Journal of Theoretical and Applied Information Technology

31st December 2023. Vol.101. No 24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MANTA RAY FORAGING OPTIMIZATION ALGORITHM WITH DEEP LEARNING ASSISTED AUTOMATED PHISHING URL DETECTION MODEL

K SUBASHINI[1], DR. V NARMATHA[2]

[1]Research Scholar, Department of Computer and Information Science, Annamalai University, Tamil Nadu, India

[2]Assistant Professor, Department of Computer and Information Science, Annamalai University, Tamil Nadu, India

E-mail: [1]subaphdscholar@gmail.com , [2]balaji.narmatha8@gmail.com

ABSTRACT

In current scenario, phishing attacks are vital threats to cyberspace security. Phishing is one of the common types of scams that attract individuals to access mischievous URLs (Uniform Resource Locators) as well as their personal data like IDs, passwords, and others. Many intelligent attacks have been launched to cheat users by retrieving a trustworthy website or any online platform in order to get data. Phishing URL classification is one of the crucial cybersecurity tasks intended to classify and moderate malevolent web addresses considered to cheat consumers by revealing sensitive data. Numerous researchers in cyberspace are interested in generating intelligent techniques as well as offering security services on a phishing website that grows more clever and malicious daily. Therefore, this study introduces a manta ray foraging optimization with deep learning-based phishing website detection (MRFODL-PWD) technique. The major intention of the MRFODL-PWD technique is to recognize and classify the presence of legitimate or phishing URLs. In the presented MRFODL-PWD technique, several stages of pre-processing to transfer data into a useful setup, and BERT is applied for feature extraction. Moreover, deep belief network (DBN) model can be used for automated phishing URL detection. Furthermore, the MRFO algorithm selects the hyperparameter values of the DBN model. An extensive comparison study stated that the MRFODL-PWD technique accomplishes enhanced phishing URL detection results over other models.

Keywords: *Phishing Attacks; Cybersecurity; Deep Learning; Parameter Tuning; Manta Ray Foraging Optimization*

1. INTRODUCTION

Phishing attacks are one of the important anxiety due to high growth. It is a commonly utilized, destructive, and effective attack that attackers attempt to trick consumers into revealing personal data like their credit card and password information [1]. A usual phishing attack model includes website phishing, where attacker traps consumers from accessing fake webpages by duplicating the names and looks of legitimate webpages like Amazon, eBay, and Facebook [2]. It is highly complex for normal one to differentiate phishing from usual because websites of phishing seem like normal websites they copy [3]. In most cases, consumers will not check out their whole website URL when they visit a website, so attackers easily grab personal as well as sensitive data [4]. Recently, numerous anti-phishing methodologies have been developed in order to recognize phishing dangers at an initial stage and protect users from such kinds of attacks. Security techniques based on deep learning (DL) devices are used more often in many industries to struggle to develop phishing attacks [5].

Machine learning (ML) and deep learning (DL) are rapid growth of intelligent models that descend under artificial intelligence (AI) and are useful in offering safety for cybersecurity and computing management [6]. The diversity of AI features accessible from identifying and concluding patterns for providing security in order to familiarize with a novel atmosphere [7].

Therefore it plays a vital part in technical systems like cybersecurity and computer vision. Human knowledge is required for performing feature extraction and selection in ML models. Feature selection and detection tasks are divided [8]. To improve performance of model, DL is employed as a single part for classification and detection. DL techniques reduce the requirement for physical feature engineering as well as confidence in third-party services due to automatic learning and feature removable when compared to the ML model [9]. However, DL has major benefits such as high performance and end-to-end problem solving over ML models. These benefits are more useful in huge datasets like image classification, speech recognition, and phishing detection particularly [10].

This study introduces a manta ray foraging optimization with DL-based phishing website detection (MRFODL-PWD) technique. The major intention of the MRFODL-PWD technique is to recognize and classify the presence of legitimate or phishing URLs. In the presented MRFODL-PWD technique, several stages of pre-processing to transfer data into useful setup and BERT is applied for feature extraction. Moreover, deep belief network (DBN) model can be used for automated phishing URL detection. Furthermore, the MRFO algorithm selects the hyperparameter values of the DBN model. An extensive comparison study stated that the MRFODL-PWD technique accomplishes enhanced phishing URL detection results over other models.

