UtilitasMathematica

ISSN 0315-3681 Volume 122, 2025

Phishing Attack Detection Method Based on Deep Learning and Metaheuristic Pelican Optimization Algorithms

Satyajit Mahapatra[1], Yeshpal Singh[2], Akshay Juneja[3], Biswakalpa Patra[4], Supreet Kaur[5], Ajay Kumar[6*]

[1]School of Computer Science and Engineering, Odisha University of Technology and Research Odisha, India. mahapatra.satyajit62@gmail.com

[2]Department of Computer Science, Government Polytechnic, ROORKEE, BAHERI, BAREILLY, UP India. softwareknowler33@gmail.com

[3]Computer Science and Engineering, College of Smart Computing, COER University, Roorkee, Uttarakhand. akshay.j1207@gmail.com

[4]Department of Electronics & Communication Engineering Department, Mizoram University, Mizoram, India. mzu2001346@mzu.edu.in

[5]Department of Computer Engineering & Technology, GNDU, Amritsar, India. er.supreet.k@gmail.com

[6*]Department of Artificial Intelligence, Ajay Research Academy, Patiala, India. ajay.researchacademy@gmail.com

Abstract: In the cyberattacks, the phishing attack is the most harmful way used by attackers to steal the sensitive information of the individual or organizations. This attack is often accomplished through clicking or opening attachments through emails, website URLs, and social media. In the previous studies, the traditional approaches, namely, blacklisting, website content, and URL features, were employed for phishing attack detection. However, these approaches are slow and fail to detect the new phishing attacks. Thus, the machine learning (ML) algorithms are employed to overcome the previous issues. In this paper, we have designed a phishing attack detection method based on ML that efficiently detects the phishing attack by analyzing the website URLs data. Initially, the optimal feature selection from the data is done by combining the metaheuristic pelican optimization (PO) algorithm with artificial neural networks (ANN). After that, a lightweight Convolutional Neural Network (CNN) is employed to detect the legitimate and malicious website URLs. Furthermore, by dividing the standard dataset into various training and testing ratios, the suggested approach can be tested on those data. The result indicates that the proposed method effectively detects the phishing attack and outperforms the previous methods by achieving an average accuracy value of 0.9995.

Keywords: ANN, Attacks, CNN, Deep Learning, Metaheuristic, Optimization, Phishing.

1. Introduction

The cybercrime is performed by the attackers to steal the sensitive information of the personal individual and businesses. The most stolen sensitive information includes credentials for a person's financial accounts and identification [1]. In the literature, several types of cyberattacks, namely, phishing, spoofing, malware, DoS, SQL injection, and social engineering [2]. Out of these attacks, we have focused on phishing attacks in this paper. In this attack, the attacker employs the email/website address to claim it is from the reputable and recognizable company to steal the personal information of the people [3]. The email/website links are provided through emails and social media.

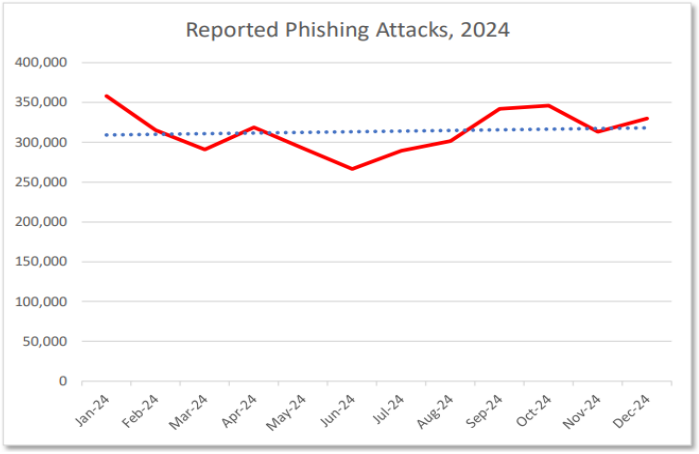

Figure 1. Reported Phishing Attacks by APWG [3]

Furthermore, in the literature, APWG reports are evaluated to determine the trends of phishing attacks. It tracks unique phishing websites, email subjects, and the number of brands under attack. According to the recent report of 2024, the total number of phishing attacks for the different months is shown in Figure 1 [4]. The graph indicates that the phishing attack lies between 290,000 and 358,000 per month. Therefore, an efficient phishing attack detection method is required to overcome this attack. In the present scenario, machine learning and its sub-field deep learning algorithms have gained popularity over the traditional approaches (blacklisting, website content, and their features) that were utilized earlier to detect the new phishing attack by analyzing the different features of the dataset [5]. In these algorithms, the ML/DL model is trained with legitimate and malicious website URLs. Based on the website URLs' characteristics, the ML/DL is efficiently learned and gains enough information to predict the new phishing attack [6-8]. Therefore, the main motive of this paper is to design a phishing attack detection method based on deep learning that effectively detects the phishing attack by analyzing the optimal features of the dataset. This paper's key contribution is presented below.

