Explainable Artificial Intelligence with Chicken Swarm Optimization Based Web Phishing Detection and Classification on Cyber-Physical Systems

Alanoud Subahi[1,*]

[1] *Faculty of Computing and Information Technology, Department of Information Technology, King Abdulaziz University, Rabigh 25732, Saudi Arabia. asubahi@kau.edu.sa*

Abstract

At present, phishing attacks have developed as the most noticeable social network attacks controlled by government, public internet users, and businesses. Phishing websites is a cyberattack that mainly targets online user to steal their confidential data including banking details and login credentials. The websites phishing arise identical to their equal legitimate websites for appealing wide range of Internet users. The attacker cheats the user by suggesting the covered webpage as reliable or legitimate to recover its significant data. Numerous solutions for phishing websites attack had been introduced like heuristics, whitelisting or blacklisting, and Machine Learning (ML) based models. This study focuses on the design of Chicken Swarm Optimization with Explainable Artificial Intelligence using Phishing Detection and Classification (CSOXAI-PDC) techniques on Cyber-Physical Systems. The projected CSOXAI-PDC method emphasizes the effectual classification and recognition of phishing based on CPS. To attain this, the developed CSOXAI-PDC technique first executes the data normalization method. Next, the classification of phishing recognition occurs utilizing deep Q network (DQN) classifier. For enhancing the classification performance of DQN classifier, the hyperparameter tuning method can be done using the chicken swarm optimization (CSO) algorithm. Eventually, the CSOXAI-PDC method incorporates the XAI method LIME for superior clarification and perception of the black-box procedure for accurate identification of intrusions. The experimental analysis of the CSOXAI-PDC method is executed against real dataset and the outcomes establish the improvement of the projected method over existing techniques.

Keywords

Phishing Detection, Artificial Intelligence, Cyber-Physical System, Chicken Swarm Optimization, Data Normalization

1. Introduction

Criminals engaging in Internet fraud are growing in number and professionality. Cyber-attacks are different, cultured, and common. Internet fraud usually involves the confidential theft of data from an individual or organization for blackmail intentions, generating important tasks for cybersecurity authorities [1]. The latest study has effectively identified phishing attacks on the internet. Phishing is the challenge to snip private data like passwords, credit card numbers, and

Proceedings of SNSFAIT 2024: International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies, Delhi, India, August 08-09th, 2024

[1*] Corresponding author: Alanoud Subahi

asubahi@kau.edu.sa

https://orcid.org/0000-0002-8642-1708

usernames (and, indirectly, money) by imitating a truthful object in electrical contact, normally for dangerous tenacities [2]. Since the usage of bait to latch a victim is equivalent, these words were coined as a fishing homophone [3]. Phishing is normally performed with direct messaging or e-mail spoofing, and it repeatedly craves the public to provide private data on a wrong webpage that look-alike the same as the genuine one [4]. Victims are regularly tempted through communications that seem from banks, social media platforms, IT administrators, auction sites, or online payment computers [5]. Numerous websites have established auxiliary machines to applications like game maps, still, they must be visibly labeled as to who assembled them, and customers should not apply similar passwords over the internet.

Machine learning (ML) and modern Artificial Intelligence (AI) methods became well-active in some human life applications, and various earlier investigators applied ML in safety domains [6]. Computer security attacks were categorized into three kinds: semantic attacks, physical attacks, and synthetic attacks [7]. Phishing is the major semantic attack type. This technique can be learned to differentiate between harmful and benign activities by seeing a range of indicators and attributes [8]. These are trained on various data sets that hold phishing and legitimate incidents together. By robotically recognizing related features from rare data inputs, deep learning (DL) models namely recurrent neural network (RNN) and Convolutional Neural Networks (CNNs) accept its ability next step [9]. CNNs are appropriate for examining the web page's content, photographs, and other visual evidence linked to phishing challenges then they are experts at developing hierarchical depictions from graphical inputs. Nevertheless, RNNs are trained at modeling consecutive information that permits for identifying time-based trends and user activities that can specify phishing work [10].

This study focuses on the design of Chicken Swarm Optimization with Explainable Artificial Intelligence using Phishing Detection and Classification (CSOXAI-PDC) techniques on Cyber-Physical Systems. To attain this, the developed CSOXAI-PDC technique first executes data normalization method. Next, the classification of phishing recognition occurs utilizing deep Q network (DQN) classifier. For enhancing the classification performance of DQN classifier, the hyperparameter tuning method can be done using the chicken swarm optimization (CSO) algorithm. Eventually, the CSOXAI-PDC method incorporates the XAI method LIME for superior clarification and perception of the black-box procedure for accurate identification of intrusions. The experimental analysis of the CSOXAI-PDC method is executed against real dataset and the outcomes establish the improvement of the projected method over recent techniques.

