ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1175

Phishdect: An Optimised Deep Neural Network Algorithm for Detecting Phishing Attacks in Online Platform

[1]Faisal Ahmad Tijjani
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Taraba, Nigeria

[2]Badamasi Imam Ya'u
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Taraba, Nigeria

[3]Usman Ali
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Bauchi, Nigeria

[4]Mustapha Abdulrahman Lawal
Department of Computing Technologies
SRM Institute of Science and Technology
Kattankulathur, Chennai, India, 603203

[5]Fatima Shittu
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Taraba, Nigeria

[6]Abdulmutalib Abdullahi
Department of Computer Sciences
University of Calabar
Cross River, Nigeria

[7]Taiwo Olatunji Qudus
Department of Survey and Geoinformatics
Abubakar Tafawa Balewa University
Bauchi, Nigeria

[8]Ismail Zahraddeen Yakubu
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Taraba, Nigeria

Abstract:- In today's world, phishing attacks are gradually increasing, resulting in individuals losing valuables, assets, personal information, etc., to unauthorized parties. In phishing, attackers craft malicious websites disguised as well-known, legitimate sites and send them to individuals to steal personal information and other related private details. The existing phishing attack detection approach suffers from overfitting, underfitting, vanishing gradients, and local minima, as it tries to optimize a highly non-convex and high-dimensional function resulting in a good fit of the model on the training data while failing to generalize well on new, unseen test data. However, from the literature, population-based WOA can avoid local optima and get a globally optimal solution. These advantages cause WOA to be an appropriate algorithm for solving different constrained or unconstrained optimization problems for practical applications without structural reformation to deep learning algorithms algorithm. Therefore, an efficient and accurate deep learning method is proposed in this study to determine whether a website is malicious using phishing attack datasets on MATLAB 2021a. The experimental results show that the proposed model attains the highest testing accuracy of 98% as against the classical MLP algorithms which achieved the highest testing accuracy of 93%. that, the proposed system achieved the highest precision score of 97%, recall of 98. % and F-score of 97% as against the other classical approaches.

Keywords:- *Deep Learning, Whale Optimisation, Multilayer Perceptron, Phishing Attack and Long Short-Term Memory.*

I. INTRODUCTION

Phishing, a growing cyber threat, targets internet users to steal sensitive credentials like usernames and passwords. Attackers create fake websites to lure victims, often focusing on platforms like e-banking and e-commerce [1]. While blacklist technology helps, attackers can evade it by manipulating URLs or posing as secure sites. This study proposes a data-driven framework using advanced deep learning techniques to detect phishing webpages effectively. The existing methods face challenges like overfitting and underfitting, highlighting the need for more robust detection methods [4]. The study aims to develop an efficient and accurate deep learning model using phishing attack datasets in MATLAB 2021a [5]. The paper is structured as follows: related work, methodology, findings, and conclusion sections.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1175

II. RELATED WORK

Numerous studies have explored AI-based algorithms for phishing attack detection, showing high reliability and detection rates. For instance, [6] proposed a machine learning-based method for Phishing website detection, achieving over 90% accuracy in distinguishing real from fake websites. However, challenges arise due to discrete feature vectors, leading to non-smooth decision boundaries [7]. In another study, [8] improved spoofed website detection using random forest with an accuracy of 99.5%, yet struggled with complex phishing attacks. Deep learning techniques have also been effective, with [9] achieving high accuracy using DNN, LSTM, and CNN models. However, these methods require substantial data and computational resources. Recent advancements include [10] using reinforcement learning for phishing detection, [12] achieving 99.18% accuracy with an RNN-GRU model, and [17] achieving 98% accuracy using Naïve Bayes. Despite these advancements, challenges like computational complexity, model generalization, and detection of non-imitative URLs remain. Overall, these studies demonstrate ongoing efforts to enhance phishing detection using a range of machine learning and deep learning techniques.

III. METHODOLOGY

The classification system's efficacy today hinges on dataset presentation, requiring time and expertise to create specific characteristics. Deep learning, unlike traditional machine learning, extracts feature from data without manual feature design. Deep learning involves computational models with multiple layers, enabling the learning of data representations with varied levels of abstraction. Unlike traditional artificial neural networks (ANNs) limited to three layers, deep learning models have numerous hidden layers, connections, and the ability to learn complex abstractions from inputs.