1. We have designed an approach for optimal feature selection from the dataset using the metaheuristic PO and ANN algorithm based on the accuracy parameter.
2. We have proposed a lightweight CNN algorithm for phishing attack detection by train the model using the optimal features.
3. We have achieved the testing average accuracy value of 0.9995, precision value of 1.0000, recall value of 0.9989, and F1-score value of 0.9995 for the proposed phishing attack detection method for different training and testing ratios.

The remaining paper is organized into five sections. Section 2 discusses previous phishing attack detection research. Section 3 defines the preliminaries in which algorithms are explain which employed for the proposed method. Section 4 explains the proposed phishing attack detection method. The proposed method's results and findings are presented in Section 5. Section 6 serves as the paper's conclusion.

2. Related Work

In the previous studies, several traditional techniques, namely, blacklisting/whitelisting, visual similarity, third-party, search engine, URL feature, and website content, were employed to detect phishing attacks [9]. However, these techniques failed to identify the new phishing attacks and were very slow in nature. Therefore, in the present scenario, ML and its subfield, DL algorithms, are employed to distinguish between the legitimate and malicious URLs in order to overcome phishing attacks [10]. Furthermore, in the literature, there are two ways employed for phishing attacks. The first one is email-based, whereas the second one is based on a website URL. In this paper, we have focused on ML-based phishing attack detection methods based on website URLs [11]. AK Dutta [12] employed the RNN and LSTM algorithms to classify the malicious and legitimate website URLs on two datasets, namely, Phishtank and Crawler. They have achieved approximately similar accuracy (97.4% value for Phishtank and 96.8% value for Crawler) in both datasets. However, in their work, the feature selection was not done, and the training/testing ratio was not

defined. Lohar et al. [13] collected the phishing attack data from the various sources, namely, Phishtank, OpenPhish, and domain. After that, I performed the feature extraction and applied several ML algorithms: RF, DT, XGBoost, LR, and SVC to detect phishing attacks on free web hosting domains. The result indicates that the RF algorithm achieves the highest detection accuracy value of 97.7%. However, their approach is complex due to utilizing a number of ML algorithms, and performance depends on the complexity of the dataset. Shombot et al. [14] presented an SVM algorithm-based phishing attack detection method based on two kernels, radial basis and polynomial. However, in their work, a limited dataset (805 data entries) was considered. Ghalechyan et al. [15] employed the two architectures, BERT and a probabilistic-based neural network, for phishing attack detection on the website URLs. In their work, several datasets are taken into consideration, such as Phishtank, OpenPhish, Alexa, and private, and split into an 80:20 ratio. Their results indicate that they have achieved an accuracy of 97%. Further, NN, RF, and SVM algorithms are employed for phishing attack detection by Mohamad et al. [16]. In their work, three datasets (Alexa, Siri, and Phishtank) are taken into consideration. After that, feature extraction from the dataset is done, and the dataset into a 70:30 ratio. The result indicates that NN achieves the highest accuracy value of 95.18%. Aldakheel et al. [17] employed the CNN algorithm on the PhishTank dataset for phishing attack detection purposes. In the CNN, they have seven layers and achieved an accuracy of 98.77%. Y. Wei and Y. Sekiya [18] designed an ensemble learning approach for phishing attack detection. In their work, AdaBoost, GBDT, LightGBM, HGB, and RF approaches are used. The results indicate that RF achieves the highest accuracy of 96.94% and the lowest accuracy value of 93.53% by AdaBoost. Like the previous approach, Karim et al. [19] designed an ensemble learning approach by taking the three algorithms, LR, SVM, and DT, and used the hard and soft voting for the final prediction. Besides that, in their work, the canopy and grid search method are employed for feature selection purposes and achieves a 98.12% accuracy value.

In the previous studies, the feature selection was done either manually or conventional grid search approach to train and test the ML/DL algorithm, which negatively impacted the detection accuracy in the output due to not selecting the optimal features. In addition, several ML and DL algorithms are used for phishing attack detection without optimizing the layers of it. Therefore, in this paper, these research challenges are taken into consideration, and a phishing attack detection method is proposed in which optimal features are selected from the dataset by utilizing the metaheuristic PO and ANN algorithms. Further, in the proposed method, we have designed a lightweight CNN for phishing attack detection purposes.

3. Preliminaries

The proposed method employs the ANN, CNN, and metaheuristic PO algorithms to construct a phishing attack detection method. Therefore, this section presents an overview of these algorithms.

3.1 ANN

An ANN is a mathematical approach that works similarly to the human brain [20]. A supervised method, an ANN learns from training data and then compares incoming data to a target sample. The hidden layer modifies the weight matrix by passing the error value if there is an output error. Figure 2 depicts the ANN's overall structure, and a description of it is provided below [21-22].