2. RELATED WORKS

In [11], an effective Hybrid Deep Learning (HDL)-centric Phishing Detection System (PDS) employing an MCS-DNN classification algorithm has been proposed. The feature selection (FS) and clustering are executed by utilizing CM-WOA as well as CoK-means consistently. The features that are preferred during the process FS are fed into MCS-DNN classification algorithm that sorts webpages of genuine and phishing. At last, K-fold cross-validations (KCV) are used for prediction purposes. Yang et al. [12] developed a combined phishing website classification model that depends on random forest (RF) as well as convolutional neural networks (CNNs). This developed method employs character embedding model to transform URLs into fixed-size conditions, remove features at various stages employing CNNs methods, and classify multi-level features employing many RF classification algorithms. At last, output estimate results utilizing a winner-take-all technique.

Zhu et al. [13] designed a trivial technique that integrates CNNs, bi-directional long short-term memory (BiLSTM), and an attention mechanism for phishing recognition. This developed method also called BiLSTM and char-convolutional with attention mechanism (CCBLA) technique, uses deep learning (DL) in order to remove features automatically from target URLs. The method employs attention mechanism to load the significance of selected features. In [14], a method based on hybrid deep neural networks (DNNs) has been developed in order to identify phishing scam accounts such as LBPS (LSTM-FCN and BPNN-based Phishing Scam accounts classification method) and validate its efficiency on Ethereum. LBPS techniques produce new techniques for examining transaction accounts through approving BPNN for attaining hidden relationships among features extracted from LSTM-FCN neural networks and transaction records.

Elsadig et al. [15] developed a new URL phishing classification model based on BERT feature removal as well as DL model. First, the natural language processing (NLP) model is employed. Next, a deep CNN model was used for identifying URLs of phishing. It was mainly utilized to establish words or n-grams to remove greater features. Then, information is categorized into genuine and phishing URLs. For evaluation, the dataset of public phishing website URLs is utilized. Benavides-Astudillo et al. [16] designed a technique employing DL as well as Natural Language Processing (NLP) methods. The model utilized Keras Embedding Layer with Global Vectors for Word Representation (GloVe)

approaches. Initially, this method executed a study employing Word Embedding and NLP. Next, this information is presented in the DL method. The study estimated four other techniques such as Gated Recurrent Unit (GRU), BiLSTM, BiGRU, and LSTM.

3. THE PROPOSED MODEL

In this study, we have focused on the design and development of automated phishing URL detection using the MRFODL-PWD model. The major intention of the MRFODL-PWD technique is to recognize and classify the presence of legitimate or phishing URLs. It follows a series of subprocesses namely data preprocessing, BERT feature extraction, DBN classification, and MRFO-based hyperparameter tuning. Figure 1 depicts the workflow of MRFODL-PWD approach.

3.1 Data Pre-processing

Preprocessing is an important step in the context of phishing URL detection, which includes cleaning and collecting data of legitimate and phishing URLs, extracting and parsing pertinent features from the URL, normalizing them, accurately labelling them, and converting the data into a mathematical representation. Then, this preprocessed information train ML models, effectively distinguish between legitimate and phishing URLs, which can contribute towards better cybersecurity measures.

3.2 BERT Feature Extraction

The bi-directional encoder representation from the transformer (BERT) is a recent language model representation. BERT was applied to natural language processing (NLP) facilitating extraction of

features. NLP is a field of computer science with ability of machinery to understand spoken words and text in related modes that humans can do. In NLP, computation linguistics—rule-based human language modelling—is incorporated with DL, ML, and statistical models. The NLP model is used for exclusive data columns and extracts considerable amount of relevant data features. The BERT is used for negating pretrained deep bi-directional representation from unclassed text via mutual training on bidirectional right and left contexts in each layer. The pretrained BERT model is finetuned with the addition of output layer to produce various models for in-depth analysis namely NLP task. The BERT could enhance the unidirectional restriction. Thus, BERT succeeds in learning context embedding for words.

The training of DBN includes iterative training of layer-wise RBM. The VL as input trains the initial RBM, and its HL activation becomes the VL for following RBM. This procedure continues until each RBM is trained. This layer-wise pretraining assists in fixing a problem that occurs when the system is originally established by arbitrary, untrained connection weight. The unit within a similar layer does not have direct connection to each other; however, the reconstruction and construction processes are facilitated by interconnection of these layers. A mass of visible entities $(v_1, v_2, \dots v_i)$ make up network's observable layer (v), which is trained on unlabelled design structure fed into it, and a massive amount of hidden entities$(h_1, h_2, \dots h_j)$. The hidden node in network has binary values, receives data from visible node, and is capable of

constructing the pattern (h).

$$R(v,h) = \sum_{i\epsilon vis} \frac{(v_i - b_i)^2}{2\lambda_i^2} - \sum_{j\epsilon hid} a_j h_j - \sum_{ij} \frac{v_i}{\lambda_i} h_j S_{ij} \qquad (1)$$

where the dispersal of Gaussian noise at i^{th} dimension is λ.