This research introduces a novel technique for enhancing phishing attack detection, using a WAO-DNN base network. The methodology comprises several stages as shown in Fig. 1:

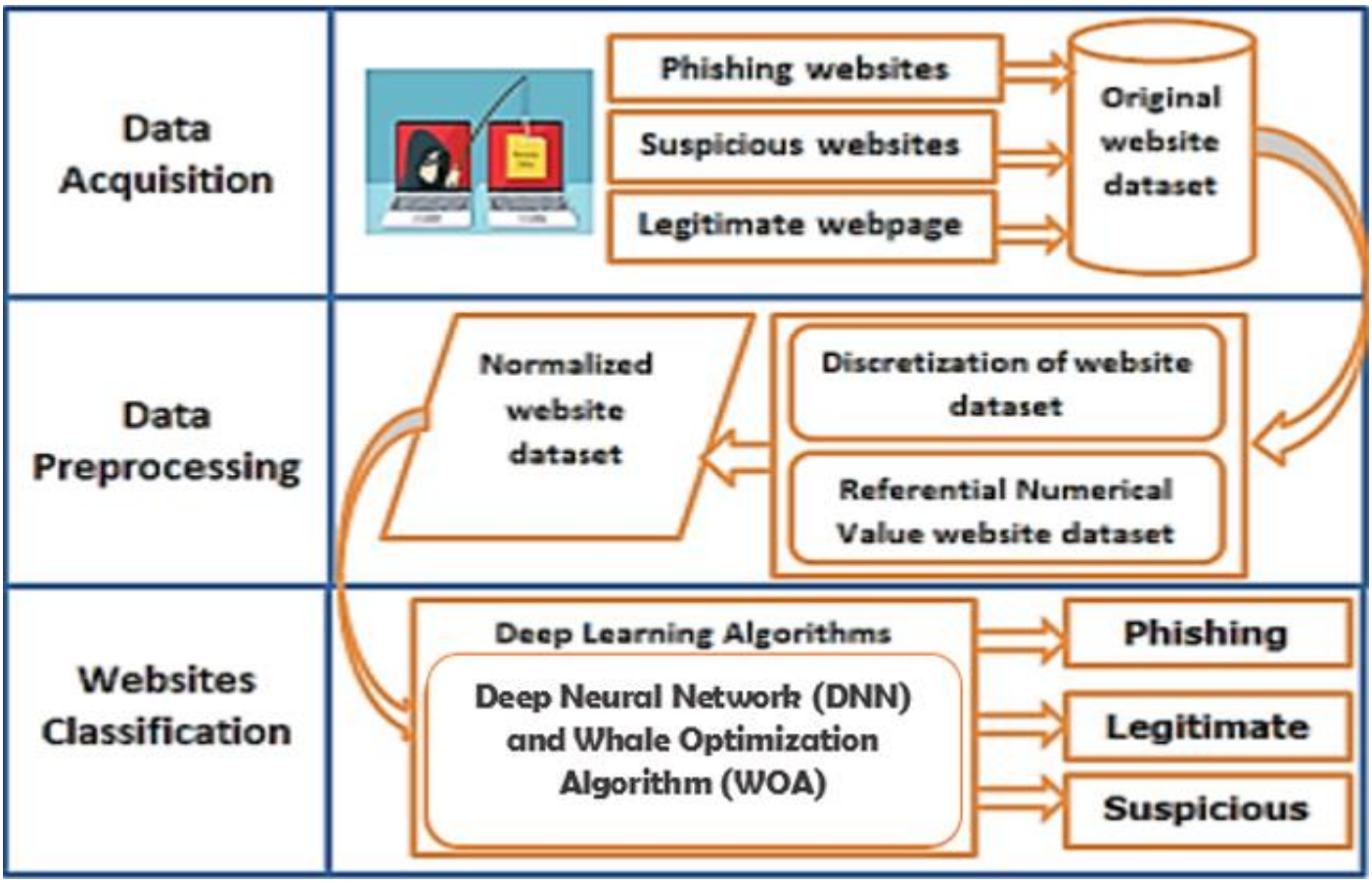

Fig 1 Overall System Architecture for The Proposed Study

➢ *The Description of the Proposed Framework is Elaborated below*

- Data Acquisition: Data sourced from www.kaggle.com contained information on over ten thousand phishing websites and various features.
- Data Preprocessing: The dataset underwent cleaning and noise removal, without any missing values.
- Deep Learning-Based Modeling: A Deep Neural Network (DNN) was trained using Whale Optimization Algorithm (WOA), optimizing connection weights.
- Deep Neural Network (DNN): The DNN includes multiple layers between input and output, enabling complex non-linear relationship modeling. The DNN architecture facilitates compositional models and feature composition from lower layers.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1175