2. Literature Survey

Alotaibi *et al.* [11] propose an adaptive mongoose optimization algorithm with a DL based ID (AMOA-DLID) technique in IoT helped UAV network. In the introduced AMOA-DLID method, AMOA is first employed for the process of FS. The next sparse AE (SAE) method could be used for intrusion identifications. At last, the SAE method recognition rate could be enhanced by using the Harris Hawks optimization (HHO) method. **Ramachandran** *et al.* [12] development and design of an efficient security methods. An improved principal component analysis (IPCA) method is utilized to mine the important features from the normalizing datasets. Later, a hybrid grasshopper crow search optimizer (GSCSO) is used to select the significant features for testing and training processes. At last, an isolated heuristic neural networks

(IHNNs) method is employed to forecast the flow of data is intrusive or normal. **Arthi** *et al.* [13] target to improve intellectual Software Defined Networks (SDNs) to enable protected structures for IoT healthcare systems. This method presents a hybrid of DL and ML methods (DNN + SVM) to detect network intrusion in the sensor based health care data. Additionally, this method could effectively monitor suspicious behaviors and connected devices. At last, the technique assesses the performances of the presented method by utilizing several metrics performances based on the scenarios of healthcare applications.

Alsubaei *et al.* [14] propose a new DL method, the ResNeXt technique, and embedding Gated Recurrent Unit (GRU) method (RNT). The systematized method contains SMOTE for handling data inequality throughout the early processing of data. This method's discriminatory ability is enhanced, especially in the process of feature extractions. The ensemble method of feature extraction exhibits critical data patterns. Fundamental to our AI classification is the RNT method, optimization by utilizing hyper-parameters over the Jaya optimizer technique (RNT-J). **Almuqren** *et al.* [15] introduce an Explainable AI Enabled Intrusion Detection Method for Secure Cyber Physical Systems (XAIID-SCPSs). The presented XAIID-SCPS method mostly focuses on the classification and ID in the CPS platforms. A Hybrid Enhanced Glowworm Swarm Optimizer (HEGSO) method has been used for FS. For ID, the Enhanced Elman Neural Networks (IENNs) method has been employed with an Enhanced Fruit Fly Optimizer (EFFO) method for the optimization of parameters. In addition, the developed method incorporates the XAI method LIME for understanding and better perceptive of the Blackbox technique for the intrusions of precise classifications.

3. Proposed Methodology

In this article, we focus on the design of CSOXAI-PDC technique on CPS. The projected CSOXAI-PDC method emphasizes the effectual classification and recognition of phishing based on CPS. To attain this, the CSOXAI-PDC technique involved data normalization, classification using DQN, CSO based fine-tuning of hyperparameter, and LIME. Fig. 1 shows the workflow of CSOXAI-PDC technique.

