AIMS Mathematics, 9(6): 15076–15096.
DOI: 10.3934/math.2024731
Received: 25 February 2024
Revised: 30 March 2024
Accepted: 11 April 2024
Published: 26 April 2024

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

Research article

Election-based optimization algorithm with deep learning-enabled false data injection attack detection in cyber-physical systems

Hend Khalid Alkahtani[1], Nuha Alruwais[2], Asma Alshuhail[3], Nadhem NEMRI[4], Achraf Ben Miled[5,*] and Ahmed Mahmud[6]

[1] Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[2] Department of Computer Science and Engineering, College of Applied Studies and Community Services, King Saud University, Saudi Arabia, P.O. Box 22459, Riyadh 11495, Saudi Arabia
[3] Department of Information Systems, College of Computer Sciences & Information Technology, King Faisal University, Saudi Arabia
[4] Department of Information Systems, College of Science & Art at Mahayil, King Khalid University, Saudi Arabia
[5] Department of Computer Science at the College of Science, Northern Border University, Arar, Saudi Arabia
[6] Research Center, Future University in Egypt, New Cairo 11835, Egypt

*** Correspondence:** Email: ashraf.benmilad@nbu.edu.sa.

Abstract: Cyber-physical systems (CPSs) are affected by cyberattacks once they are more connected to cyberspace. Advanced CPSs are highly complex and susceptible to attacks such as false data injection attacks (FDIA) targeted to mislead the systems and make them unstable. Leveraging an integration of anomaly detection methods, real-time monitoring, and machine learning (ML) algorithms, research workers are developing robust frameworks to recognize and alleviate the effect of FDIA. These methods often scrutinize deviations from predictable system behavior, using statistical analysis and anomaly detection systems to determine abnormalities that can indicate malicious activities. This manuscript offers the design of an election-based optimization algorithm with a deep learning-enabled false data injection attack detection (EBODL-FDIAD) method in the CPS infrastructure. The purpose of the EBODL-FDIAD technique is to enhance security in the CPS environment via the detection of FDIAs. In the EBODL-FDIAD technique, the linear scaling normalization (LSN) approach can be used to scale the input data into valuable formats. Besides, the

EBODL-FDIAD system performs ensemble learning classification comprising three classifiers, namely the kernel extreme learning machine (KELM), long short-term memory (LSTM), and attention-based bidirectional recurrent neural network (ABiRNN) model. For optimal hyperparameter selection of the ensemble classifiers, the EBO algorithm can be applied. To validate the enriched performance of the EBODL-FDIAD technique, wide-ranging simulations were involved. The extensive results highlighted that the EBODL-FDIAD algorithm performed well over other systems concerning numerous measures.

Keywords: cyber-physical system; false data injection attack; deep learning; election-based optimization; ensemble learning
Mathematics Subject Classification: 11Y40

1. Introduction

Today, cyber-physical systems (CPSs) are a focal point due to the development of network communication technology, information technology (IT), control theory, and technological developments. Incessantly, the security of CPSs is considered by progressive researchers, and an increasing number of attacks against numerous CPSs are performed [1]. In several instances, the CPSs have been attacked through false data injection attacks (FDIA). In 2015, the "BlackEnergy" virus provoked an electricity failure of the Ukrainian power grids, and later a different version of the virus attacked a railway operation system and mining company. It is noticeable that the attacks of the CPSs have been tremendously dangerous [2]. Consequently, the security of CPSs will be increasingly examined by several researchers.

Nowadays, the three leading categories of attacks against CPSs are denial of service (DoS) attacks, replay attacks, and FDIA [3]. The FDIA interrupts execution or stability by inserting false data without identification. Thus, figuring out how to recognize the FDIA is a major exploration domain. FDIA was devised reliant on the physical information of the system, which makes it complex for traditional identification techniques to detect the attacks [4]. Automatically, while the information of the CPSs is changed on FDIA, the connection between the output and input should be modified and what remains between actual and ideal outputs must be altered. Various attacks are caused by different false and even collapses in every part of CPSs, such as physical parts of the system or cyber modules [5]. In general, two important kinds of cyberattacks are denial of service (DoS) and deception attacks. In each category of deception attacks, the target of the attacker is to cooperate with the transferred data at the sensor to decrease the data packet's integrity [6]. Particularly, a few varieties of deception attacks arise frequently in industrial CPSs. Such popular attacks comprise FDIAs where the produced fault data (noise) from the attacker is inserted into the communication network to reduce the data authenticity of the system [7], replay attacks where the prior time data packets will be stored and transmitted recurrently for preventing the submodels from accomplishing the steady-state stage, and time-delay attacks where a delay parameter is inserted into the systems for affecting instability in the system's functions [8]. Deep learning (DL) methods have presented significant achievements in numerous sectors namely speech identification, natural language processing (NLP), and image identification, providing effective possibilities to enhance cybersecurity in Industry 5.0 [9]. Transformer, CNNs, and RNN methods are among the systems that will automatically learn intricate representations and patterns in the raw data [10].

This ability allows DL methods to identify new and complex attacks that should be avoided by standard machine learning (ML) techniques [11]. Additionally, DL methods are modified to deal with the challenges related to cybersecurity datasets, like non-stationarity, noise, and imbalance [12]. It will be integrated with other artificial intelligence (AI) methods, namely reinforcement learning (RL) and adversarial learning, to make highly strong and adaptable attack detection models [13]. DL algorithms can be used to considerably increase the identification and avoidance of web-based attacks in the CPS platform.

This manuscript offers the design of an election-based optimization algorithm with a deep learning-enabled false data injection attack detection (EBODL-FDIAD) technique in the CPS environment. In the EBODL-FDIAD system, the linear scaling normalization (LSN) approach can be used to scale the input data into a useful format. Besides, the EBODL-FDIAD method performs ensemble learning classification comprising three classifiers, namely the kernel extreme learning machine (KELM), long short-term memory (LSTM), and attention-based bidirectional recurrent neural network (ABiRNN) model. For optimal hyperparameter selection of the ensemble classifiers, the EBO algorithm can be applied. The impact of the presented method, EBODL-FDIAD, lies in its widespread manner of detecting FDIA utilizing DL approaches and advanced optimizer models. By combining an ensemble of classifiers with the EBO approach for hyperparameter tuning, we can improve the model's adaptability and performance, ensuring optimum configuration to generate reliable recognition of and correct cyber threats. The extensive results highlighted that the EBODL-FDIAD technique performed well over other approaches with respect to diverse measures. The major contributions of the study are listed as follows:

- The EBODL-FDIAD methodology provides a widespread solution to FDIA detection by integrating ensemble learning and an EBO-based hyperparameter tuning model in the CPS platform. As we know it, the EBODL-FDIAD approach has never occurred in previous literature.
- Employing an ensemble model by integrating KELM, LSTM, and ABiRNN enables the model to control the unique strengths of all of the methods, enhancing complete recognition performance. The inclusion of ABiRNN presents a new model for examining graph-structured data that is most relevant for identifying difficult connections and dependencies in CPS networks.
- Deploying the EBO approach for hyperparameter tuning improves the effectiveness and efficacy of the model by automatically optimizing main parameters, decreasing the need for manual tuning, and enhancing detection accuracy.