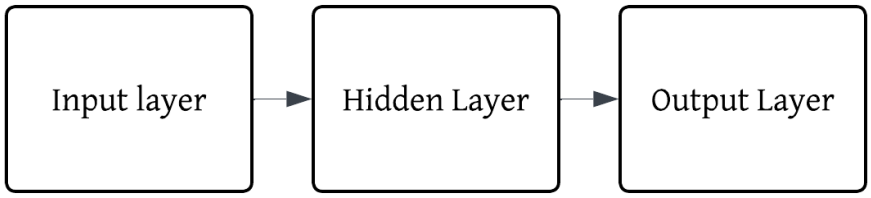

Figure 2. Structure of ANN [20]

- **Input Layer:** The responsibility of this layer to receive the raw input data. The input data's characteristics are represented by the neurons in this layer.
- **Hidden Layer:** "Hidden layers" refer to the levels that exist between the "input" and "output" layers. The majority of the network's computations are performed by them. Both the quantity and size of these hidden layers could change depending on how complicated the overall task is. After each hidden layer applies its own biases and weights to the input data, non-linearity is introduced using an activation function.
- **Output Layer: It generates the predicted output. Each layer has a certain number of neurons, equal to the number of classes in a classification problem.**

3.2 CNN

A CNN algorithm comes under neural networks and is utilized in several applications for classification purposes. Therefore, in this research, CNN is employed for phishing attack detection purposes. To accomplish this goal, the CNN algorithm needs to train with a large amount of labeled data during training [23]. In the CNN, the main layers are input, convolution, max-pooling, and fully connected layer, as shown in Figure 3. Below is a description of these layers [24-25].

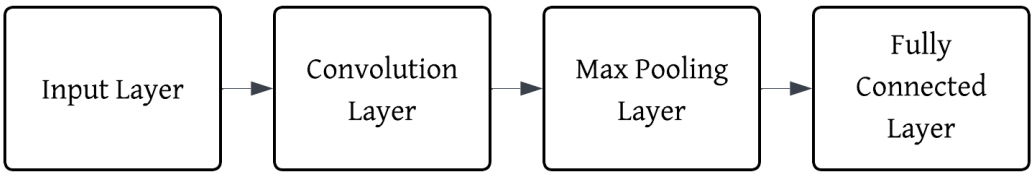

Figure 3. Main Layers of CNN [24]

- **Input Layer:** In this layer, the dataset is given with optimal features, and this layer converts the data into a matrix for processing in the upcoming layers.
- **Convolution layer:** After that, the convolution layer receives the input layer matrix and uses it to extract robust characteristics that may be used to identify a phishing website. Convolutional filters are used to gather such characteristics.
- **Pooling:** After the convolution layer output passes through a max pooling layer, it selects the highest feature value in the feature map. The pool is two-dimensional. This layer greatly decreases output vectors, resulting in a reduced output matrix.
- **Fully Connected:** By passing the maximum pooled output matrix through a flattening layer, the two-dimensional feature map is reduced to a one-dimensional representation. After that, we'll feed the form into a Fully Connected (FC) layer. This layer will analyze the input and output neurons to decide if the website is phishing or not.

3.3 Metaheuristic PO Algorithm

This section presents the metaheuristic PO algorithm employed for optimal feature selection from the dataset based on the objective function. The main principle of the PO algorithm is based on the hunting behavior of the pelicans. The pelican birds dive in the water to catch fish from a certain height and spread their wings on the water surface to force the fish to go into the shallow water, and this process helps them to catch the fish. These characteristics are studied by researchers, and they have designed an exploration (moving towards prey) and exploitation (spreading the wings) phase to search for the optimal solution [26]. The metaheuristic PO algorithm searches for the optimal solution similar to previously metaheuristic algorithms, such as defining the population, evaluating the population based on the objective function, and determining the optimal solution. After that, new populations are explored by utilizing the exploration and exploitation phases of the PO algorithm to determine the best solution. In the literature, the PO algorithm is successfully used in energy dispatch [27], energy management [28], facial emotion recognition [29], wind turbine fault classification [30], and trajectory planning [31].

4. Proposed Phishing Attack Detection Method

This section presents the proposed phishing attack detection method, which efficiently detects the website phishing URL. The main novelty of the proposed method is that optimal features from the dataset are determined to enhance the detection. Besides that, we have designed a lightweight CNN algorithm to reduce the method's complexity. The block diagram of the proposed phishing attack detection method is shown in Figure 4.