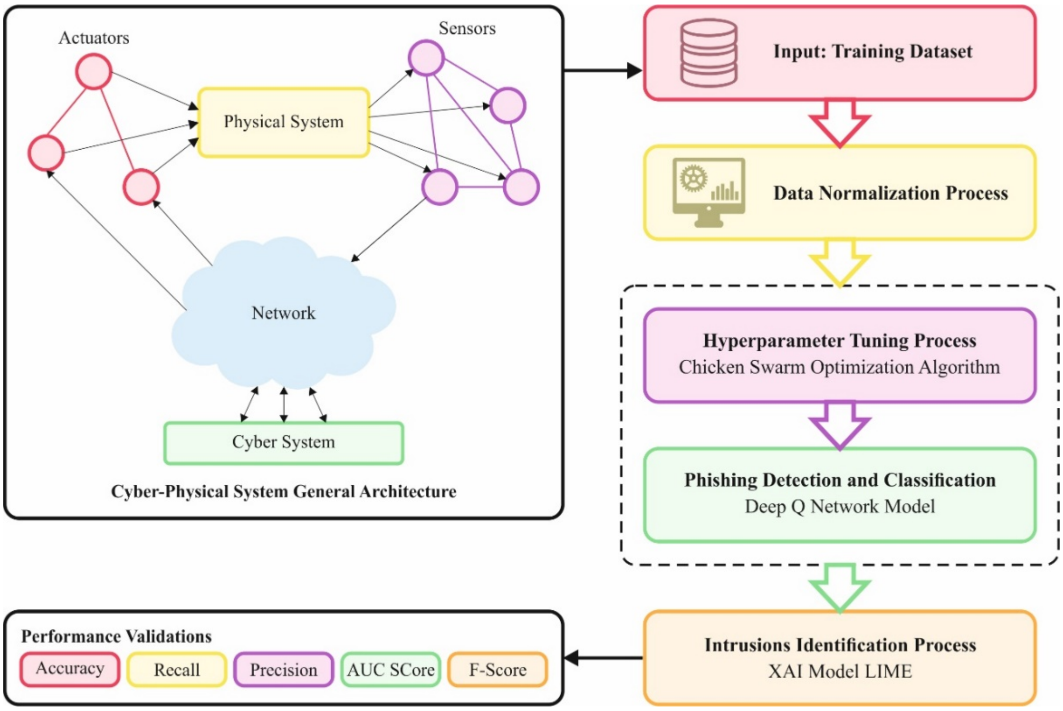

Actuators
Sensors
Physical System
Network
Cyber System
Cyber-Physical System General Architecture
Input: Training Dataset
Data Normalization Process
Hyperparameter Tuning Process
Chicken Swarm Optimization Algorithm
Phishing Detection and Classification
Deep Q Network Model
Intrusions Identification Process
XAI Model LIME
Performance Validations
Accuracy
Recall
Precision
AUC SCore
F-Score

Figure 1: Overall flow of CSOXAI-PDC technique

3.1. Data Normalization

Primarily, the CSOXAI-PDC technique executes data normalization method. Z-score normalization is a critical data pre-processing approach for phishing recognition, as it converts a value of features within a standard scale using a standard deviation of 1 and mean of 0 [16]. These methodologies underline differences from the mean to make it simple to identify abnormalities symbolic of phishing challenges. Through Z-score normalization, data standardization improves the reliability and precision of machine learning (ML) methods to detect phishing attacks.

3.2. DQN Classifier

Next, the classification of phishing recognition occurs by utilizing the DQN classifier. To diminish the cost of computational related to the iterative procedure, neural networks are used to estimate the value function of state-action [17]. Firstly, the upgrade function of 0-learning can be stated as:

$$Q(s,a) \leftarrow Q(s,a) + \alpha \left[r + \gamma \max_{a'} Q(s^{I}, a^{I}) - Q(s,a) \right] \tag{1}$$

A fluctuating rate of learning α within the interval [0,1] is employed to balance the importance of the present environment's learning experience against previous ones. Where, s' and a' denotes the state and action numbers in the following process. The Deep Q-Network (DQN) incorporates neural network methods with Q-learning and was presented to estimate the action- value function in higher-dimensional state space.

$$Q(s,a|\theta) \approx Q(s,a) \tag{2}$$

In Q-Learning, only neural networks and a target Q network are employed, DQN includes experience replay in training. The stochastic gradient descent (SGD) technique is used to upgrade the parameters of network in the training procedure. The DQN loss function is stated below:

$$L(\theta) = E[(targetQ - Q(s, a|\theta))^2] \tag{3}$$

The optimization objective for the state-action function is expressed below:

$$targetQ = r + \gamma \max_{a'} Q(s', a'|\theta) \tag{4}$$

Here, θ signifies a parameter of neural network, the policy gradient model is a model-free technique intended to enhance the predictable total return of a tactic, discovering the optimum tactic directly in the strategy space. The greedy policy picks the action, which boosts the function of value on every occasion. Conversely, action and state values that were not tested earlier will not be selected afterward because they are not assessed. The ε-greedy policy integrates the advantages of exploitation and exploration. Actions are selected stochastically from every obtainable action with a probability of ε, whereas the finest action is nominated with a probability of $1 - \varepsilon$.

3.3. Parameter Selection

For enhancing the classification performance of DQN classifier, the hyperparameter tuning method can be done using the CSO algorithm. The nature of chickens creates them a special type of poultry animal, and often they manage their food-searching efforts in clusters [18]. Hens, chicks, and roosters are three different classes of chicken flocks. According to different foraging capacities, there is a foraging hierarchal order in the group. Hens forage after roosters owing to their less foraging abilities, whereas chicks follow the lead because they have inferior foraging abilities. The chicken population shows that the chicks are arranged around the hen, the rooster occupies the center of population, and the hens are positioned around the rooster. Accordingly, there is competition among similar individual species, namely hens and hens, roosters and roosters, or among members of diverse species, namely hens and chicks, through the foraging process. For instance, hen groups H_1, H_2 forage around rooster R_2 and acquire the foraging pattern of rooster R_2 that define the foraging direction of hens H_1, H_2. Simultaneously, as hen H_2 is closer to the rooster R_1, the foraging patterns of rooster R_1 affects hen H_2 towards a certain range. Chicks C_4, C_5 and C_6 will forage around hen H_2, which learn foraging patterns, and hen H_2 define the foraging direction of chicks C_4, C_5 and C_6. The CSO algorithm was inspired by self-organizing evolution of intelligence and the coexistence of learning.