The learning approach becomes a challenge if the concealed and exposed states are Gaussian. The standard deviation of the noise level is used for calculating the coefficient of the quadratic "containment" term that keeps the activity within realistic boundaries.

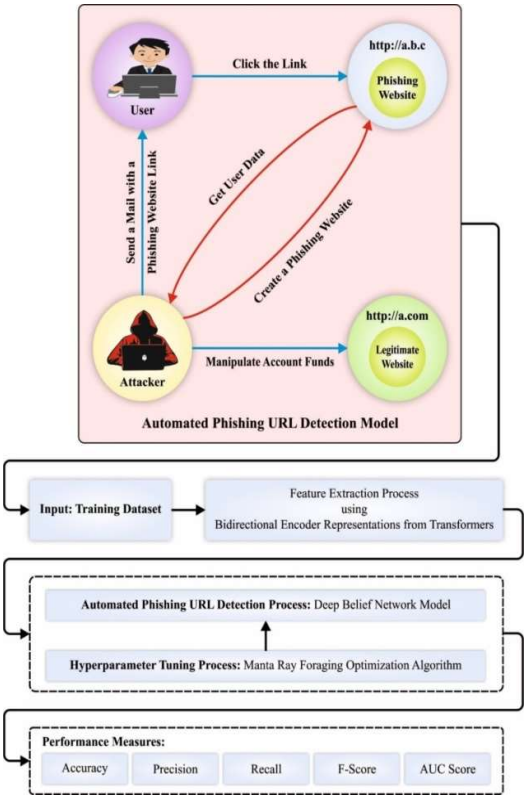


Figure 1: Workflow of MRFODL-PWD algorithm

$$R(v,h) = \sum_{i \epsilon vis} \frac{(v_i - b_i)^2}{2\lambda_i^2} + \sum_{j \epsilon hid} \frac{(h_j - a_j)^2}{2\lambda_i^2} - \sum_{ij} \frac{v_i h_j}{\lambda_i \lambda_j} S_{ij} \quad (2)$$

The training set data was used to guess the probability of concealed units and to graphically characterize the prediction.

$$M(h_j = 1) = l\left(a_j + \sum v_i w_{ij}\right) \quad (3)$$

With sample of$h$, we could recreate the unseen parameter v ' at observable level. Then, we gather new series of h' hidden activations.

$$M(v_i = 1) = l\left(b_i + \sum h_j s_{ij}\right) \quad (4)$$

The results of multiplying v' by h' from outside is important to these solutions.

$$\Delta Sij = \eta((v_i \bullet hj)_{data} - (v_i' \bullet h'j)_{model}) \quad (5)$$

where η is assumed as learner speed. Make the modifications to b_i and h_j in Eqs. (6) & (7), and the logistic activation function is represented as $(\bullet)$

$$b = b + l(v - v') \quad (6)$$

$$a = a + l(h - h') \quad (7)$$

$$\emptyset(x) = \frac{1}{1 + e^{-x}} \quad (8)$$

Finally, a logistic activation function is defined as well as demonstrated and utilized in all the nodes of processing (8). It takes an input value (x) and exploits logistic conversion to squash output within [0, 1]. Figure 2 illustrates the architecture of DBN.

3.3 Hyperparameter Tuning using MRFO Algorithm

At last, the MRFO algorithm adjusts the hyperparameter values of the DBN model. The MRFO approach originates from the performance of MRs while catching the prey [18]. The MRFO algorithm was applied to resolve different problems of the optimization algorithm which applies three fundamental foraging tactics such as chain foraging, cyclone foraging, and somersault foraging.