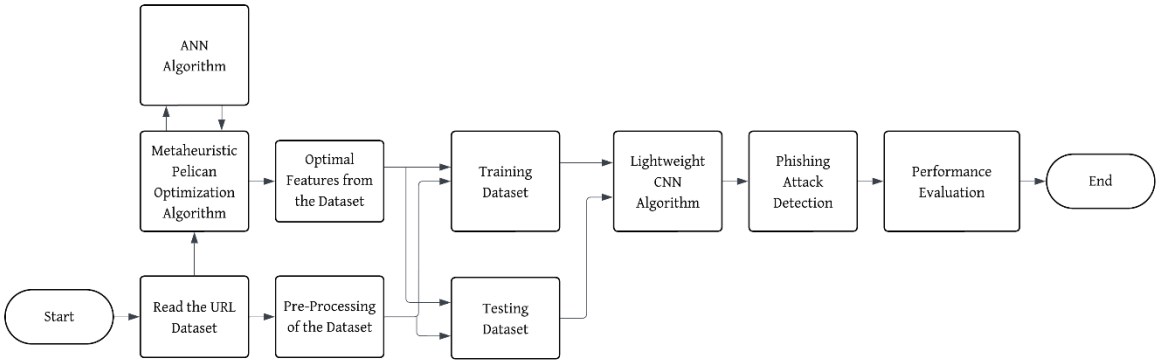

Figure 4. Block Diagram of the Proposed Method

- **Standard Dataset:** The standard dataset of Phishing is employed in the proposed method [32]. This dataset contains legitimate and malicious website URLs and various features of it. In this study, 10,000 data values are considered, and it contains the 50 attributes that represent the various information of the URLs. Furthermore, this dataset is available in *.csv* format.
- **Pre-Processing the Dataset:** In this step, the dataset is pre-processed to check the missing or null value. Followed by separating the input and output attributes for the ML algorithm.
- **Feature Selection using Metaheuristic PO and ANN Algorithm:** In this step, the dataset along with the input parameters (such as population and its dimension, iteration, and objective function) of metaheuristic PO is initialized. After that, a random population is generated to select the features from the dataset and evaluated based on the objective function. In the objective function, the ANN algorithm is trained and tested based on the selected features by utilizing the feedforward network. Furthermore, ten cross-fold validations are considered. Finally, in the objective function, Eq. (1) is employed to evaluate the ANN algorithm, and its value is minimized in the proposed method. Further, metaheuristic PO algorithms generate the new population by performing the various operations and evaluate the objective function to determine which population gives the superior results over others. This process is iterated for a fixed number of iterations.

$$OF = 1 - Accuracy \quad \textbf{(1)}$$

- **Splitting the Dataset:** Here, we validate the suggested method's performance by splitting the website URL dataset into training and testing ratios. Three different ratios—70:30, 60:40, and 80:20—are used in this paper. In addition, the ideal features of the test and training datasets are determined in the preceding stage.
- **Phishing Attack Detection using the Lightweight CNN Algorithm:** In this step, a lightweight CNN algorithm is designed for phishing attack detection purposes. To accomplish this goal, the training and testing dataset is given to the lightweight CNN algorithm along with layers and training options. In a lightweight CNN, the layers considered in the proposed method are input, convolution, max-pooling, and the fully connected layer. On the other hand, the training options considered for the proposed method are the Adam optimizer, maximum epochs, and batch size. Based on this information, the lightweight CNN algorithm detects the phishing attack. Finally, based on the detection value, the performance evaluation of the proposed method with the actual value is done.
- **Performance Evaluation:** In this section, the different parameters are defined that are considered to evaluate the suggested method. Initially, the confusion matrix is evaluated for the proposed method,

and based on other parameters such as accuracy (A), precision (P), recall (R), and F1-score, it is derived [33-35]. We calculate these parameters using Eq. (2-5).

$$A = \frac{TP+TN}{TP+TN+FP+FN} \quad (2)$$

$$P = \frac{TP}{TP+FP} \quad (3)$$

$$R = \frac{TP}{TP+FN} \quad (4)$$

$$F1 - Score = 2 * \frac{P \times R}{P+R} \quad (5)$$

We use Equation (2) to gauge the overall effectiveness of the proposed method in distinguishing between legitimate and malicious website URLs. Furthermore, Equations (3-4) are utilized to determine how correctly the proposed method identifies the phishing attack. A high value of these equations indicates that the false identification is minimal. Finally, Eq. (5) is used to check the balance between the precision and recall parameters. A high value of this equation indicates that both parameters are balanced. Furthermore, we have evaluated the performance of the metaheuristic PO algorithm based on the convergence rate graph. This graph is drawn in between fitness function vs. iteration. This graph reflects how many iterations the metaheuristic PO algorithm takes to achieve the desired objective function.