The objective function that requires an optimum solution is the optimizer object, and its variables are composed of nj-dimensional vector space X, where n is the number and j is the dimensionality, and n represents positive integer. The fitness value f differentiates the chick, rooster, and hen flocks. The chick group C_i is allocated to the CN individual with the high fitness values; the rooster group R_i is allocated to the RN individual with the lower fitness values; and, the residual HN individuals are allocated to the hen cluster H_j. RN, HN and CN denotes the rooster, hen, and chick groups, respectively.

$$R_j = \{R_1, R_2, \dots, R_{RN}\} \tag{5}$$

$$c_i = \{C_1, C_2, \dots, C_{CN}\} \tag{6}$$

$$H_i = \{H_1, H_2, \dots, H_{HN}\} \tag{7}$$

All the chicks have an individual mother hen, and all the hens have a matching individual dominant male. The succeeding formula updates the foraging position of rooster, hen, and chick individuals:

1) Computation equation for the rooster group

$$R_{\mathrm{i,j}}^{t+} = R_{i,j}^{t}[1 + randn(0, \delta^2)] \tag{8}$$

$$\delta^2 = \begin{cases} 1, & f_i \leq f_s \\ e^{\frac{f_{s\cdot} - f_i}{|J_i| + \mathcal{E}}}, & f_i > f_s \\ s \in [1, n], & s \neq i \end{cases} \tag{9}$$

Where R^t denotes the location of the i^{th} roosters at the j^{th} dimension after t^{th} iteration, $0, \delta^2$ denotes the Gaussian distribution random value within [0,1]. The fitness value of an individual is f, and S is the random rooster index keeping the denominator from 0.

2) Computation equation for the hen group

$$H_{i,j}^{t+1} = H_{\mathrm{i,j}}^{t} + k_1 * rand * \left(R_{Hi}^{t} - M_{\mathrm{i,j}}^{t}\right) + k_2 * rand * \left(RH^t - H_{\mathrm{i,j}}^{t}\right) \tag{10}$$

$$k_1 = e\frac{f_{Hi} - f_{rHi}}{|f_{Hi}| + \varepsilon} \tag{11}$$

$$k_2 = e^{f_{RH} - f_{Hi}} \tag{12}$$

Where H^t denotes the location of i^{th} hens in the j^{th} dimension after t^{th} iterations. $rand$ denotes the random $numit_{er}$ within [0,1]. R_{Hi}^{t} shows the leader rooster location of the i^{th} hen afterward t^{th} iterations; RH^t shows the location after t^{th} iterations of the random individual chosen between the other roosters and k_1, and k_2 are the influence factors of roosters and hens. The fitness value of the i^{th} hens are indicated as f_{Hi}. f_{rHi} and f_{RH} are the fitness values of the rooster and random individuals.

3) Calculation formula for the hen group:

$$C_{i,j}^{t+1} = C_{i,j}^{t} + F * (Hi_j^t - C_{\mathrm{i,j}}^{t} \tag{13}$$

Where C_{ij}^{t} and $Hi_j^t$are the location of the i^{th} chick and hens in the j^{th} dimension after t^{th} iterations; F refers to a random integer within [0,2].

The CSO obtains a FF to achieve heightened classifier performances. It identifies a positive numeral to express the best performances of the candidate solutions. In this research, the minimization of the classifier rate of error is examined as the FF, as delivered in Eq. (14).

$$\begin{aligned} fitness(x_i) &= ClassifierErrorRate(x_i) \\ &= \frac{no.of\ misclassified\ instances}{Total\ no.of\ instances} * 100 \end{aligned} \tag{14}$$

3.4. LIME Model

Eventually, the CSOXAI-PDC method incorporates the XAI method LIME for enhanced clarification and perception of the black-box procedure for precise identification of intrusions. LIME has appeared as a dominant device in the domain of XAI, mainly for the classification of text responsibilities [19]. LIME functions by creating disturbed input data examples and spotting the changes in the predictive model. In the text classification context, LIME offers local, human-accountable descriptions for single predictions, permitting users to know how a particular decision was achieved. For example, in natural language processing (NLP) applications, LIME can emphasize the important phrases or terms in a document that are greatly subjective to the classification result. This interpretability is critical for constructing trust in the AI approach, particularly in fields where accountability and transparency are paramount namely finance or healthcare. LIME's capability for shedding light on the decision-making method of the composite approach improves its value in different applications and promotes the liable utilization of AI schemes. Its assistance with interpretability and transparency makes good a valuable device for practitioners, investigators, and stakeholders to try to find validate, and comprehend the results.