- Whale Optimization Algorithm (WOA): WOA, inspired by humpback whales' hunting behavior, is a stochastic optimization algorithm used to find global optima in optimization problems.

➢ *The main Mathematical Equation Proposed in this Algorithm is as follows:*

$$X(t+1) = X^*(t) - AD \quad \text{for} \quad p < 0.5 \tag{1}$$

$$X(t+1) = D' e^{bl} \cos(2\pi t) + X^*(t) \quad \text{for} \quad p \geq 0.5 \tag{2}$$

Where:

P is a random number in [0, 1],

X is a position vector,

X* is the position vector of the best solution obtained so far,

D' = $|X^*(t) - X(t)|$ indicates the best solution obtained so far,

b is a constant for defining the shape of the logarithmic spiral,

l is a random number in [−1, 1],

t shows the current iteration,

$$\mathbf{D} = |CX^*(t) - X(t)| \tag{3}$$

➢ *The Vectors A and C are Calculated as follows:*

$$\mathbf{A} = 2ar - a \tag{4}$$

$$C = 2r \tag{5}$$

A linearly decreases from 2 to 0 over the course of iterations (in both exploration and exploitation phases), and **r** is a random vector in [0, 1]. Equation (2) simulates the encircling mechanism, whereas equation (3) mimics the bubble-net technique. The variable p switches between these two components with an equal probability.

The WOA starts optimizing a given problem by creating a set of random solutions. In each step of optimization, search agents update their positions based on a randomly selected search agent or the best search agent obtained so far. To guarantee exploration and convergence, the best solution is the pivot point to update the position of other search agents when |X| > 1. In other situations (when |X| < 1), the best solution obtained so far plays the role of the pivot point. The flowchart of the proposed DNN base WOA are shown in Fig. 2.