By moving one after another, MR forms a head-to-tail chain and starts foraging in this strategy. Except for the first individual, other MRs move towards the food and the nearby MR for cooperation. The mathematical equation of chain foraging is formulated by Eq. (9):

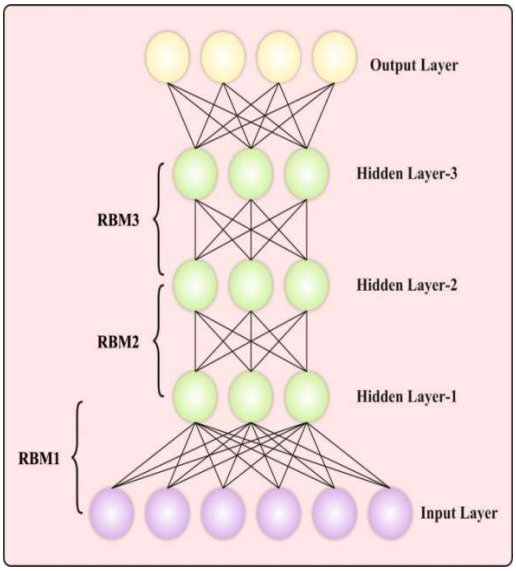


Figure 2: DBN architecture

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$p_i^{t+1} = \begin{cases} p_i^t + r.(p_{Best} - p_i^t) + \alpha.(p_{Best} - p_i^t), i = 1 \\ p_i^t + r.(p_{i-1}^t - p_i^t) + \alpha.(p_{Best} - p_i^t), \quad i = 2, \dots, N \end{cases} \quad (9)$$

$$\alpha = 2.r.\sqrt{\log(r)} \quad (10)$$

In the equation, p_i^t represents the i^{th} individual location at t^{th} iterations. A random vector in the range $[0,1]$ is r. A weight coefficient is α. The best location obtained is p_{Best}.

Cyclone foraging strategy is described by the spiral movement of MRs towards the food and the individual in front of it. In the following equation, it can be mathematically given as follows:

$$p_i^{t+1} = \begin{cases} p_i^t + r.(p_{Best} - p_i^t) + \beta.(p_{Best} - p_i^t), i = 1 \\ p_i^t + r.(p_{i-1}^t - p_i^t) + \beta.(p_{Best} - p_i^t), \quad i = 2, \dots, N \end{cases} \quad (11)$$

$$p_{rand} = Lb + r.(Ub - Lb) \quad (12)$$

$$p_i^{t+1} = \begin{cases} p_i^t + r.(p_{rand} - p_i^t) + \beta.(p_{rand} - p_i^t), i = 1 \\ p_i^t + r.(p_{i-1}^t - p_i^t) + \beta.(p_{rand} - p_i^t), \quad i = 2, \dots, N \end{cases} \quad (13)$$

$$\beta = 2.e^{\left(r_1 \frac{T-t+1}{T}\right)}.\sin(2.\pi.r1) \quad (14)$$

Here, p_{rand} is a random location in the space enclosed by the lower and upper boundaries Lb and Ub correspondingly. β represents the weight coefficient. r_1 is a random integer ranging from $[0,1]$. The maximum number of iterations is T.

In somersault foragning strategy, the food location is represented as a pivot. The MRs swim to and fro around the food and somersault towards a novel location. These behaviors are formulated by Eq. (15):

$$p_i^{t+1} = p_i^t + S.(r_2.p_{Best} - r_3.p_i^t), i = 1, \dots, N. \quad (15)$$

Here, the somersault factor set as 2 is represented as S. The random number ranges from zero to one and is denoted by $r2$ and $r3$.

The fitness selection is a major factor influencing the performance of the MRFO method. The hyperparameter selection process encompasses the solution encoding approach to estimate the efficiency of candidate solutions.

Algorithm 1: The Pseudocode of MRFO Algorithm

Initialize MRFO parameters: Maximal amount of iterations T, Population' size N, Dimension Dim, α, δ, and so on.

Initialize the population of MRFO: $X_i(i = 1,2, \dots, N)$

Compute the fitness value $f(X)$

Define the better location X_{best}

While $(t < T)$ do

For $i = 1,2, \dots N$ do

If $rand < 0.5$ then

If $\left(\frac{t}{T}\right) < rand$ then

$X_{rand} = Lb + rand.(Ub - Lb)$

Update the location $X_i(t + 1)$ based on the Eq. (13)

Else

Update the location $X_i(t + 1)$ based on the Eq. (11)

End if

Else

Update the location $X_i(t + 1)$ based on the Eq. (9)

End if

Compute the fitness value $f(X_i(t + 1))$

Update the optimum location X_{best}

Update the location $X_i(t + 1)$ based on Eq. (15)

Compute the fitness value $f(X_i(t + 1))$

Update the optimum location X_{best}

End for

$t = t + 1$

End while

Return to the optimum location X_{best}

In this work, the MRFO approach considers accuracy as the key criterion for designing the fitness function as follows.