4. Experimental Results and Analysis

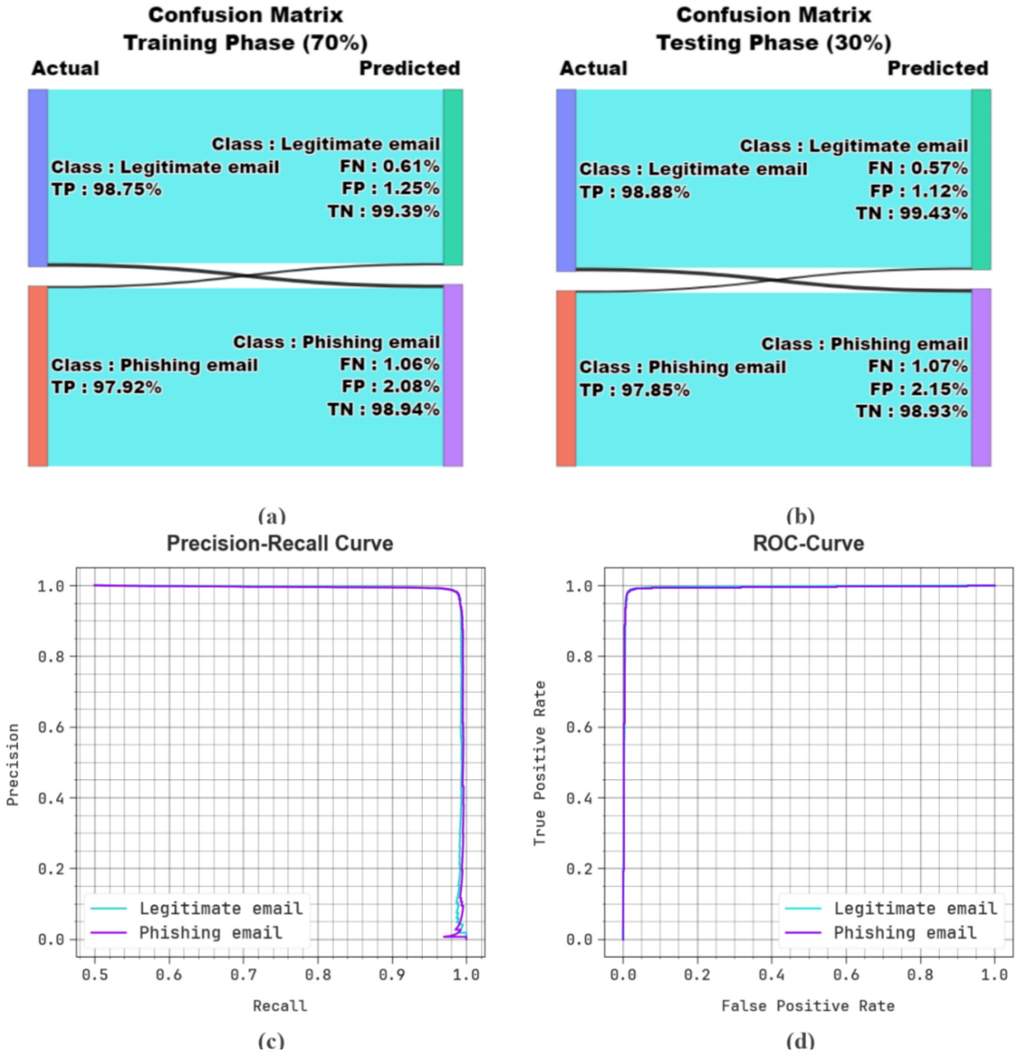
The experimental analysis of the CSOXAI-PDC technique is examined utilizing phishing emails dataset [20], which encompasses 10000 samples with two classes illustrated in Table 1.

Table 1
Details of dataset

Classes	No. of Instances
Legitimate email	5000
Phishing email	5000
Total Instances	**10000**

Fig. 2 offers the performances of the CSOXAI-PDC model under the test data. Figs. 2a-2b displays the confusion matrix with precise classification and identification of all 2 classes on a 70:30 TRAP/TESP. Fig. 2c reported the study of PR recognizing superior performance across all class labels. Finally, Fig. 2d portrayed the ROC study indicating efficient outcomes with greater values of ROC for different class labels.

The phishing detection results of the CSOXAI-PDC method are visibly portrayed in Table 2 and Fig. 3. The stimulation values gather the efficient ability of the CSOXAI-PDC approach on the recognition method. With 70%TRAP, the CSOXAI-PDC methodology achieves an average $accu_y$ of 98.33%, $prec_n$ of 98.34%, $reca_l$ of 98.33%, F_{score} of 98.33%, and AUC_{score} of 98.33%. Similarly, with 30%TESP, the CSOXAI-PDC approach acquires average $accu_y$ of 98.38%, $prec_n$ of 98.36%, $reca_l$ of 98.38%, F_{score} of 98.37%, and AUC_{score} of 98.38%.



