-SCPS	98.87	98.95	98.87	98.91
FURIA Model	98.14	97.57	96.93	98.26
AE-RF Model	97.62	97.35	97.79	97.30
Forest-PA	96.72	96.97	97.32	98.13
WISARD	96.64	97.58	97.29	98.65
GSAE Model	97.63	95.97	98.39	98.19
LIB-SVM	96.57	96.96	96.83	97.92

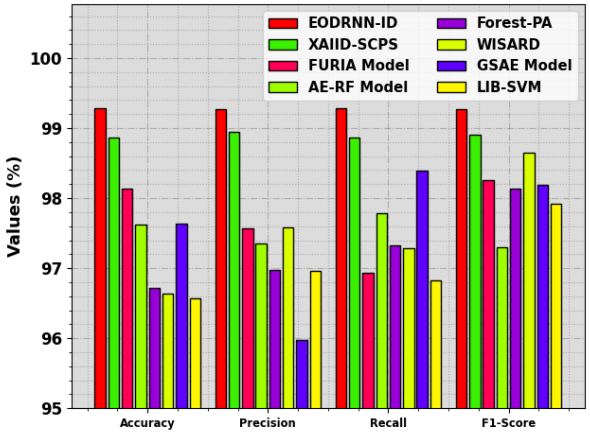

Figure 12. Comparative outcome of EODRNN-ID system with existing techniques.

5. Conclusions

In this manuscript, we have established the EODRNN-ID methodology for cyberattack recognition in the CPS platform. The major intention of the EODRNN-ID algorithm is to classify and detect the intrusive actions from the CPS platforms. In the proposed EODRNN-ID method, four sets of operations are included such as data normalization, COA-based parameter tuning, DRNN-based classification, and EO-based feature subset selection. The simulation study of EODRNN-ID method can be verified on a benchmark data. Extensive outcomes illustrate the significant performance of the EODRNN-ID method over existing techniques

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. V. Jayagopal, M. Elangovan, S. S. Singaram, K. B. Shanmugam, B. Subramaniam, S. Bhukya, Intrusion detection system in industrial cyber-physical system using clustered federated learning, *SN Comput. Sci.*, **4** (2023), 452. https://doi.org/10.1007/s42979-023-01821-1
2. H. Mittal, A. K. Tripathi, A. C. Pandey, M. D. Alshehri, M. Saraswat, R. Pal, A new intrusion detection method for cyber–physical system in emerging industrial IoT, *Comput. Commun.*, 190 (2022), 24–35. https://doi.org/10.1016/j.comcom.2022.04.004
3. I. V. Mboweni, D. T. Ramotsoela, A. M. Abu-Mahfouz, Hydraulic data preprocessing for machine learning-based intrusion detection in cyber-physical systems, *Mathematics*, **11** (2023), 1846. https://doi.org/10.3390/math11081846