2. Related works

In [14], a modified red fox optimizer with a DL-based FDIA detection (MRFODL-FDIAD) method was developed at the cyber-physical production system (CPPS) infrastructure. This introduced MRFODL-FDIAD system primarily identifies and categorizes FDIAs at the CPPS platform. This includes a three-phase method of identification, parameter tuning, and preprocessing. For FDIA detection, the MRFODL-FDIAD method employs a multihead attention-based LSTM (MBA-LSTM) system. In [15], an intelligent attack detection and recognition system was developed that can categorize the attack varieties on the physical layer dependent upon the ELM algorithm. Additionally, the developed method finds the attack or false to precise features or capacities in the model to support cybersecurity experts in alleviating the effects of the attack on the communication networks.

Liu et al. [16] examined the identification of irregular FDIA under CPSs. Deep-RL (DRL) was

implemented to make an FDIA detection. Initially, the uneven attack detection issue was labeled as a partially observable Markov decision process (POMDP) and an neural network can be employed to analyze the POMDP. At this network, sliding observation windows consisting of the offline fragment of previous data have been employed as the input. In [17], a graph convolutional network (GCN) algorithm was developed to identify the FDIA. This presented method examined the representational features of FDIAs by executing the graphical architecture of the power network to analyze the changing state assessment values dependent upon the network topology and identified the position of the FDIAs.

In [18], a testbed of the process industry was designed that was a hardware-in-the-loop environment for simulating real-time industrial manufacturing and implemented an FDIA at this infrastructure. A host improved the physical method, and the cyber product was an engineer station or real industrial controller. Then, this developed method built an effective FDIA detection system, named the DRIF. In [19], an FDIA detection technique dependent upon protected federated DL was developed by integrating a transformer, federated learning (FL), and Paillier cryptosystem. The transformer is a detector employed for edge nodes, examining deeply the relationship among separate electrical measures by employing the multi-class self-attention mechanism. With the help of the FL model, the technique exploits the data at every node for collaboratively training a detection system.

Fu et al. [20] projected an innovative attack technique called the temporal FDI (TFDI) attack. The virus created outcomes dependent upon temporal interpretations of the CPPS, and a deep Q network (DQN) architecture stimulated the attack. For example, DQN captured vectors of incessant variables as input conditions, and the developed technique is allowed to the state space explosion issue. Additionally, for implementing time-series measures as quasi-dynamic analysis, LSTM cells could be utilized as a layer of the Q network. In [21], an end-wise DL method was established dependent upon a huge volume of real-time sensor data. Primarily, an innovative recursive model with multi-lookback inputs was developed. An innovative learning method called recursive gradient descent (RGD) was made for the designed model for decreasing combined prediction variability. Later, a classification method dependent upon temporal convolutions through numerous channels with decay impact was developed.

Tian et al. [22] investigated adversarial example attacks on multi-label FDIA locational detectors and presented a common multi-label adversarial attack structure like the multi-label adversarial false data injection attack (LESSON). In [23], the authors analyzed the tasks of adversarial attacks against DL-based Unmanned Aerial Vehicles (UAVs) and presented two adversarial attack approaches against regression methods in UAVs. The investigations exhibited that the presented non-targeted and targeted attack models crafted imperceptible adversarial images and presented a significant attack on the navigation and control systems of UAVs. Tian et al. [24] examined the joint adversarial example and FDIAs (AFDIAs) to discover several attack conditions for state evaluation in power systems. If perturbations are directly added to measurements, they are more likely to be identified by BDDs. The presented approach of adding perturbations to state variables ensures that the attack is secret to BDDs. Afterward, malicious data that are stealthy to both BDDs and DL-based detectors are created.

3. The proposed method

In the manuscript, we offer the design of an EBODL-FDIAD technique in the CPS infrastructure. The purpose of the EBODL-FDIAD technique is to enhance security in the CPS environment via the detection of FDIAs. It contains three different processes namely data preprocessing, ensemble learning,

and EBO-based parameter tuning. Figure 1 demonstrates the entire procedure of the EBODL-FDIAD technique.

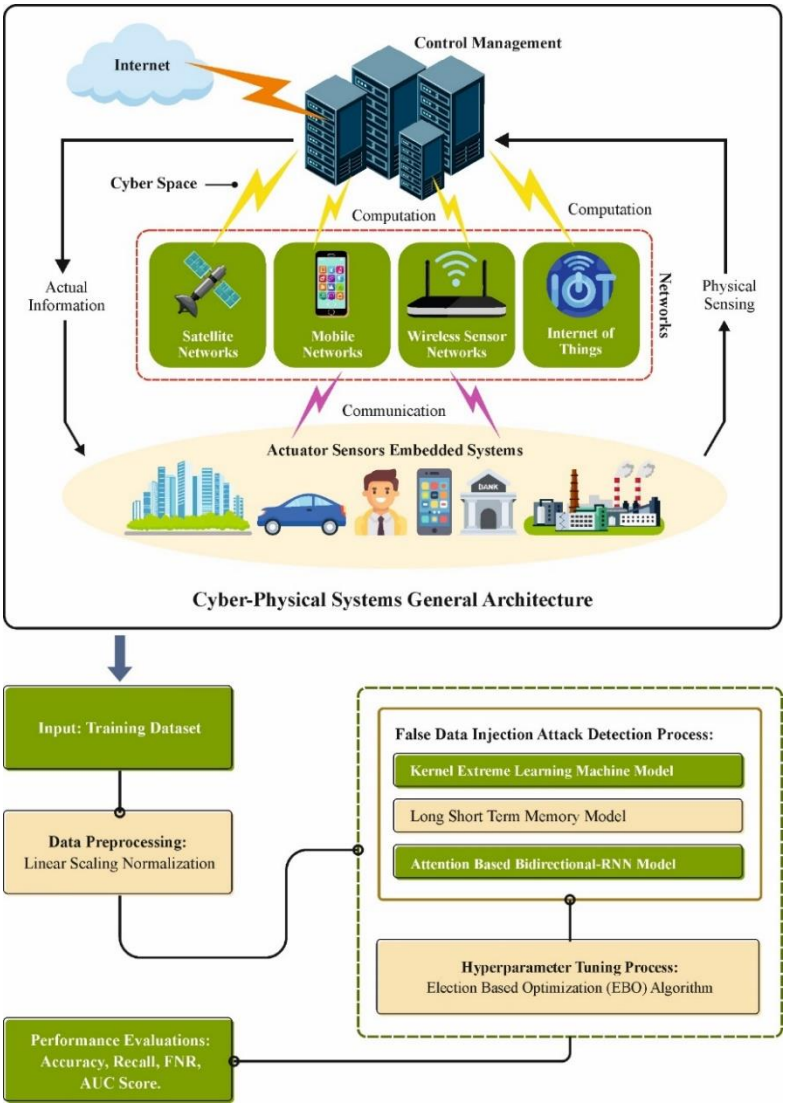

Figure 1. Overall process of the EBODL-FDIAD technique.

3.1. Data preprocessing

At the primary level, the EBODL-FDIAD technique applies the LSN approach to be used for scaling the input data into valuable formats. The LSN is a data preprocessing method developed for improving the comparability of features within a dataset [25]. By converting the values of distinct features through linear scaling, LSN confirms that every feature gives proportionally to the overall analysis without being disproportionately impacted by variances in scale. This system maps the original feature values to a standardized range, normally between 0 and 1, making the data more responsive to different ML methods and statistical analyses. LSN is mainly valued in conditions where disparate scales among features could skew model efficiency, offering a robust and effectual means to standardize datasets for increased interpretability and accuracy in analytical methods.

3.2. Ensemble learning

The EBODL-FDIAD technique performs ensemble learning classification comprising three classifiers, namely the KELM, LSTM, and ABiRNN models.