5. Results and Discussion

This section presents the simulation results of the proposed phishing attack detection method and a comparative analysis with the existing methods. The proposed method was designed and simulated in MATLAB 2018a software. Furthermore, a large amount of data was considered for evaluation using deep learning and metaheuristic algorithms. A high-end system with an Intel i7 processor running at 2.70 GHz, 64-bit Windows, and 8 GB of RAM was therefore taken into consideration. Table 1 shows the simulation setup configuration of the ANN, CNN, and metaheuristic PO algorithms used for the proposed method. Initially, in this table, the training and testing ratios are considered and defined. Followed by that, the parameter values of the ANN, CNN, and metaheuristic PO algorithms are defined.

Table 1. Simulation Setup Configuration

Parameter	**Value**
Training and Testing Ratio	60:40, 70:30, 80:20
ANN	
Cross-Fold Validation	10
Network	Feed-Forward
CNN	
Input Data	[8,8]
Filter Size and Number of Filters	[5,20]
Max Pooling Size	[2,2]
Activation Function	'Softmax'
Metaheuristic PO	
Population	[10]
Iteration	50
Lower and Upper Limit of the Parameter	[0-1]

For various testing and training ratios that were considered for the suggested strategy, the confusion matrix is displayed in Table 2-4. For various ratios, the results indicate that the suggested method defines true positive and negative situations quite well, outperforming false positives and negatives. This evidence demonstrates that the suggested strategy effectively uses features to differentiate between legitimate and malicious websites.

Table 2. Confusion Matrix for Proposed Method for 60:40 Ratio

		Predicted Value	
		Positive	Negative
Actual Value	Positive	2008	0
	Negative	1	1991

Table 3. Confusion Matrix for Proposed Method for 70:30 Ratio

		Predicted Value	
		Positive	Negative
Actual Value	Positive	1495	0
	Negative	1	1504

Table 4. Confusion Matrix for Proposed Method for 80:20 Ratio

		Predicted Value	
		Positive	Negative
Actual Value	Positive	1006	0
	Negative	2	992

Furthermore, we calculate the other parameters (accuracy, precision, recall, and F-score) based on the confusion matrix to demonstrate the effectiveness of the proposed method. The result indicates that the proposed method achieves the accuracy value in the range of 0.9990-0.9998, precision value in the range of 1.000, recall value in the range of 0.9980-0.9995, and F1-score value in the range of 0.9990-0.9997 for different training and testing ratios. This evidence indicates that the proposed method is efficient in detecting the phishing attack for the dataset.

Table 5. Performance Evaluation of the Proposed Phishing Attack Detection Method

Parameter	**Training and Testing Ratio**	**Accuracy**	**Precision**	**Recall**	**F1-Score**
Proposed Method	60:40	0.9998	1.0000	0.9995	0.9997
Proposed Method	70:30	0.9997	1.0000	0.9993	0.9997
Proposed Method	80:20	0.9990	1.0000	0.9980	0.9990
	Average	0.9995	1.0000	0.9989	0.9995

Table 6 shows the comparative analysis of the presented method with the previous phishing attack detection method based on the accuracy parameter. The result indicates that the presented method achieves the highest average accuracy value of 99.95% over the previous approaches, such as AK. Dutta [4], Lohar et al. [5], Ghalechyan et al. [7], and Aldakheel et al. [9] achieved the accuracy values of 97.4%, 97.7%, 97%, and 98.77%, respectively, due to training the lightweight CNN algorithm with the optimal feature selection using the metaheuristic PO and ANN algorithms.

Table 6. Comparative Analysis

Methods	**AK Dutta [10]**	**Lohar et al. [11]**	**Ghalechyan et al. [13]**	**Aldakheel et al. [15]**	**Proposed Method**
Accuracy	97.4%	97.7%	97%	98.77%	**99.95%**

Finally, Figures 5-7 show the convergence rate graph for the metaheuristic PO algorithm for different training and testing ratios. The result indicates that in between 23 and 49 iterations, the PO algorithm achieves its desired objective function.