4. M. Umer, S. Sadiq, H. Karamti, R. M. Alhebshi, K. Alnowaiser, A. A. Eshmawi, et al., Deep learning-based intrusion detection methods in cyber-physical systems: Challenges and future trends, *Electronics*, **11** (2022), 3326. https://doi.org/10.3390/electronics11203326
5. S. Safavat, D. B. Rawat, Asynchronous federated learning for intrusion detection in vehicular cyber-physical systems, In: *IEEE INFOCOM 2023–IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2023. https://doi.org/10.1109/INFOCOMWKSHPS57453.2023.10225917
6. M. A. Alohali, F. N. Al-Wesabi, A. M. Hilal, S. Goel, D. Gupta, A. Khanna, Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment, *Cogn. Neurodyn*., **16** (2022), 1045–1057. https://doi.org/10.1007/s11571-022-09780-8
7. R. Colelli, F. Magri, S. Panzieri, F. Pascucci, Anomaly-based intrusion detection system for cyber-physical system security. In: *2021 29th Mediterranean Conference on Control and Automation (MED)*, 2021. https://doi.org/10.1109/MED51440.2021.9480182
8. A. A. Nour, A. Mehbodniya, J. L. Webber, A. Bostani, B. Shah, B. Z. Ergashevich, et al., Optimizing intrusion detection in industrial cyber-physical systems through transfer learning approaches, *Comput. Electr. Eng.*, **111** (2023), 108929. https://doi.org/10.1016/j.compeleceng.2023.108929
9. M. Catillo, A. Pecchia, U. Villano, CPS-GUARD: Intrusion detection for cyber-physical systems and IoT devices using outlier-aware deep autoencoders, *Comput. Secur.*, **129** (2023), 103210. https://doi.org/10.1016/j.cose.2023.103210
10. Q. Lin, R. Ming, K. Zhang, H. Luo, Privacy-enhanced intrusion detection and defense for cyber-physical systems: A deep reinforcement learning approach, *Secur. Commun. Netw.*, **2022** (2022), 4996427. https://doi.org/10.1155/2022/4996427
11. L. Almuqren, M. S. Maashi, M. Alamgeer, H. Mohsen, M. A. Hamza, A. A. Abdelmageed, Explainable artificial intelligence enabled intrusion detection technique for secure cyber-physical systems, *Appl. Sci*., **13** (2023), 3081. https://doi.org/10.3390/app13053081
12. A. M. Hilal, S. Al-Otaibi, H. Mahgoub, F. N. Al-Wesabi, G. Aldehim, A. Motwakel, et al., Deep learning enabled class imbalance with sand piper optimization based intrusion detection for secure cyber physical systems, *Cluster Comput.*, **26** (2023), 2085–2098. https://doi.org/10.1007/s10586-022-03628-w
13. P. F. de Araujo-Filho, G. Kaddoum, D. R. Campelo, A. G. Santos, D. Macêdo, C. Zanchettin, Intrusion detection for cyber–physical systems using generative adversarial networks in fog environment, *IEEE Internet Things J.*, **8** (2021), 6247–6256. https://doi.org/10.1109/JIOT.2020.3024800
14. L. Almutairi, R. Daniel, S. Khasimbee, E. L. Lydia, S. Acharya, H. Kim, Quantum dwarf mongoose optimization with ensemble deep learning based intrusion detection in cyber-physical systems, *IEEE Access*, **11** (2023), 66828–66837. https://doi.org/10.1109/ACCESS.2023.3287896
15. P. Ramadevi, K. N. Baluprithviraj, V. A. Pillai, K. Subramaniam, Deep learning based distributed intrusion detection in secure cyber physical systems, *Intell. Autom. Soft Comput.*, **34** (2022), 2067–2081. https://doi.org/10.32604/iasc.2022.026377
16. Y. Xiao, J. Liu, L. Zhang, Cyber-physical system intrusion detection model based on software-defined network, In: *2021 IEEE 12th International Conference on Software Engineering and Service Science (ICSESS)*, 2021. https://doi.org/10.1109/ICSESS52187.2021.9522345

17. M. A. Duhayyim, K. A. Alissa, F. S. Alrayes, S. S. Alotaibi, E. M. Tag El Din, A. A. Abdelmageed, et al., Evolutionary-based deep stacked autoencoder for intrusion detection in a cloud-based cyber-physical system, *Appl. Sci.*, **12** (2022), 6875. https://doi.org/10.3390/app12146875
18. A. K. Dutta, R. Negi, S. K. Shukla, Robust multivariate anomaly-based intrusion detection system for cyber-physical systems, In: *Cyber security cryptography and machine learning*, Springer, Cham, 2021. https://doi.org/10.1007/978-3-030-78086-9_6
19. T. Ma, G. Xiang, Y. Shi, Y. Liu, Horizontal in situ stresses prediction using a CNN-BiLSTM-attention hybrid neural network, *Geomech. Geophys. Geo-Energ. Geo-Resour.*, **8** (2022), 152. https://doi.org/10.1007/s40948-022-00467-2
20. S. I. Seleem, H. M. Hasanien, A. A. El-Fergany, Equilibrium optimizer for parameter extraction of a fuel cell dynamic model, *Renew. Energ.*, **169** (2021), 117–128. https://doi.org/10.1016/j.renene.2020.12.131
21. M. Scarpiniti, D. Comminiello, A. Uncini, Y. C. Lee, Deep recurrent neural networks for audio classification in construction sites. In: *2020 28th European Signal Processing Conference (EUSIPCO)*, 2021. https://doi.org/10.23919/Eusipco47968.2020.9287802
22. W. Tang, S. Yang, M. Khishe, Profit prediction optimization using financial accounting information system by optimized DLSTM, *Heliyon*, **9** (2023), e19431. https://doi.org/10.1016/j.heliyon.2023.e19431

AIMS Press