3.2.1. KELM model

As an advanced model, KELM is proposed based on the ELM model [26]. The kernel function has faster learning ability and better generalization performance. ELM is a feedforward neural network that consists of a hidden layer (HL), input layers, and output layers, and it can be mathematically modeled by,

$$H\beta = T, \tag{1}$$

$$H(w_1, \ldots, w_1, b_1, \ldots, b_1, x_1, \ldots, x_n) = \begin{pmatrix} g(w_1 \cdot x_1 + b_1) & \ldots & g(w_1 \cdot x_1 + b_1) \\ \vdots & \ddots & \vdots \\ g(w_1 \cdot x_n + b_1) & \ldots & g(w_1 \cdot x_n + b_1) \end{pmatrix} \tag{2}$$

In the equation, H indicates the output matrix of HL, w_l shows the weight of the l^{th} neurons in the HL, T indicates the target output matrix, β refers to the output weight, and b_l shows the bias of the l^{th} neurons in the HL. The learning algorithm of ELM is used to resolve the output weight β using the least square model:

$$\beta_{ELM} = H^T(HH^T)^{-1}T = H^+T. \tag{3}$$

In Eq (3), H^+ denotes the generalized inverse matrix of H. Figure 2 shows the structure of the KELM model.

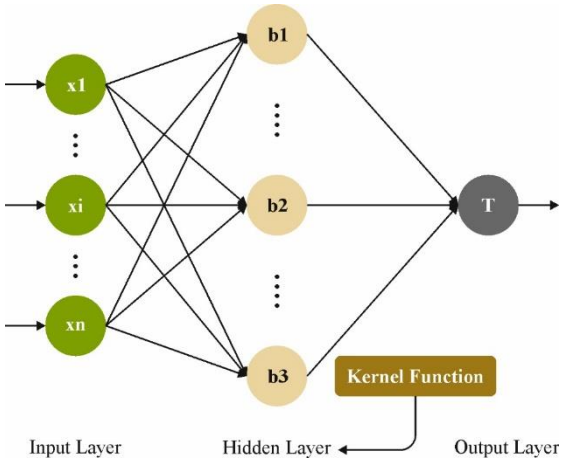

Figure 2. Framework of KELM.

In KELM, the kernel function parameters γ and regularization coefficient C are introduced to enhance KELM accuracy, and the kernel function matrix can be formulated by:

$$\Omega = HH^T, \tag{4}$$

$$\Omega_{ij} = h(X_i)h(x_j) = K(x_i \times x_j). \tag{5}$$

Next, the least square (LS) solution of β values of the KELM is:

$$\beta_{KELM} = H^T \left(\frac{I}{C} + HH^T\right)^{-1} T. \tag{6}$$

According to the abovementioned equation, the output function of KELM is formulated by:

$$f(x) = \begin{bmatrix} K(x, x1) \\ \vdots \\ K(x, x_n) \end{bmatrix} \left(\Omega + \frac{I}{C}\right)^{-1} T. \tag{7}$$

Additionally, the radial basis function (RBF) is desired as a kernel operation and its formula can be written as:

$$K(x_i, x_j) = \exp\left(-\frac{||x-x||^2}{2\gamma^2}\right). \tag{8}$$

In Eq (8), γ implies the kernel parameter.

3.2.2. LSTM model

LSTM can be a type of RNN. LSTM is used to replace the computation of hidden states with multiple gate functions [27]. This allows for capturing long-term dependence in the temporal data sequence. The LSTM presents an original flow, the cell state $m_t \in \mathbb{R}^n$ revealed at the top of the cell structure than traditional RNN. LSTM can add or remove the data to the cell states. The cell state retains the LSTM memory. A 3-gating model regulates the data flow in LSTM consisting of the input gate $i_t \in \mathbb{R}^n$, the forget gate $f_t \in \mathbb{R}^n$, and the output gate $o_t \in \mathbb{R}^n$. The input gate is used to adjust the level of data from the existing input x_t and the prior HL s_{t-1} is fed into the existing state. The forget gate regulates what data at the prior cell state m_{t-1} must be retained. The output gate regulates what amount of data is passed into the existing hidden state s_t. The operation of this gate is given below:

$$i_t = \sigma(V_i x_t + W_i s_{t-1} + b_i), \tag{9}$$

$$f_t = \sigma(V_f x_t + W_f s_{t-1} + b_f), \tag{10}$$

$$o_t = \sigma(V_o x_t + W_o s_{t-1} + b_o), \tag{11}$$

with the parameters V_i, V_f, $V_o \in \mathbb{R}^{n\times p}$; W_i, W_f, $W_o \in \mathbb{R}^{n\times n}$; and b_i, b_f, $b_o \in \mathbb{R}^{n\times 1}$. σ refers to the sigmoid activation function.

Next, the cell state and HL are attained as follows.

$$g_t = \tanh(V_m x_t + W_m s_{t-1} + b_m), \tag{12}$$

$$m_t = f_t \circ m_{t-1} + i_t \circ g_t, \tag{13}$$

$$s_t = o_t \circ \tanh(m_t). \tag{14}$$

The equation ∘ indicates the component-wise multiplication.$V_m \in \mathbb{R}^{n\times p}$;$W_m \in \mathbb{R}^{n\times n}$;and $b_m \in \mathbb{R}^{n\times 1}$. tanh refers to the hyperbolic tangent function.

The LSTM training is performed by the BPTT by reducing the main function on the set of training sequences. This gradient of weight and bias is evaluated at each time step. Next, with the traditional optimization approaches (for example, stochastic gradient descent (SGD), root mean square propogation (RMSprop), or adaptive moment estimation (Adam)), the optimum parameter is attained.

3.2.3. ABiRNN model

RNN can capture temporal patterns in the information [28]. Typical RNN is unidirectional, such that the input dataset is processed in a temporal sequence. The shortcoming of RNNs is that they are limited to the usage of prior context. A bidirectional recurrent neural network (BRNN) provides a solution by performing the data processing in backward and forward directions. The structure of BRNN unfolded in time for the T time step. The BRNN includes backward and forward layers. The h_t^f forward layer can be evaluated by processing the input dataset from $t = 1, \ldots, T$, and the h_t^b backward layer can be evaluated by processing the input dataset from $t = T, \ldots, 1$ with output from both layers combined using the following equations:

$$h_t^f = tanh\left(W_{xh}^f x_t + W_{hh}^f h_{t-1} + b_h^f\right), \tag{15}$$

$$h_t^b = tanh\left(W_{xh}^b x_t + W_{hh}^b h_{t+1} + b_h^b\right), \tag{16}$$

$$y_t = W_{hy}^f h_t^f + W_{hy}^b h_t^b + b_y). \tag{17}$$

The output vector y_t attained by processing the series of input datasets from $t = 1, \ldots, T$ was later fed into the attention layer. The dimensional of the hidden layer in the backward and forward direction is 50, with the output at the time step being a 100-size vector.

Paroxysmal atrial fibrillation (PAF) takes place as an intermittent period of AF scattered with episodes of normal sinus rhythm. Therefore, a soft attention module is applied on top of BRNN such that more attention (or emphasis) is gained with a high prevalence of AF. The attention model is expressed in the following. The output from BRNN $[y_1, y_2, y_T]$ is combined into matrix Y, which is of N x T size, where N denotes the size of output vector y_t and T refers to the length of the input series. The weight output vector h_{att} of the attention layer is given below:

$$\alpha = softmax(w_{att}^T Y), \tag{18}$$

$$h_{att} = Y\alpha^T. \tag{19}$$

α refers to the weight vector calculated from matrix y, and the output h_{att} is computed as a weighted sum of the output vector from BRNN (h_{att} is a 100-dimensional vector).