(a)

(b)

(c)

(d)

Figure 2: Classifier outcome of (a-b) Confusion matrices and (c-d) PR and ROC curves

Table 2
Phishing detection result of CSOXAI-PDC method with 70%TRAP and 30%TESP

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	AUC_{Score}
			TRAP (70%)		
Legitimate email	97.87	98.75	97.87	98.31	98.33
Phishing email	98.78	97.92	98.78	98.35	98.33
Average	**98.33**	**98.34**	**98.33**	**98.33**	**98.33**
			TESP (30%)		

Legitimate email	97.90	98.88	97.90	98.39	98.38
Phishing email	98.85	97.85	98.85	98.35	98.38
Average	**98.38**	**98.36**	**98.38**	**98.37**	**98.38**

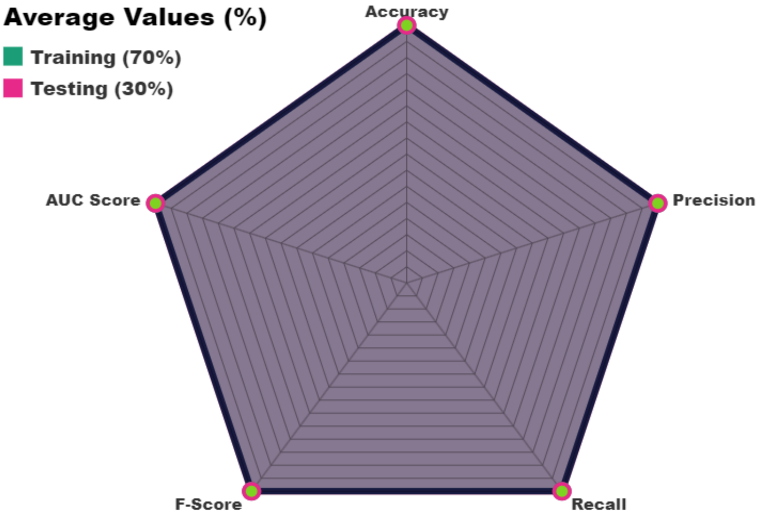


Figure 3: Average of CSOXAI-PDC technique with 70%TRAP and 30%TESP

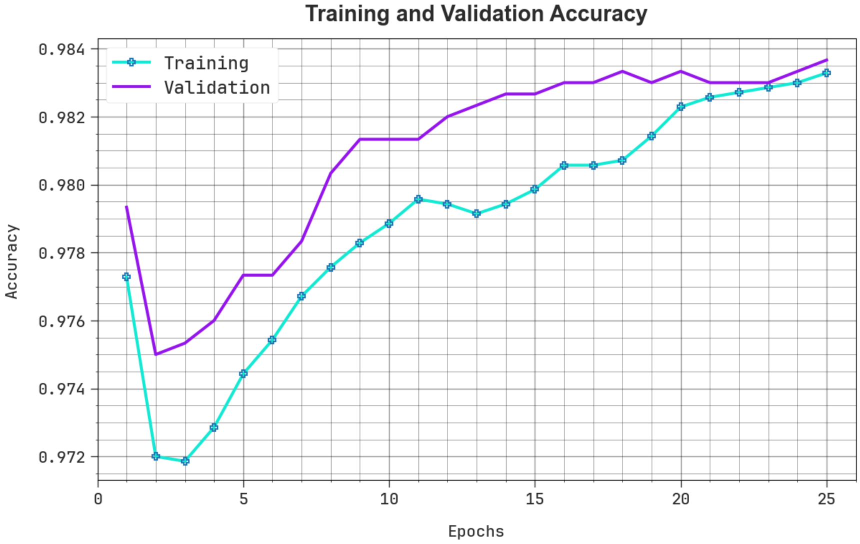


Figure 4: $Accu_y$ curve of the CSOXAI-PDC technique

In Fig. 4, the training and validation accuracy outcomes of the CSOXAI-PDC methodology can be displayed. The accuracy values are computed throughout 0-25 epoch counts. This figure underscored that the training and validation accuracy values show growing trend that informed the capacity of the CSOXAI-PDC method with better performance over numerous iterations. Furthermore, the training accuracy and validation accuracy rest nearer over the epoch counts that exhibit least minimum overfitting and display improved performance of the CSOXAI-PDC technique, ensuring continuous prediction on hidden samples.

In Fig. 5, the training and validation loss graph of the CSOXAI-PDC system was depicted. The loss values are calculated for 0-25 epoch counts. It is denoted that the training and validation accuracy values demonstrate a minimum trend that reported the capability of the CSOXAI-PDC system to balance a trade-off between generalization and data fitting. The steady decrease in loss values in addition assurances the superior performance of the CSOXAI-PDC approach and tuning the prediction outcomes in time.