$$Fitness = \max(P) \quad (16)$$

$$P = \frac{TP}{TP + FP} \quad (17)$$

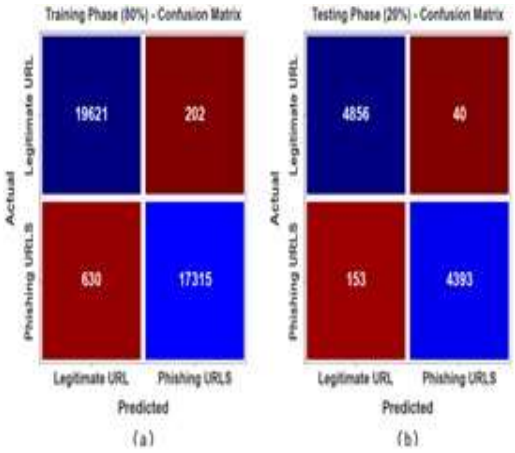
Where TP and FP are the true and the false positive values.

4 RESULTS AND DISCUSSION

In this study, the phishing URL detection results of the MRFODL-PWD system can be tested using the database [19, 20], including 47210 samples with two classes as defined in Table 1.

Table 1: Details of Datasets

Class	No. of Samples
Legitimate URL	24719
Phishing URLS	22491
Total Samples	**47210**



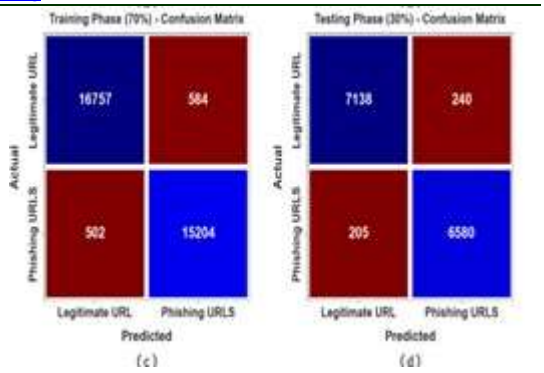


Figure 3: Confusion matrices of (a-c) TR phase of 80% and 70% and (b-d) TS phase of 20% and 30%

Figure 3 illustrates the confusion matrices produced by the MRFODL-PWD technique under 80:20 and 70:30 of TR phase/TS phase. The obtained value indicates the effectual recognition of legitimate and phishing URL samples with all two classes.

In Table 2 and Figure 4, the phishing detection analysis of the MRFODL-PWD system at 80:20 of TR Phase/TS Phase is reported. The results clarified that the MRFODL-PWD technique recognized legitimate and phishing URLs proficiently. On 80% of TR Phase, the MRFODL-PWD system provides an average $accu_y$ of 97.80%, $prec_n$ of 97.87%, $reca_l$ of 97.74%, F_{score} of 97.79%, and AUC_{score} value of 97.74%. Additionally, with 20% of TS Phase, the MRFODL-PWD methodology gives an average $accu_y$ of 97.96%, $prec_n$ of 98.02%, $reca_l$ of 97.91%, F_{score} of 97.95%, and AUC_{score} value of 97.91%.

Table 2: Phishing detection outcome of MRFODL-PWD system with 80:20 of TR phase/TS phase

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
TR Phase (80%)					
Legitimate URL	97.80	96.89	98.98	97.92	97.74
Phishing URLS	97.80	98.85	96.49	97.65	97.74
Average	**97.80**	**97.87**	**97.74**	**97.79**	**97.74**
TS Phase (20%)					
Legitimate URL	97.96	96.95	99.18	98.05	97.91
Phishing URLS	97.96	99.10	96.63	97.85	97.91
Average	**97.96**	**98.02**	**97.91**	**97.95**	**97.91**

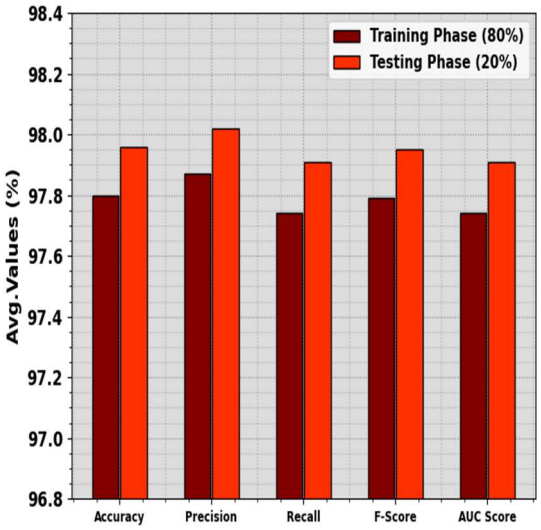


Figure 4: Average of MRFODL-PWD approach with 80:20 of TR phase/TS phase

In Table 3 and Fig. 5, the phishing detection analysis of the MRFODL-PWD methodology at 70:30 of TR Phase/TS Phase can be demonstrated. The accomplished outcomes pointed out that the MRFODL-PWD system recognized legitimate and phishing URLs effectively.