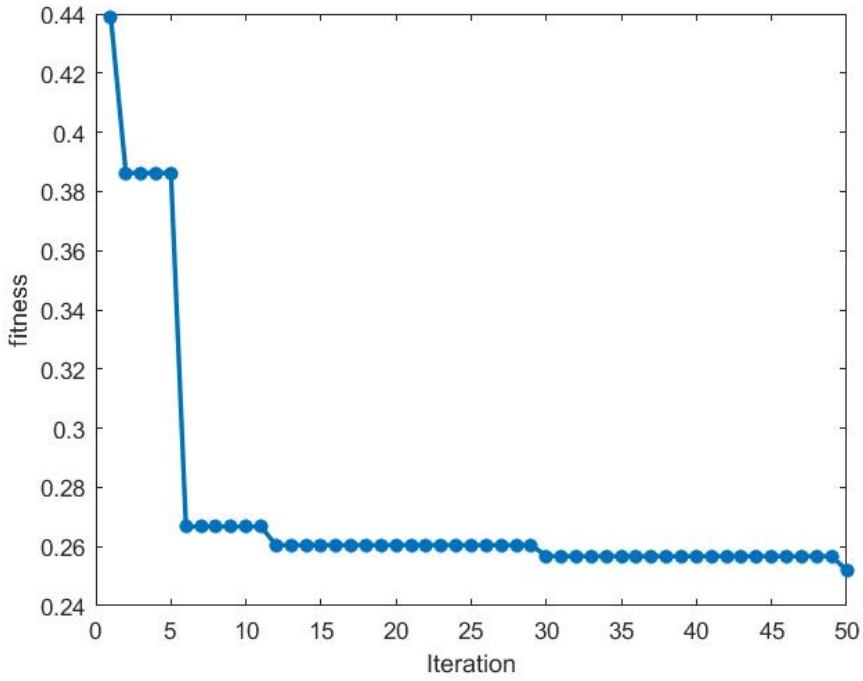

Figure 5. Convergence Rate Graph of Metaheuristic PO Algorithm for 60:40 Ratio

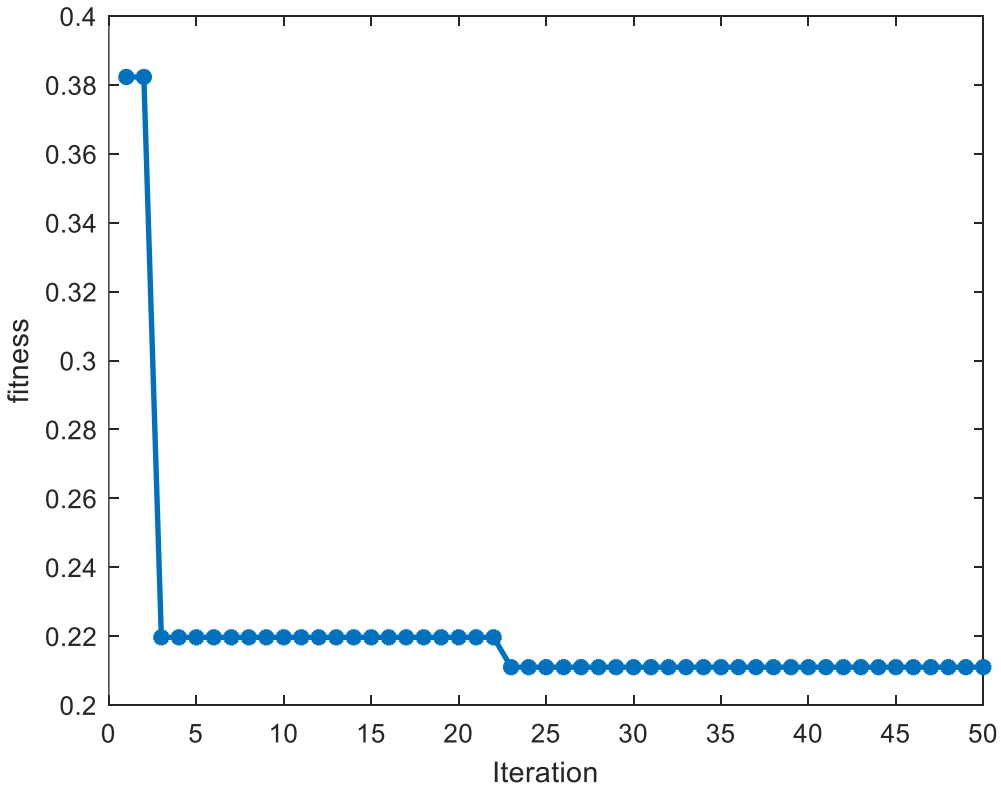

Figure 6. Convergence Rate Graph of Metaheuristic PO Algorithm for 70:30 Ratio

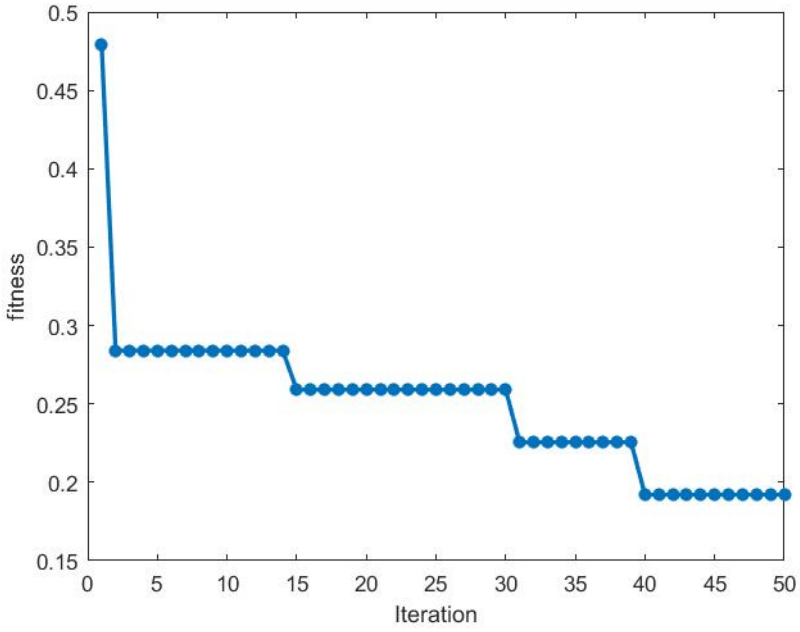

Figure 7. Convergence Rate Graph of Metaheuristic PO Algorithm for 80:20 Ratio

6. Conclusion

In this paper, we have presented a phishing attack detection method by utilizing deep learning and metaheuristic algorithms, namely, ANN, CNN, and PO. The main contribution of the presented method is that the PO and ANN algorithms are employed for optimal feature selection from the dataset, whereas a lightweight CNN is designed for detecting the phishing attack. The simulation evaluation is performed for the standard dataset by splitting the dataset into a 70:30 ratio. The results indicate that approximately 50% of the dataset attributes are reduced due to feature selection. Furthermore, the proposed method achieves an average accuracy value of 0.9995, a precision value of 1.000, a recall value of 0.9989, and an F1-Score value of 0.9995, respectively. Finally, the comparative analysis based on the accuracy and F1 score shows that the proposed method achieves the highest value of these parameters over the existing methods.

References

[1] Duy, P. T., Minh, V. Q., Dang, B. T. H., Son, N. D. H., Quyen, N. H., & Pham, V. H. (2024). A study on adversarial sample resistance and Defense Mechanism for Multimodal Learning-based phishing website detection. *IEEE Access*.

[2] Sadiq, A., Anwar, M., Butt, R. A., Masud, F., Shahzad, M. K., Naseem, S., & Younas, M. (2021). A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. *Human behavior and emerging technologies*, *3*(5), 854-864.

[3] Siddiqui, N., Chaudhary, L., Tripathi, P., Kumar, N., & Kumar, S. (2022). A comparative analysis of us and Indian laws against phishing attacks. *Materials Today: Proceedings*, *49*, 3646-3649.

[4] APWG. (2024). *APWG | Phishing Activity Trends Reports*. Apwg.org. https://apwg.org/trendsreports/