3.3. Hyperparameter tuning using EBO

For choosing the optimum hyperparameter for the ensemble classifiers, the EBO algorithm can be applied. Trojovsky and Dehghani proposed EBOA as a stochastic-based optimizer [29]. The

mathematical modeling of the optimizer is discussed below:

1) Initialization

A participant of the community makes up the EBOA, a metaheuristic approach that works in the population dynamics manner. In the EBOA population, all individuals have a different method to address the issues at hand. A matrix named as a population matrix depicts the EBOA population from a mathematical perspective.

Initial positions of individuals in the search space are randomly allocated as follows:

$$x_{i,j} = lb_j + r \cdot \left(ub_j - lb_j\right), |i = 1,2, \dots, N, j = 1,2, \dots, m \tag{20}$$

In Eq (20), a random integer in the range [0,1] is r, and lb_j and ub_j are the upper and lower limits of the j^{th} variable, correspondingly. According to the value suggested by each participant of EBO, the value for the objective function (OF) is evaluated for the problem variable. The vector shows the estimated value for the OF of the problem:

$$OF = \begin{bmatrix} \&OF_{\&1} \\ \&. \\ \&. \\ \&. \\ \&OF_{\&i} \\ \&. \\ \&. \\ \&. \\ \&OF_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} \&OF_{\&1} \\ \&. \\ \&. \\ \&. \\ \&OF_{\&i} \\ \&. \\ \&. \\ \&. \\ \&OF(X_N) \end{bmatrix}_{N\times 1} . \tag{21}$$

In Eq (21), OF refers to the objective function value of the vector of the EBOA population and OF_i is the computed value of OF for i^{th} participants of EBOA. Similar to other optimization techniques, EBOA has two different stages, namely the mathematical representation and physical explanation, which are described in the following section.

2) Voting and holding elections methods (exploration stage)

Participants of EBOA vote for a candidate in the election depending upon how well-informed they are. Their awareness may rely on how high quality the OFs will be and it can be mathematically modeled as follows:

$$A_i = \begin{cases} \frac{OF_i - OF_{worst}}{OF_{best} - OF_{worst}}, | \ OF_{best} \neq OF_{worst}; \\ 1, | \qquad else, \end{cases} \tag{22}$$

In Eq (22), A_i refers to the level of awareness of i^{th} participants and oF_{best} and OF_{worst} are the best and worst values of OF, correspondingly. In the minimization problem, there is a minimum of two people running for choice on the default assumption of EBOA that the minimal candidate number of (N_C), (viz., $N_C \geq 2$) is two.

The voter's responsiveness is evaluated to be a random integer for determining who gets voted

for in EBOA. If the voter's information is higher than the random integer, then that voter must select the fittest candidate (C_1). Then, the vote will be randomly distributed among the remaining contenders. This voting procedure can be mathematically modeled as follows:

$$V_i = \begin{cases} C_1, & A_i > r; \\ C_k, & else. \end{cases} \tag{23}$$

In Eq (23), y_i refers to the i^{th} voter's preference, C_1 denotes the top pick, and C_k indicates the k^{th} candidates, where k indicates an integer selected randomly from $\{2,3,\dots,N_C\}$.

Finally, the winner is determined (leader) when each vote has been counted. Even individuals who did not vote for the leader nevertheless sensed the effect of their decisions and policies. Based on the elected leader's recommendation, participants of the EBOA are specified new roles and tasks. This leader enhances the EBOA's ability for exploration by guiding the population method to different portions of the search space.

The leader directs the EBOA process with new individuals, and each receives a new role. The positions that are generated are recognized to use, thereby increasing the worth of the goal function. The participants retain their prior status in the absence of movement. Using Eqs (24) and (25), the EBOA process for updating itself is given:

$$x_{i,j}^{new,P1} = \begin{cases} x_{i,j} + r \cdot (L_j| - |l| \cdot |x_{i,j}), & OF_L < OF_i; \\ x_{i,j} + r \cdot (x_{i,j}| - |L_j), & else. \end{cases} \tag{24}$$

$$X_i = \begin{cases} X_i^{new.P1}, & OF_i^{new,P1} < OF_i; \\ X_i, & else. \end{cases} \tag{25}$$

where $X_i^{new.P1}$ is a new location generated for the i^{th} participants, $x_{i,j}^{new,P1}$ refers to the i^{th} participant of j^{th} dimensions, $OF_i^{new,P1}$ indicates the value of OF, I shows the random integer within [1,2], L refers to the leader, L_i shows the j^{th} dimensions, and OF_L indicates the OF value.

3) Raising awareness via public movement (exploitation stage)

Person awareness has a big effect on how we make decisions. A restricted search near the predicted solution might support determining the best one, to put it mathematically. Increasing the values of OF makes that individual extra aware and makes them make better decisions in the upcoming choice. Eqs (26) and (27) are used for increasing the public awareness of EBOA.

$$x_{i.j}^{new,P2} = x_{i,j} + (1 - 2r) \cdot R \cdot \left(1 - \frac{t}{T}\right) \cdot x_{i,j}, \tag{26}$$

$$X_i = \begin{cases} X_i^{new,P2}, | & OF_i^{new,P2} < OF_i; \\ X_i, | & else. \end{cases} \tag{27}$$

where $X_i^{new.P2}$ indicates a new location for the i^{th} population, $OF_i^{new,P2} j$ refers to the j^{th} variable, $OF_i^{new,P2}$ refers to the value of OF, R refers to the constant equivalent to 0.02, t denotes the repetition counter, and T indicates the overall performed iterations.

The fitness selection is the substantial factor impacting the effectiveness of the EBO methods. The hyperparameter selection procedure contains the solution encoding technique for evaluating the efficacy of the candidate solutions. The EBO algorithm deliberates accuracy as the important measure to develop the fitness function (FF) that can be given in equation form:

$$Fitness = \max(P), \tag{28}$$

$$P = \frac{TP}{TP+FP}. \tag{29}$$

Here, FP denotes the false positive and TP means the true positive values.

4. Experimental validation

The FDIA detection results of the EBODL-FDIAD technique are demonstrated in this section. The results were tested using two aspects: IEEE-14 and IEEE-39 standard bus systems. Table 1 reports a detailed comparison study of the EBODL-FDIAD technique under the IEEE-14 standard bus system [14].

Table 1. Comparison outcome of the EBODL-FDIAD technique with other systems on the IEEE14 standard system [14].

IEEE14 standard system				
Methods	$Accu_y$	$Reca_l$	***FNR***	AUC_{score}
Training Phase				
EBODL-FDIAD	97.97	97.85	2.08	98.79
MRFODL-FDIAD	96.89	96.85	3.37	97.61
SVM Model	90.33	91.80	8.43	91.86
CNN Algorithm	89.71	92.95	7.30	90.96
MSA Model	90.53	90.48	9.77	89.89
CDBN Algorithm	91.82	92.75	7.49	93.64
SVM-GAB	90.82	92.07	8.16	92.30
Testing Phase				
EBODL-FDIAD	98.60	98.37	1.34	98.73
MRFODL-FDIAD	97.81	97.57	2.68	97.08
SVM Model	91.17	90.66	9.57	91.44
CNN Algorithm	92.21	92.93	7.30	90.96
MSA Model	90.23	89.44	10.81	91.62
CDBN Algorithm	93.72	92.95	7.31	90.07
SVM-GAB	93.79	91.38	8.86	90.30

Figure 3 provides a brief, comparative $accu_y$ analysis of the EBODL-FDIAD technique on the IEEE14 standard system. The figure implies that the SVM, CNN, MSA, CDBN, and SVM-GAB techniques reported the least performance and the MRFODL-FDIAD model exhibited slightly boosted results. In addition, the results show that the EBODL-FDIAD technique gained increased values of $accu_y$. With TRP, the EBODL-FDIAD technique offered a higher $accu_y$ of 97.97%, whereas the MRFODL-FDIAD, SVM, CNN, MSA, CDBN, and SVM-GAB models obtained reduced $accu_y$ of 96.89%, 90.33%, 89.71%, 90.53%, 91.82%, and 90.82%, respectively.