Table 3: Phishing detection outcome of MRFODL-PWD system with 70:30 of TR phase/TS phase

Class Labels	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
TR Phase (70%)					
Legitimate URL	96.63	97.09	96.63	96.86	96.72
Phishing URLS	96.80	96.30	96.80	96.55	96.72
Average	**96.72**	**96.70**	**96.72**	**96.71**	**96.72**
TS Phase (30%)					
Legitimate URL	96.75	97.21	96.75	96.98	96.86
Phishing URLS	96.98	96.48	96.98	96.73	96.86
Average	**96.86**	**96.84**	**96.86**	**96.85**	**96.86**

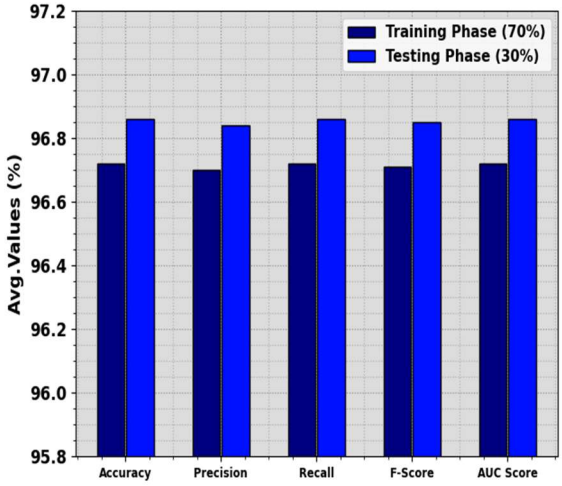


Figure 5: Average of MRFODL-PWD system with 70:30 of TR phase/TS phase

According to 70% of TR Phase, the MRFODL-PWD algorithm offers an average $accu_y$ of 96.72%, $prec_n$ of 96.70%, $reca_l$ of 96.72%, F_{score} of 96.71%, and AUC_{score} of 96.72%. Also, based on 30% of TS Phase, the MRFODL-PWD methodology provides an average $accu_y$ of 96.86%, $prec_n$ of 96.84%, $reca_l$ of 96.86%, F_{score} of 96.85, and AUC_{score} value of 96.86% respectively.

To determine the effectiveness of the MRFODL-PWD algorithm with 80:20 of TR phase/TS phase, we have produced accuracy curves for both the training (TR) and testing (TS) phases, as exhibited in Fig. 6. These curves gives valuable insights into the model's capability and learning development to generalize. As we improves the count of epochs, an observable enrichment in both TR and TS accuracy curves can be obvious. This enhancement represents the model's capacity to higher recognize patterns within both the TR and TS databases.

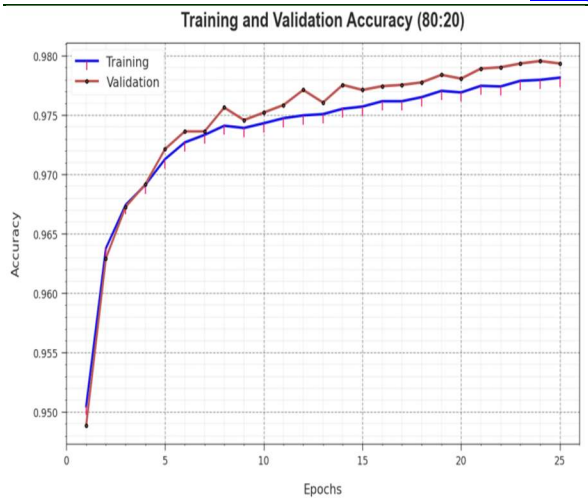


Figure 6: $Accu_y$ curve of MRFODL-PWD approach with 80:20 of TR phase/TS phase

Fig. 7 also illustrates an overview of the MRFODL-PWD methodology loss values during the training process. The diminishing trend in TR loss over epochs states that the model continuously enhances its weights to decrease predictive errors on both TR and TS data. This loss curve considers how well the model fits the training data. Especially, the TR and TS loss constantly minimalize, showing the model's efficient learning of patterns existing in both databases. Also, it exhibits the model's adaptation for reducing differences between original and the predicted training labels.