[5] Kapan, S., & Sora Gunal, E. (2023). Improved phishing attack detection with machine learning: A comprehensive evaluation of classifiers and features. *Applied Sciences*, *13*(24), 13269.

[6] Mosa, D. T., Shams, M. Y., Abohany, A. A., El-kenawy, E. S. M., & Thabet, M. (2023). Machine learning techniques for detecting phishing URL attacks. *Computers, Materials and Continua*, *75*(1), 1271-1290.

[7] Do, N. Q., Selamat, A., Krejcar, O., Herrera-Viedma, E., & Fujita, H. (2022). Deep learning for phishing detection: Taxonomy, current challenges and future directions. *Ieee Access*, *10*, 36429-36463.

[8] Catal, C., Giray, G., Tekinerdogan, B., Kumar, S., & Shukla, S. (2022). Applications of deep learning for phishing detection: a systematic literature review. *Knowledge and Information Systems*, *64*(6), 1457-1500.

[9] Shukla, S., Misra, M., & Varshney, G. (2024). HTTP header based phishing attack detection using machine learning. *Transactions on Emerging Telecommunications Technologies*, *35*(1), e4872.

[10] Jupin, J. A., Sutikno, T., Ismail, M. A., Mohamad, M. S., Kasim, S., & Stiawan, D. (2019). Review of the machine learning methods in the classification of phishing attack. *Bulletin of Electrical Engineering and Informatics*, *8*(4), 1545-1555.

[11] Benavides, E., Fuertes, W., Sanchez, S., & Sanchez, M. (2019). Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review. *Developments and Advances in Defense and Security: Proceedings of MICRADS 2019*, 51-64.

[12] Dutta, A. K. (2021). Detecting phishing websites using machine learning technique. *PloS one*, *16*(10), e0258361.

[13] Lohar, R., Tripathi, M., & Shirazi, H. (2025). Free-Phish: detecting phishing websites hosted on free web hosting domains. *International Journal of Computers and Applications*, 1-7.

[14] Shombot, E. S., Dusserre, G., Bestak, R., & Ahmed, N. B. (2024). An application for predicting phishing attacks: A case of implementing a support vector machine learning model. *Cyber Security and Applications*, *2*, 100036.

[15] Ghalechyan, H., Israyelyan, E., Arakelyan, A., Hovhannisyan, G., & Davtyan, A. (2024). Phishing URL detection with neural networks: an empirical study. *Scientific Reports*, *14*(1), 25134.