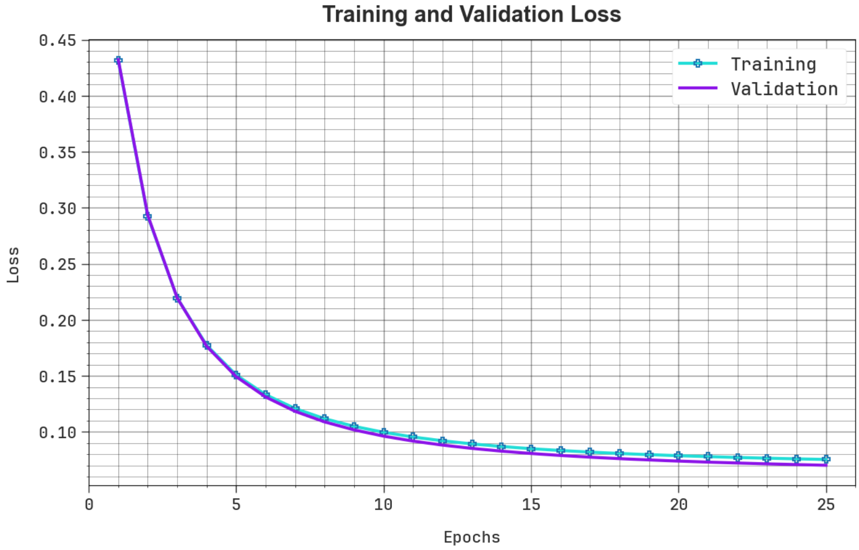


Figure 5: Loss curve of the CSOXAI-PDC technique

To demonstrate the superior performance of the CSOXAI-PDC model, a short comparative analysis can be produced in Table 3 and Fig. 6 [21]. This outcome illustrated that the LR and the decision forest technique have demonstrated least classification outcomes. In the meanwhile, SVM, the locally-deep SVM, Boosted DT, and averaged perceptron approaches have been tested to execute slightly adjacent classification results [22]. Additionally, the NN model has shown reasonable performance with $accu_y$ of 97.70%, $prec_n$ of 96.40%,$reca_l$ of 89.30%, and F_{score} of 92.70%. On the other hand, the CSOXAI-PDC model illustrates promising performance with $accu_y$ of 98.38%, $prec_n$ of 98.36%,$reca_l$ of 98.38%, and F_{score} of 98.37%.

Table 3

Comparative analysis of CSOXAI-PDC technique with recent methods

Algorithm	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
CSOXAI-PDC	98.38	98.36	98.38	98.37
Locally-deep SVM	96.80	90.00	90.60	90.30
SVM Classifier	97.40	95.00	89.30	92.00
Boosted DT	97.20	93.10	89.90	91.50
Logistic Regression	95.60	95.00	77.20	85.20
Averaged Perceptron	97.70	94.40	91.30	92.80
Neural Network	97.70	96.40	89.30	92.70
Decision Forest	95.30	95.00	75.80	84.30

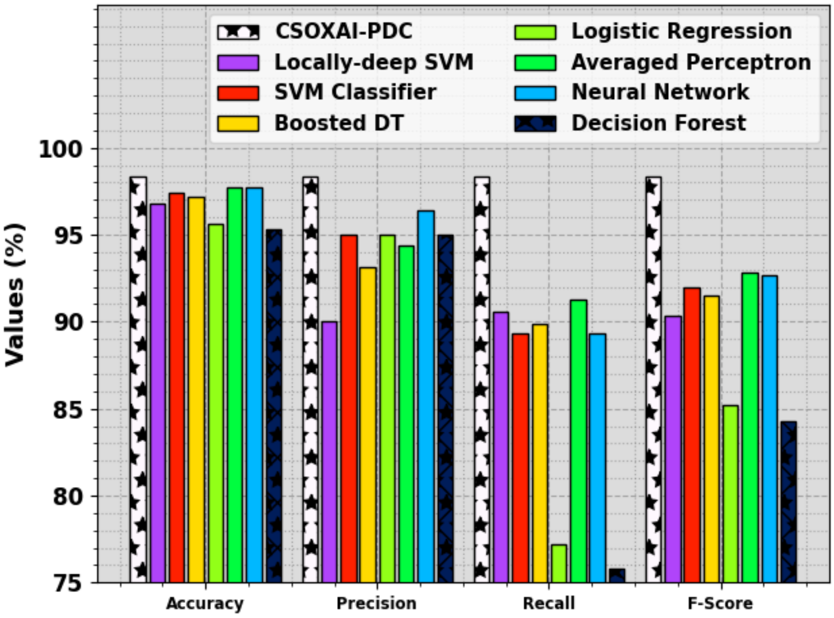


Figure 6: Comparative analysis of CSOXAI-PDC technique with recent methods

5. Conclusion

In this study, we focus on the design of CSOXAI-PDC technique on CPS. The projected CSOXAI-PDC method emphasizes the effectual classification and recognition of phishing based on CPS. To attain this, the CSOXAI-PDC technique first executes data normalization method. Next, the classification of phishing recognition occurs by utilizing DQN classifier. For enhancing the classification performance of DQN classifier, the hyperparameter tuning method can be done using the CSO algorithm. Eventually, the CSOXAI-PDC method incorporates the XAI method LIME for superior clarification and perception of the black-box procedure for accurate identification of intrusions. The experimental analysis of the CSOXAI-PDC algorithm is executed against real dataset and the results establish the improvement of the projected method over recent techniques.