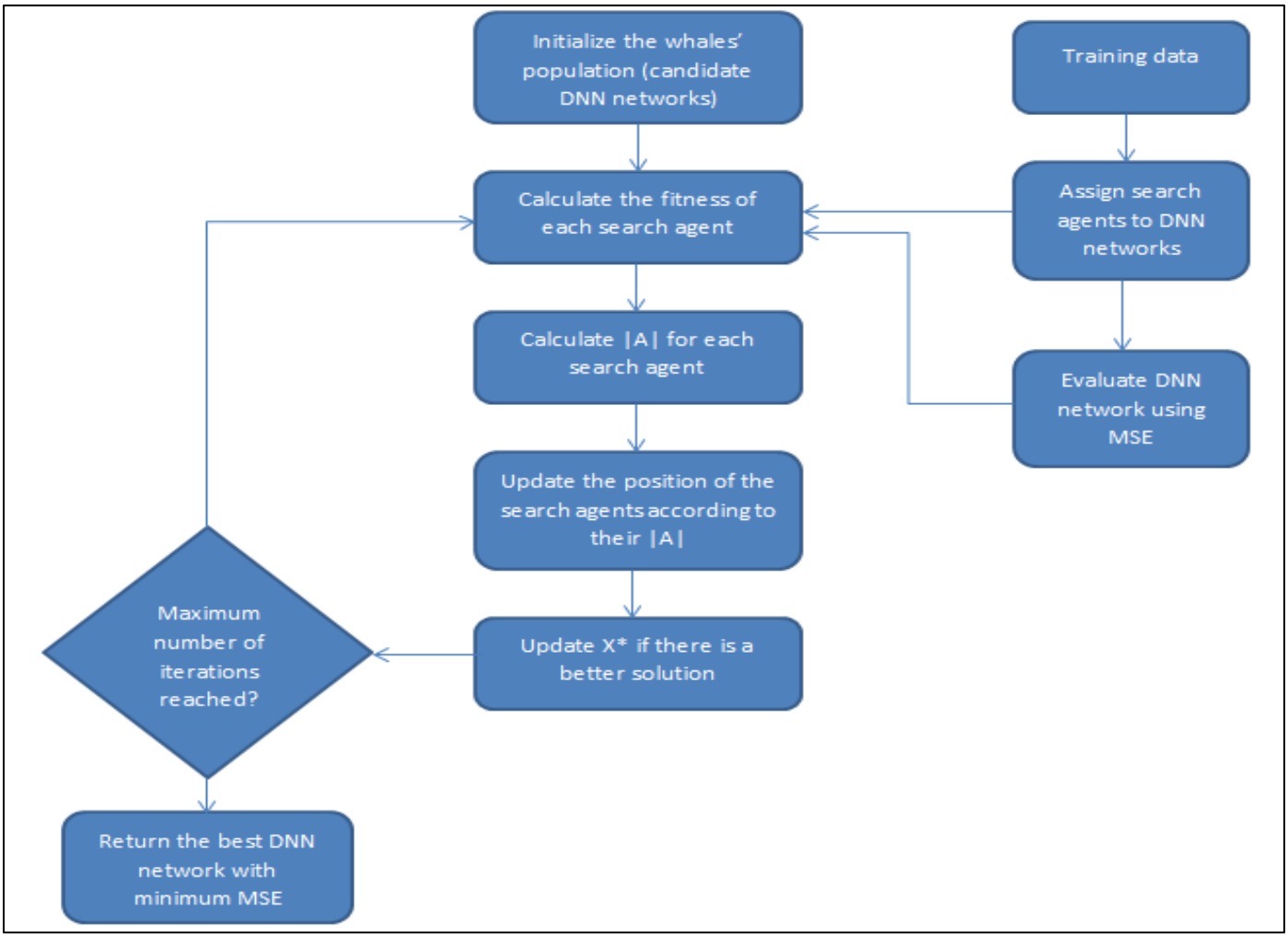

Fig 2 Flow of the Proposed Optimization Technique

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1175

It was proven by the inventors of WOA that this algorithm can solve optimization problems of different kinds. It was argued in the main work that this is due to the flexibility, gradient-free mechanism, and high local optima avoidance of this algorithm. These motivated our attempts to employ WOA as a trainer for FFNNs due to the difficulties of the learning process. Theoretically speaking, WOA should be able to train any ANN subject to proper objective function and problem formulation. In addition, providing the WOA with enough number of search agents and iterations is another factor for the success of this algorithm.

The proposed framework integrates deep learning with WOA for enhanced phishing attack detection, as illustrated in Figure 1. This approach aims to improve classification performance compared to traditional machine learning methods.

IV. RESULT AND DISCUSSION

P In this section, the proposed WOA approach for training deep network is evaluated on phishing attack datasets obtain from Kaggle. The chapter presents the result obtained after simulating the network on MATLAB 2021a. The results are presented in tabular and graphical forms which are analyzed using standard performance evaluation metrics as specified during the design. After the simulation, the decision support accuracy was used to evaluate the performance of the algorithms on phishing attack datasets. All the experiment was conducted on MATLAB 2021 using the system specification defined in the previous section. To achieve our objective, first, we set the Number of search agents to 30 and the Maximum number of iterations to 500 to enable us to load details of the selected benchmark.

Table 1 Parameter Settings

SN	Parameter	Setting
1	Input Layer	Input size
2	Hidden Layer	5
3	Fully Connected Layer	1
4	SoftMax Layer	1
5	Classification Layer	1
6	Max Epochs	7
7	Mini Batch Size	27
8	Gradient Threshold	1
9	Verbose	False
10	Execution Environment	CPU
11	Number of Hidden Neurons	500

A. Results Presentation

The proposed WOA-based deep learning algorithm is compared with the classical approach based on decision support accuracy as specified in the evaluation measures. To provide a fair comparison, all algorithms were terminated when a maximum number of iterations was reached. Finally, the accuracy, precision, recall, and F-Score is also investigated in the results to provide a comprehensive comparison. Table 2 show the statistical results and classification accuracy, as well as the most accurate result of the proposed the proposed model. Here parametric analysis is carried out in terms of accuracy, precision, recall and F-1 score.