[16] Mohamed, G., Visumathi, J., Mahdal, M., Anand, J., & Elangovan, M. (2022). An effective and secure mechanism for phishing attacks using a machine learning approach. *Processes*, *10*(7), 1356.

[17] Aldakheel, E. A., Zakariah, M., Gashgari, G. A., Almarshad, F. A., & Alzahrani, A. I. (2023). A deep learning-based innovative technique for phishing detection in modern security with uniform resource locators. *Sensors*, *23*(9), 4403.

[18] Wei, Y., & Sekiya, Y. (2022). Sufficiency of ensemble machine learning methods for phishing websites detection. *IEEE Access*, *10*, 124103-124113.

[19] Karim, A., Shahroz, M., Mustofa, K., Belhaouari, S. B., & Joga, S. R. K. (2023). Phishing detection system through hybrid machine learning based on URL. *IEEE Access*, *11*, 36805-36822.

[20] Kajal, A., & Nandal, S. K. (2020). A hybrid approach for cyber security: improved intrusion detection system using Ann-Svm. *Indian Journal of Computer Science and Engineering*, *11*(4), 325-412.

[21] GeeksforGeeks. (2024, July 19). *Layers in Artificial Neural Networks (ANN)*. GeeksforGeeks; GeeksforGeeks. https://www.geeksforgeeks.org/layers-in-artificial-neural-networks-ann/

[22] Mridha, K., Hasan, J., & Ghosh, A. (2021, September). Phishing URL classification analysis using ANN algorithm. In *2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON)* (pp. 1-7). IEEE.

[23] Alshingiti, Z., Alaqel, R., Al-Muhtadi, J., Haq, Q. E. U., Saleem, K., & Faheem, M. H. (2023). A deep learning-based phishing detection system using CNN, LSTM, and LSTM-CNN. *Electronics*, *12*(1), 232.

[24] Alotaibi, R., Al-Turaiki, I., & Alakeel, F. (2020, March). Mitigating email phishing attacks using convolutional neural networks. In *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-6). IEEE.

[25] Gupta, B. B., Gaurav, A., Attar, R. W., Arya, V., Bansal, S., Alhomoud, A., & Chui, K. T. (2024). A Hybrid CNN-Brown-Bear Optimization Framework for Enhanced Detection of URL Phishing Attacks. *Computers, Materials & Continua*, *81*(3).

[26] Trojovský, P., & Dehghani, M. (2022). Pelican optimization algorithm: A novel nature-inspired algorithm for engineering applications. *Sensors*, *22*(3), 855.

[27] SeyedGarmroudi, S., Kayakutlu, G., Kayalica, M. O., & Çolak, Ü. (2024). Improved Pelican optimization algorithm for solving load dispatch problems. *Energy*, *289*, 129811.

[28] Alamir, N., Kamel, S., Megahed, T. F., Hori, M., & Abdelkader, S. M. (2023). Developing hybrid demand response technique for energy management in microgrid based on pelican optimization algorithm. *Electric Power Systems Research*, *214*, 108905.

[29] Alonazi, M., Alshahrani, H. J., Alotaibi, F. A., Maray, M., Alghamdi, M., & Sayed, A. (2023). Automated facial emotion recognition using the pelican optimization algorithm with a deep convolutional neural network. *Electronics*, *12*(22), 4608.

[30] Tuerxun, W., Xu, C., Haderbieke, M., Guo, L., & Cheng, Z. (2022). A wind turbine fault classification model using broad learning system optimized by improved pelican optimization algorithm. *Machines*, *10*(5), 407.

[31] Khaleel, R. Z., Khaleel, H. Z., Abdullah Al-Hareeri, A. A., Mahdi Al-Obaidi, A. S., & Humaidi, A. J. (2024). Improved Trajectory Planning of Mobile Robot Based on Pelican Optimization Algorithm. *Journal Européen des Systèmes Automatisés*, *57*(4).

[32] Sundari, S. G. (2023, October 13). *Phishing Website Detection by Machine Learning Techniques*. GitHub. https://github.com/shreyagopal/Phishing-Website-Detection-by-Machine-Learning-Techniques

[33] Li, W., Laghari, S. U. A., Manickam, S., Chong, Y. W., & Li, B. (2024). Machine Learning-Enabled Attacks on Anti-Phishing Blacklists. *IEEE Access*.

[34] Bahaghighat, M., Ghasemi, M., & Ozen, F. (2023). A high-accuracy phishing website detection method based on machine learning. *Journal of Information Security and Applications*, *77*, 103553.

[35] Divakaran, D. M., & Oest, A. (2022). Phishing detection leveraging machine learning and deep learning: A review. *IEEE Security & Privacy*, *20*(5), 86-95.