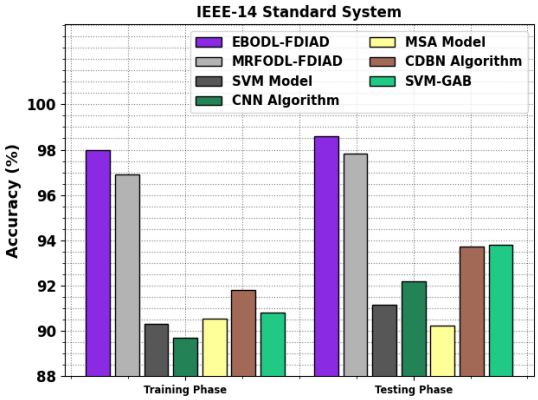

Figure 3. $Accu_y$ analysis of the EBODL-FDIAD technique on the IEEE14 standard system.

Figure 4 displays a comprehensive, comparative $reca_l$ analysis of the EBODL-FDIAD system on the IEEE14 standard system. The figure shows that the SVM, CNN, MSA, CDBN, and SVM-GAB methods described the least performance and the MRFODL-FDIAD system shows somewhat increased results. Moreover, the results revealed that the EBODL-FDIAD technique had increased values of $reca_l$. With TRP, the EBODL-FDIAD method provided a higher $reca_l$ of 97.85%, whereas the MRFODL-FDIAD, SVM, CNN, MSA, CDBN, and SVM-GAB techniques acquired decreased $reca_l$ of 96.85%, 91.80%, 92.95%, 90.48%, 92.75%, and 92.07%, respectively.

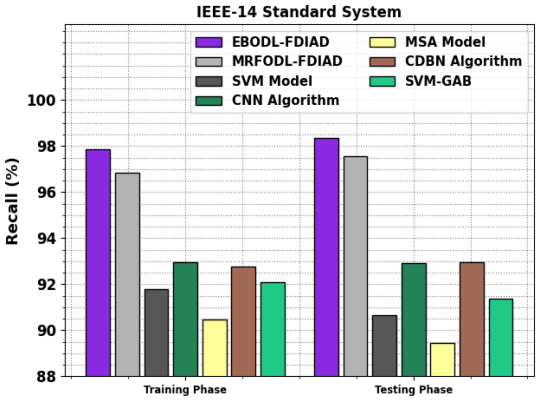

Figure 4. $Reca_l$ analysis of the EBODL-FDIAD technique on the IEEE14 standard system.

Figure 5 offers a brief, comparative AUC_{score} analysis of the EBODL-FDIAD method on the IEEE14 standard system. The figure exhibits that the SVM, CNN, MSA, CDBN, and SVM-GAB algorithms reported decreased performance and the MRFODL-FDIAD method displays slightly boosted results. In addition, the outcomes prove that the EBODL-FDIAD method gained increased values of AUC_{score}. According to TRP, the EBODL-FDIAD system provided a greater AUC_{score} of 98.79%, but the MRFODL-FDIAD, SVM, CNN, MSA, CDBN, and SVM-GAB algorithms had a diminished AUC_{score} of 97.61%, 91.86%, 90.96%, 89.89%, 93.64%, and 92.30%, respectively.

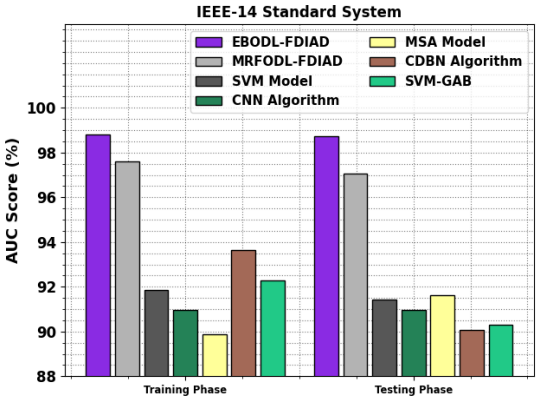

Figure 5. AUC_{score} analysis of the EBODL-FDIAD technique on the IEEE14 standard system.

Figure 6 illustrates a wide-ranging comparison of the FNR analysis of the EBODL-FDIAD method with the IEEE14 standard system. This figure showcases that the SVM, CNN, MSA, CDBN, and SVM-GAB techniques informed poorer performance and the MRFODL-FDIAD system displayed moderately improved outcomes. Additionally, the results revealed that the EBODL-FDIAD system had higher values of FNR. With TRP, the EBODL-FDIAD system acquired an increased FNR of 2.08, however, the MRFODL-FDIAD, SVM, CNN, MSA, CDBN, and SVM-GAB techniques had minimized FNR of 3.37, 8.43, 7.30, 9.77, 7.49, and 8.16, respectively.

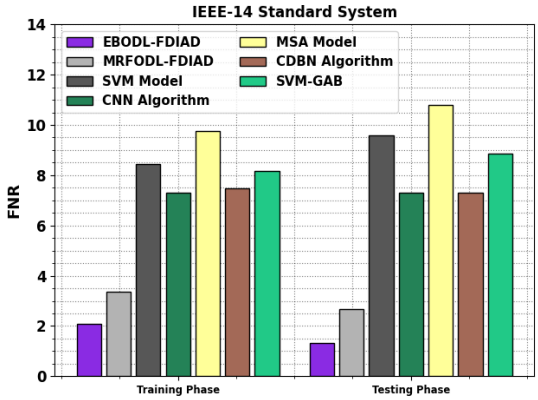

Figure 6. FNR analysis of the EBODL-FDIAD technique on the IEEE14 standard system.

The $accu_y$ curves for training (TRA) and validation (VL) shown in Figure 7 for the EBODL-FDIAD technique on the IEEE14 standard system give valued insights into its effectiveness at varying epochs. Mainly, it can be a reliable upgrade in both TRA and TES $accu_y$ with raised epochs, representing the proficiency of the model for learnable and recognizable patterns from TRA and TES data. The increased trends in TES $accu_y$ underscore the model flexibility of the TRA dataset and the ability to precisely create predictions on unnoticed data, emphasizing capabilities of robust generalization.

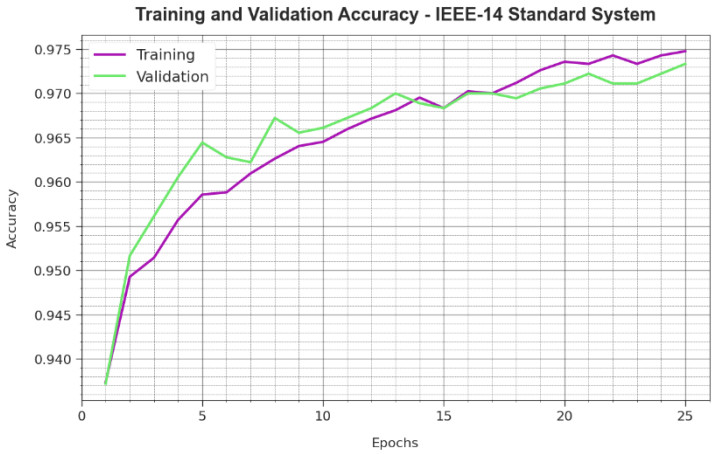

Figure 7. $Accu_y$ curve of the EBODL-FDIAD technique on the IEEE14 standard system.