References

[1] C. B. Monteiro, R. P. França, R. Arthur, Y. Iano, A Look at Machine Learning in the Modern Age of Sustainable Future Secured Smart Cities, in Data-Driven Mining, Learning and Analytics for Secured Smart Cities, Cham: Springer, (2021) 359-383.

[2] P.A. Barraclough, G. Fehringer, J. Woodward, Intelligent cyber-phishing detection for online, Computers & Security, 104, (2021) 102123.

[3] O. Balogun, N. O. Akande, F. E. Usman-Hamza, V. E. Adeyemo, M. A. Mabayoje, A. O. Ameen, Rotation Forest-Based Logistic Model Tree for Website Phishing Detection, in Proc. International Conference on Computational Science and Its Applications, Cham, Springer, (2021) 154-169

[4] A. Singh, A. Tiwari, A study of feature selection and dimensionality reduction methods for classification-based phishing detection system, International Journal of Information Retrieval Research (IJIRR), 11.1, (2021) 1-35.

[5] R. Salama, M. Ragab, Blockchain with Explainable Artificial Intelligence Driven Intrusion Detection for Clustered IoT Driven Ubiquitous Computing System, Computer Systems Science & Engineering, 46.3 (2023) 2917-2932.

[6] M. Ragab, M.F. S. Sabir, Outlier detection with optimal hybrid deep learning enabled intrusion detection system for ubiquitous and smart environment, Sustainable Energy Technologies and Assessments, 52 (2022) 102311.

[7] M.A. Ahad, S. Paiva, G. Tripathi, N. Feroz, Enabling technologies and sustainable smart cities, Sustainable cities and society, 61 102301, 2020.

[8] Y.A. Aina, Achieving smart sustainable cities with GeoICT support: The Saudi evolving smart cities, Cities, 71, (2017) 49-58.

[9] E. Gandotra, D. Gupta, An efficient approach for phishing detection using machine learning, in Multimedia Security, Singapore: Springer, (2021) 239-253.

[10] N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, H. Fujita, Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions, in IEEE Access, 10, (2022) 36429-36463.

[11] L. Yang, J. Zhang, X. Wang, Z. Li, Z. Li, Y. He, An improved ELM-based and data preprocessing integrated approach for phishing detection considering comprehensive features, Expert Systems with Applications, 165, (2021) 113863.

[12] S. S. Alotaibi, A. Sayed, E. Samir Abd Elhameed, O. Alghushairy, M. Assiri, S. Saadeldeen Ibrahim, Enhancing Security in IoT-Assisted UAV Networks Using Adaptive Mongoose Optimization Algorithm With Deep Learning, in IEEE Access, 12, (2024) 63768-63776.

[13] D. Ramachandran, M. Albathan, A. Hussain, Q. Abbas, Enhancing cloud-based security: a novel approach for efficient cyber-threat detection using GSCSO-IHNN model, Systems, 11.10, (2023) 518.

[14] R. Arthi, S. Krishnaveni, S. Zeadally, An intelligent SDN-IoT enabled intrusion detection system for healthcare systems using a hybrid deep learning and machine learning approach, China Communications., (2024).

[15] F. S. Alsubaei, A. A. Almazroi, N. Ayub, Enhancing Phishing Detection: A Novel Hybrid Deep Learning Framework for Cybercrime Forensics, in IEEE Access, 12, (2024) 8373-8389.

[16] 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, Applied Sciences, 13.5, (2023) 3081.

[17] H.A. Prihanditya, The implementation of z-score normalizatio, boosting techniques to increase accuracy of c4, 5 algorithm in diagnosing chronic kidney disease. Journal of Soft Computing Exploration, 1.1, (2020) 63-69.

[18] R. BOUMEGOURA, Y. ZENNIR, S.F. TAMINE, Deep Q-Learning-Based Trajectory Optimization for Vehicle Navigation in CARLA, Algerian Journal of Signals and Systems, 9.2, (2024) 128-133.

[19] Chen, L. Cao, C. Chen, Y. Chen, Y. Yue, A comprehensive survey on the chicken swarm optimization algorithm and its applications: state-of-the-art and research challenges, Artificial Intelligence Review, 57.7, (2024) 170.

[20] T. Aljrees, Improving Prediction of Arabic Fake News Using ELMO's Features-Based Tri-Ensemble Model and LIME XAI, in IEEE Access,12, (2024) 63066-63076.

[21] https://www.kaggle.com/datasets/subhajournal/phishingemails

[22] A. Mughaid, S. AlZu'bi, A. Hnaif, S. Taamneh, A. Alnajjar, E.A. Elsoud, An intelligent cyber security phishing detection system using deep learning techniques, Cluster Computing, 25.6, (2022) 3819-3828.

[23] M. Ragab, Hybrid firefly particle swarm optimisation algorithm for feature selection problems, Expert Systems, 41.7(2024) e13363.