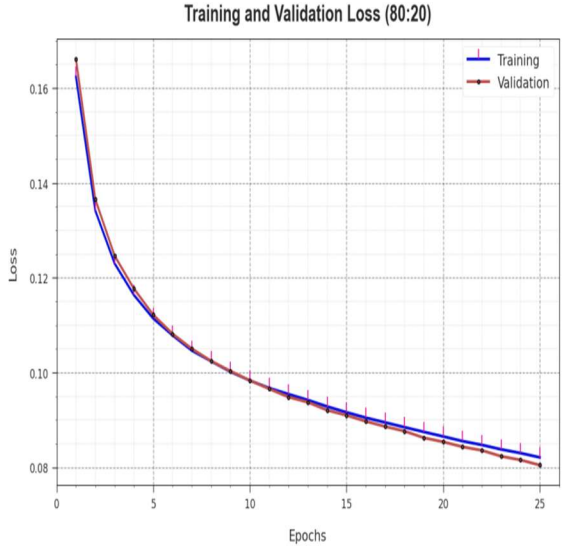


Figure 7: Loss curve of MRFODL-PWD system with 80:20 of TR phase/TS phase

Finally, a detailed comparative analysis of the MRFODL-PWD system is stated in Table 4 and Fig. 8 [15]. The results indicate that the URLNet-DLMD, Multi-layer-DNN, ML+HV+ Random Forest, Random forest, and CNN + BERT systems get worse performance. At the same time, the ML-PDURLs and DPWEFB-MLP models have shown slightly improved performance. But the MRFODL-PWD methodology exhibited maximum performance with $prec_n$ of 98.02%, $reca_l$ of 97.91%, F_{score} of 97.95%, and $accu_y$ of 97.96%. Therefore, the MRFODL-PWD algorithm can be applied for automated and accurate phishing URL detection process.

Table 4. Comparison analysis of MRFODL-PWD algorithm with other systems

Metrics	$Prec_n$	$Reca_l$	F_{score}	$Accu_y$
ML-PDURLs	97.00	97.00	97.00	97.18
DPWEFB-MLF	97.04	97.12	97.23	97.25
URLNet-DLMD	96.78	95.24	95.27	95.49
Multi-layer-DNN	95.89	96.48	96.46	95.73
ML+HV+ Random Forest	96.30	95.23	95.99	97.50
Random forest	95.48	95.17	96.70	94.50
CNN + BERT	95.71	96.80	95.21	96.66
MRFODL-PWD	98.02	97.91	97.95	97.96

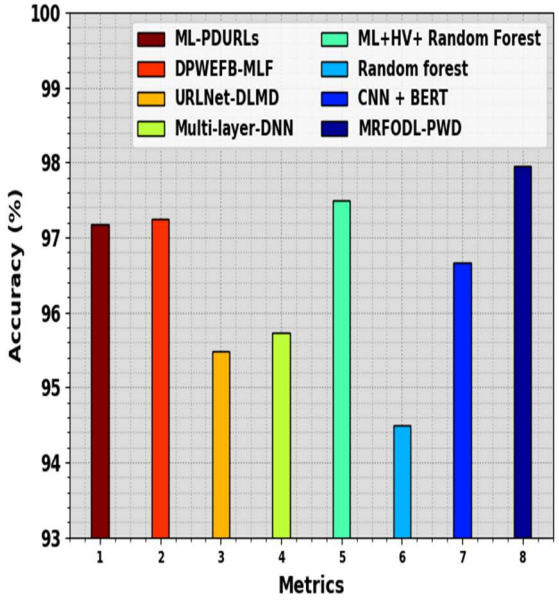


Figure 8: $Accu_y$ analysis of MRFODL-PWD algorithm with other systems

5 CONCLUSION

In this study, we have focused on the design and development of automated phishing URL detection using the MRFODL-PWD model. The major intention of the MRFODL-PWD technique is to recognize and classify the presence of legitimate or phishing URLs. It follows a series of subprocesses namely data preprocessing, BERT feature extraction, DBN classification, and MRFO-based hyperparameter tuning. In the presented MRFODL-PWD technique, several stages of pre-processing are to transfer data into useful setup and BERT is applied for feature extraction. Moreover, the DBN model can be used for automated phishing URL detection. Furthermore, the MRFO algorithm selects the hyperparameter values of the DBN model. An extensive comparison study stated that the MRFODL-PWD technique accomplishes enhanced phishing URL detection results over other models.