Figure 8 displays a comprehensive overview of the TRA and TES loss values for the EBODL-FDIAD algorithm on the IEEE14 standard system at diverse epochs. The TRA loss reliably decreases as the model refines weights to diminish the classification errors under both datasets. These loss curves explain the arrangement of the model with the TRA data, emphasizing the ability to capture patterns effectually. The incessant improvement of parameters in the EBODL-FDIAD system can be significant, targeted at lessening differences between predictions and actual TRA labels.

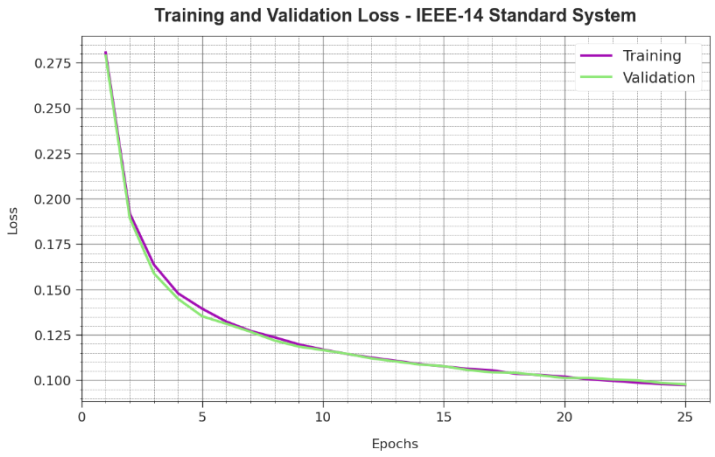

Figure 8. Loss curve of the EBODL-FDIAD technique on the IEEE14 standard system.

Table 2 reports an extensive comparison outcome of the EBODL-FDIAD technique on the IEEE-39 standard bus system. Figure 9 represents a wide-ranging, comparative $accu_y$ analysis of the EBODL-FDIAD method with the IEEE39 standard system.

Table 2. Comparison result of the EBODL-FDIAD model with other algorithms on the IEEE-39 standard system [14].

IEEE39 standard system				
Methods	$Accu_y$	$Reca_l$	FNR	AUC_{score}
Training Phase				
EBODL-FDIAD	98.17	98.56	1.47	97.98
MRFODL-FDIAD	96.79	97.70	2.55	96.82
SVM Model	90.72	92.03	8.22	90.72
CNN Algorithm	94.21	91.11	9.14	93.89
MSA Model	94.06	89.51	10.73	89.89
CDBN Algorithm	92.26	94.10	6.13	94.29
SVM-GAB	91.33	89.83	10.41	90.62
Testing Phase				
EBODL-FDIAD	98.52	97.96	1.28	98.58
MRFODL-FDIAD	97.28	96.80	3.15	97.08
SVM Model	92.46	89.39	7.19	93.04
CNN Algorithm	92.67	93.65	10.48	89.77
MSA Model	90.11	91.22	6.41	93.82
CDBN Algorithm	91.66	90.69	10.75	89.49
SVM-GAB	89.91	89.64	8.38	91.86

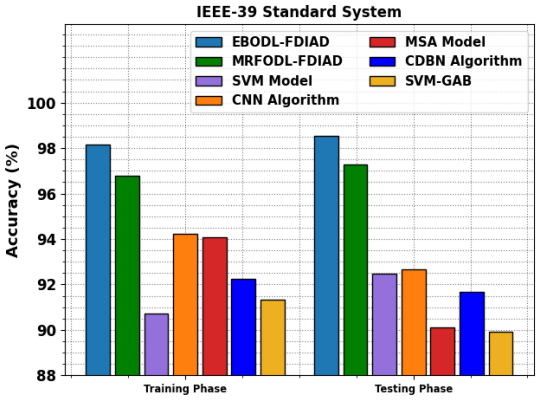

Figure 9. $Accu_y$ analysis of the EBODL-FDIAD technique on the IEEE39 standard system.

This figure indicates that the SVM, CNN, MSA, CDBN, and SVM-GAB techniques described minimized performance and the MRFODL-FDIAD method shows moderately improved outcomes. Moreover, the results exhibit that the EBODL-FDIAD technique had improved values of $accu_y$. With TRP, the EBODL-FDIAD algorithm had boosted $accu_y$ of 98.77%, while the MRFODL-FDIAD, SVM, CNN, MSA, CDBN, and SVM-GAB algorithms obtained decreased $accu_y$ of 96.79%, 90.72%, 94.21%, 94.06%, 92.26%, and 91.33%, respectively.

Figure 10 illustrates a comprehensive, comparative $reca_l$ analysis of the EBODL-FDIAD system on the IEEE39 standard system. This figure shows that the SVM, CNN, MSA, CDBN, and SVM-GAB algorithms had the least performance and the MRFODL-FDIAD system reveals somewhat improved

results. Meanwhile, the results denoted that the EBODL-FDIAD method achieved greater values of $reca_l$. With TRP, the EBODL-FDIAD method provided an increased $reca_l$ of 98.56%, while the MRFODL-FDIAD, SVM, CNN, MSA, CDBN, and SVM-GAB approaches acquired lessened $reca_l$ of 97.70%, 92.03%, 91.11%, 89.51%, 94.10%, and 89.83%, respectively.

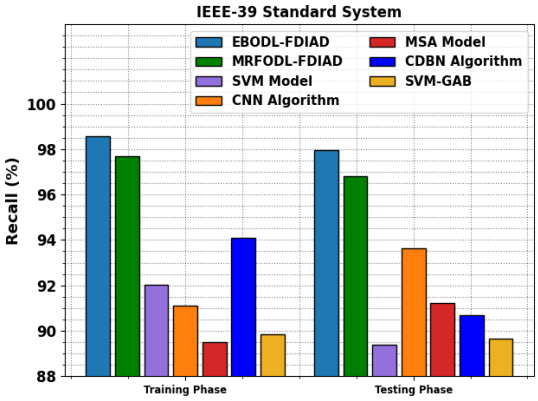

Figure 10. $Reca_l$ outcome of the EBODL-FDIAD method with the IEEE39 standard system.

Figure 11 demonstrates an extensive, comparative AUC_{score} analysis of the EBODL-FDIAD method with the IEEE39 standard system. This figure indicates that the SVM, CNN, MSA, CDBN, and SVM-GAB systems stated less performance and the MRFODL-FDIAD system displayed moderately boosted outcomes. Additionally, the results presented that the EBODL-FDIAD algorithm had greater values of AUC_{score}. With TRP, the EBODL-FDIAD technique offered an increased AUC_{score} of 98.79%, whereas the MRFODL-FDIAD, SVM, CNN, MSA, CDBN, and SVM-GAB algorithms achieved minimized AUC_{score} of 97.98%, 96.82%, 90.72%, 93.89%, 89.89%, and 94.29%, respectively.

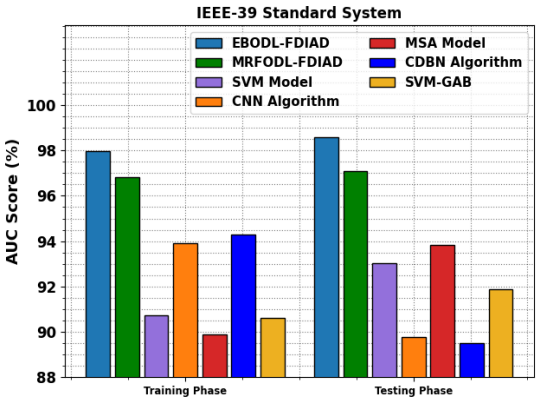

Figure 11. AUC_{score} outcomes of the EBODL-FDIAD algorithm with the IEEE39 standard system.

Figure 12 displays a brief comparison of the FNR outcomes of the EBODL-FDIAD method on the IEEE39 standard system. The figure implies that the SVM, CNN, MSA, CDBN, and SVM-GAB

algorithms reported the least performance and the MRFODL-FDIAD model exhibited somewhat boosted results. Simultaneously, the results show that the EBODL-FDIAD method gained raised values of FNR. With TRP, the EBODL-FDIAD algorithm provided a higher FNR of 1.47, whereas the MRFODL-FDIAD, SVM, CNN, MSA, CDBN, and SVM-GAB techniques obtained reduced FNR of 2.55, 8.22, 9.14, 10.73, 6.13, and 10.41, respectively.

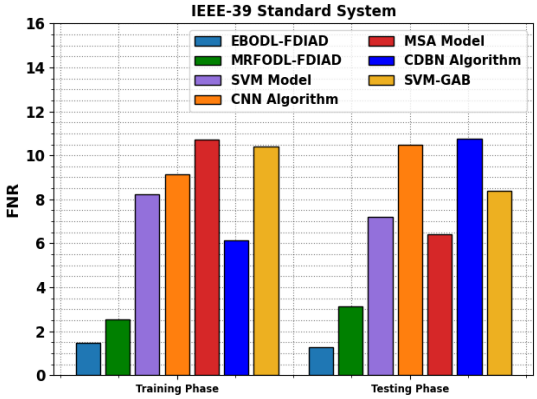

Figure 12. FNR analysis of the EBODL-FDIAD technique on the IEEE39 standard system.

The $accu_y$ curves for TRA and VL shown in Figure 13 for the EBODL-FDIAD algorithm with the IEEE39 standard system provide valued insights into its efficiency at various epochs. Primarily, it can be a consistent upgrade in both TRA and TES $accu_y$ with higher epochs, representing the proficiency of the model for learnable and recognizable patterns from both TRA and TES data. The raised trends in TES $accu_y$ underscore the model flexibility of the TRA dataset and the ability to precisely produce predictions on undetected data, underscoring capabilities of robust generalization.

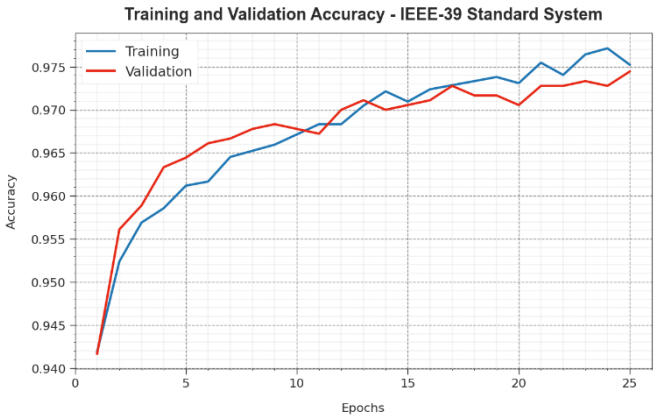

Figure 13. $Accu_y$ curve of the EBODL-FDIAD technique under the IEEE39 standard system.

Figure 14 provides an extensive outcome of the TRA and TES loss values for the EBODL-FDIAD method on the IEEE39 standard system at diverse epochs. The TRA loss is reliably minimized as the model refines weights to lessen the classification errors under both datasets. The loss curves represent

the model arrangements with the data of TRA, emphasizing the ability to capture patterns successfully. The continuous improvement of parameters in the EBODL-FDIAD system can be significant, targeted at lessening variances between actual and predicted TRA labels. These accomplished outcomes ensure the enhanced performance of the EBODL-FDIAD method on the FDIA detection process.

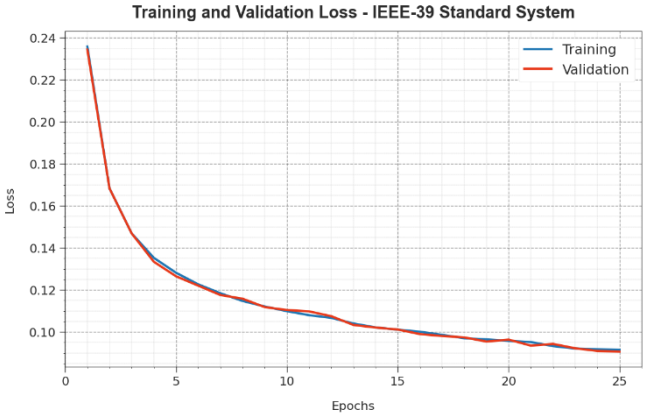

Figure 14. Loss curve of the EBODL-FDIAD technique with the IEEE39 standard system.

5. Conclusions

In this manuscript, we offered the design of an EBODL-FDIAD method in the CPS platform. The purpose of the EBODL-FDIAD algorithm was to enhance security in the CPS environment via the detection of FDIAs. It contains three different processes, namely data preprocessing, ensemble learning, and EBO-based parameter tuning. At the primary level, the EBODL-FDIAD technique applies the LSN approach, which can be used for scaling the input data into valuable formats. In addition, the EBODL-FDIAD technique performs ensemble learning classification comprising three classifiers, namely the KELM, LSTM, and ABiRNN models. For optimal hyperparameter selection of the ensemble classifiers, the EBO algorithm was applied. To validate the enriched performance of the EBODL-FDIAD method, comprehensive simulations were involved. The extensive results highlighted that the EBODL-FDIAD technique performed well over other systems for diverse measures. In future work, the EBODL-FDIAD methodology can be provided by integrating methods from adversarial ML to improve its robustness against sophisticated attacks. By actively creating adversarial examples and training the model to detect and diminish them, this model is optimum for defending against evasion and poisoning efforts by adversaries. Also, exploring the application of federated learning methods to allow collaborative training across distributed CPS platforms are additional developments of the scalability and generalization abilities of the model that can be studied, enabling more effectual recognition of FDIAs in large-scale and heterogeneous systems.

Use of AI tools declaration

The authors declare that they have not used artificial intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through a large group research project under grant number (RGP2/02/44); Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R384), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia; and Research Supporting Project number (RSPD2024R608), King Saud University, Riyadh, Saudi Arabia. The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA, for funding this research work through the project number "NBU-FPEJ-2024-2847-01". This study is partially funded by the Future University in Egypt (FUE).

Conflict of interest

The authors declare that they have no conflicts of interest.