REFERENCES:

[1] Sánchez-Paniagua, M., Fernández, E.F., Alegre, E., Al-Nabki, W. and Gonzalez-Castro, V., 2022. Phishing URL detection: A real-case scenario through login URLs. IEEE Access, 10, pp.42949-42960.

[2] F. Tajaddodianfar, J.W. Stokes, and A. Gururajan, 2020, May. "Texception: a character/word-level deep learning model for phishing URL detection." In ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 2857-2861.

[3] S.R. Abdul Samad, S. Balasubaramanian, A.S. Al-Kaabi, B. Sharma, S. Chowdhury, A. Mehbodniya, J.L. Webber, and A. Bostani, 2023. "Analysis of the Performance Impact of Fine-Tuned Machine Learning Model for Phishing URL Detection." Electronics, 12(7), p.1642.

[4] M. Alshehri, A. Abugabah, A. Algarni, and S. Almotairi, 2022. "Character-level word encoding deep learning model for combating cyber threats in phishing URL detection." Computers and Electrical Engineering, 100, p.107868.

[5] S.S. Roy, A.I. Awad, L.A. Amare, M.T. Erkihun, and M. Anas, 2022. "Multimodel phishing URL detection using LSTM, bidirectional LSTM, and GRU models." Future Internet, 14(11), p.340.

[6] J. Hong, T. Kim, J. Liu, N. Park, and S.W. Kim, 2020. "Phishing URL detection with lexical features and blacklisted domains." Adaptive Autonomous Secure Cyber Systems, pp.253-267.

[7] M. Sameen, K. Han, and S.O. Hwang, 2020. "PhishHaven—An efficient real-time AI phishing URLs detection system." IEEE Access, 8, pp.83425-83443.

[8] Y. Wang, W. Zhu, H. Xu, Z. Qin, K. Ren, and W. Ma, 2023, June. "A Large-Scale Pretrained Deep Model for Phishing URL Detection." In ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) pp. 1-5.

[9] S.H. Ahammad, S.D. Kale, G.D. Upadhye, S.D. Pande, E.V. Babu, A.V. Dhumane, and M.D.K.J. Bahadur, 2022. "Phishing URL

detection using machine learning methods." Advances in Engineering Software, 173, p.103288.

[10] M.M. Alani and H. Tawfik, 2022. "PhishNot: a cloud-based machine-learning approach to phishing URL detection." Computer Networks, 218, p.109407.

[11] J. Anitha and M. Kalaiarasu, 2022. "A new hybrid deep learning-based phishing detection system using MCS-DNN classifier." Neural Computing and Applications, pp.1-16.

[12] R. Yang, K. Zheng, B. Wu, C. Wu, and X. Wang, 2021. "Phishing website detection based on deep convolutional neural network and random forest ensemble learning." Sensors, 21(24), p.8281.

[13] E. Zhu, Q. Yuan, Z. Chen, X. Li, and X. Fang, 2023. "CCBLA: a Lightweight Phishing Detection Model Based on CNN, BiLSTM, and Attention Mechanism." Cognitive Computation, 15(4), pp.1320-1333.

[14] T. Wen, Y. Xiao, A. Wang, and H. Wang, 2023. "A novel hybrid feature fusion model for detecting phishing scam on Ethereum using deep neural network." Expert Systems with Applications, 211, p.118463.

[15] M. Elsadig, A.O. Ibrahim, S. Basheer, M.A. Alohali, S. Alshunaifi, H. Alqahtani, N. Alharbi, and W. Nagmeldin, 2022. "Intelligent Deep Machine Learning Cyber Phishing URL Detection Based on BERT Features Extraction." Electronics, 11(22), p.3647.

[16] E. Benavides-Astudillo, W. Fuertes, S. Sanchez-Gordon, D. Nuñez-Agurto, and G. Rodríguez-Galán, 2023. "A Phishing-Attack-Detection Model Using Natural Language Processing and Deep Learning." Applied Sciences, 13(9), p.5275.

[17] N. Alqahtani, S. Alam, I. Aqeel, M. Shuaib, I. Mohsen Khormi, S.B. Khan, and A.A. Malibari, 2023. "Deep Belief Networks (DBN) with IoT-Based Alzheimer's Disease Detection and Classification." Applied Sciences, 13(13), p.7833.

[18] H.T. Kahraman, M. Akbel, and S. Duman, 2022. "Optimization of optimal power flow problem using multi-objective manta ray foraging optimizer." Applied Soft Computing, 116, p.108334.

[19] https://www.alexa.com/

[20] https://phishtank.org/