References

1. K. D. Lu, Z. G. Wu, Multi-objective false data injection attacks of cyber-physical power systems, *IEEE T. Circuits Syst. II*, **69** (2022), 3924–3928. https://doi.org/10.1109/TCSII.2022.3181827
2. P. L. Bhattar, N. M. Pindoriya, A. Sharma, A combined survey on distribution system state estimation and false data injection in cyber-physical power distribution networks, *IET Cyber Phys. Syst. Theory Appl*., **6** (2021), 41–62. https://doi.org/10.1049/cps2.12000
3. Y. Li, Y. Wang, Developing graphical detection techniques for maintaining state estimation integrity against false data injection attack in integrated electric cyber-physical system, *J. Syst. Architect.*, **105** (2020), 101705. https://doi.org/10.1016/j.sysarc.2019.101705
4. Q. Wang, W. Tai, Y. Tang, M. Ni, Review of the false data injection attack against the cyber-physical power system, *IET Cyber Phys. Syst. Theory Appl.*, **4** (2019), 101–107. https://doi.org/10.1049/iet-cps.2018.5022
5. S. Padhan, A. K. Turuk, Design of false data injection attacks in cyber-physical systems, *Inform. Sci.*, **608** (2022), 825–843. https://doi.org/10.1016/j.ins.2022.06.082
6. T. Zhou, K. Xiahou, L. L. Zhang, Q. H. Wu, Real-time detection of cyber-physical false data injection attacks on power systems, *IEEE T. Ind. Inform*., **17** (2021), 6810–6819. https://doi.org/10.1109/TII.2020.3048386
7. Z. Qu, Y. Dong, N. Qu, H. Li, M. Cui, X. Bo, et al., False data injection attack detection in power systems based on cyber-physical attack genes, *Front. Energy Res.*, **9** (2021), 644489. https://doi.org/10.3389/fenrg.2021.644489
8. G. Cao, W. Gu, G. Lou, W. Sheng, K. Liu, Distributed synchronous detection for false data injection attack in cyber-physical microgrids, *Int. J. Elec. Power Energy Syst.*, **137** (2022), 107788. https://doi.org/10.1016/j.ijepes.2021.107788
9. J. Li, C. Sun, Q. Su, Analysis of cascading failures of power cyberphysical systems considering false data injection attacks, *Global Energy Interconnect.*, **4** (2021), 204–213. https://doi.org/10.1016/j.gloei.2021.05.002

10. T. Zou, A. S. Bretas, C. Ruben, S. C. Dhulipala, N. Bretas, Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks, *Electr. Pow. Syst. Res.*, **187** (2020), 106490. https://doi.org/10.1016/j.epsr.2020.106490
11. M. Mazare, Adaptive optimal secure wind power generation control for variable speed wind turbine systems via reinforcement learning, *Appl. Energ.*, **353** (2024), 122034. https://doi.org/10.1016/j.apenergy.2023.122034
12. M. Mazare, M. Taghizadeh, H. Asharioun, Attack-resilient pitch angle control for variable-speed wind turbine systems under cyber threats, *Int. J. Adapt. Control*, **37** (2023), 1423–1439. https://doi.org/10.1002/acs.3580
13. M. Mazare, Reinforcement learning-based fixed-time resilient control of nonlinear cyber physical systems under false data injection attacks and mismatch disturbances, *J. Franklin I.*, **360** (2023), 14926–14938. https://doi.org/10.1016/j.jfranklin.2023.10.026
14. H. Alamro, K. Mahmood, S. S. Aljameel, A. Yafoz, R. Alsini, A. Mohamed, Modified red fox optimizer with deep learning enabled false data injection attack detection, *IEEE Access*, **11** (2023), 79256–79264. https://doi.org/10.1109/ACCESS.2023.3298056
15. J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach, *Phys. Commun.*, **47** (2021), 101394. https://doi.org/10.1016/j.phycom.2021.101394
16. K. Liu, H. Zhang, Y. Zhang, C. Sun, False data-injection attack detection in cyber–physical systems with unknown parameters: A deep reinforcement learning approach, *IEEE T. Cybernetics*, **11** (2023), 7115–7125. https://doi.org/10.1109/TCYB.2022.3225236
17. E. Vincent, M. Korki, M. Seyedmahmoudian, A. Stojcevski, S. Mekhilef, Detection of false data injection attacks in cyber–physical systems using graph convolutional network, *Electr. Pow. Syst. Res.*, **217** (2023), 109118. https://doi.org/10.1016/j.epsr.2023.109118
18. Y. Zhang, W. Deng, K. Huang, C. Yang, False data injection attack testbed of industrial cyber-physical systems of the process industry and a detection application. In: *2021 IEEE International Conference on Recent Advances in Systems Science and Engineering (RASSE)*, 2021, 1–7. https://doi.org/10.1109/RASSE53195.2021.9686839
19. Y. Li, X. Wei, Y. Li, Z. Dong, M. Shahidehpour, Detection of false data injection attacks in smart grid: A secure federated deep learning approach, *IEEE T. Smart Grid*, **13** (2022), 4862–4872. https://doi.org/10.1109/TSG.2022.3204796
20. W. Fu, Y. Yan, Y. Chen, Z. Wang, D. Zhu, L. Jin, Temporal false data injection attack and detection on cyber-physical power system based on deep reinforcement learning, *IET Smart Grid*, **7** (2024), 78–88. https://doi.org/10.1049/stg2.12141
21. H. Ruan, B. Dorneanu, H. Arellano-Garcia, P. Xiao, L. Zhang, Deep learning-based fault prediction in wireless sensor network embedded cyber-physical systems for industrial processes, *IEEE Access*, **10**(2022), 10867–10879. https://doi.org/10.1109/ACCESS.2022.3144333
22. J. Tian, C. Shen, B. Wang, X. Xia, M. Zhang, C. Lin, Q. Li, LESSON: Multi-label adversarial false data injection attack for deep learning locational detection, *IEEE T. Depend. Secure Comput.*, 2024, 1–15. https://doi.org/10.1109/TDSC.2024.3353302
23. J. Tian, B. Wang, R. Guo, Z. Wang, K. Cao, X. Wang, Adversarial attacks and defenses for deep-learning-based unmanned aerial vehicles, *IEEE Internet Things J.*, **9** (2021), 22399–22409. https://doi.org/10.1109/JIOT.2021.3111024

24. J. Tian, B. Wang, Z. Wang, K. Cao, J. Li, M. Ozay, Joint adversarial example and false data injection attacks for state estimation in power systems, *IEEE T. Cybernetics*, **52** (2022), 13699–13713. https://doi.org/10.1109/TCYB.2021.3125345
25. S. Sorguli, H. Rjoub, A novel energy accounting model using fuzzy restricted boltzmann machine—Recurrent neural network, *Energies*, **16** (2023), 2844. https://doi.org/10.3390/en16062844
26. Q. Hu, H. Zhou, C. Wang, C. Zhu, J. Shen, P. He, Time-frequency fusion features-based GSWOA-KELM model for gear fault diagnosis, *Lubricants*, **12** (2024), 10. https://doi.org/10.3390/lubricants12010010
27. M. Xia, X. Zheng, M. Imran, M. Shoaib, Data-driven prognosis method using hybrid deep recurrent neural network, *Appl. Soft Comput.*, **93** (2020), 106351. https://doi.org/10.1016/j.asoc.2020.106351
28. S. P. Shashikumar, A. J. Shah, G. D. Clifford, S. Nemati, Detection of paroxysmal atrial fibrillation using attention-based bidirectional recurrent neural networks, In: *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2018, 715–723. https://doi.org/10.1145/3219819.3219912
29. M. Abd Elaziz, M. E. Zayed, H. Abdelfattah, A. Q. Aseeri, E. M. Tag-eldin, M. Fujii, et al., Machine learning-aided modeling for predicting freshwater production of a membrane desalination system: A long-short-term memory coupled with election-based optimizer, *Alex. Eng. J.*, **86** (2024), 690–703. https://doi.org/10.1016/j.aej.2023.12.012

AIMS Press