Table 2 Experimental Results

Algorithm	Alpha Parameter	Train Acc	Test Acc	Precision	Recall	F-1
Proposed	WOA	96	98	97	98	97
MLP	0.0001	92	87	89	88	86
MLP	0.00001	94	89	92	92	91
MLP	1	95	93	91	94	92

For decision support accuracy (Accuracy, Precision, recall and F-score), the values were reported between 0 to 100. Values close to 100 means perfect detection performance while on the other hand, values close to zero implies poor detection rate. Hence, the higher the value, the better the performance of the model. Thus, from table 2, the proposed system achieved the best performance in terms of accuracy, precision, recall and F-Measure. This demonstrates the superiority of the proposed model against the classical MLP algorithms. In the next subsections, we provide the detail discussion, analysis and evaluation based on the standard evaluation metric use in this study. They include; accuracy, precision, recall and f-measure.

B. Discussion of Results

In machine learning, Training Accuracy and Testing Accuracy are two important metrics used to evaluate the performance of a trained model. They serve different purposes and provide insights into how well a model is learning and generalizing from the data. Training Accuracy measures how well a model performs on the data it was trained on. It is one of several metrics, along with recall, precision, and F1 score, that can help evaluate the overall performance of a phishing detection system. It is calculated by dividing the number of correctly predicted instances in the training dataset by the total number of instances in the training dataset. A high training accuracy indicates that the model has learned the training data well and can make accurate predictions on the data it has seen

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1175

during training. Hence, the proposed model achieved the best training accuracy of 96% as against the classical MLP which attains the best training accuracy of 95% as shown in Figure 3.

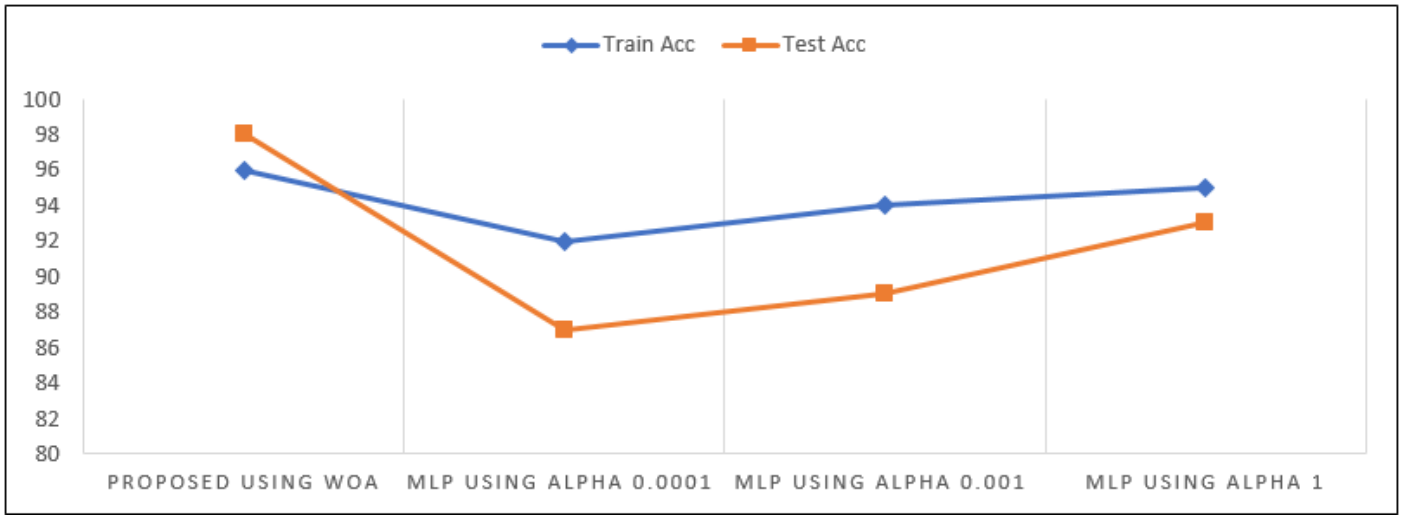

Fig 3 Training and Testing Accuracy for all Methods

However, high training accuracy doesn't guarantee that the model will perform well on unseen data (generalization). Overfitting can occur when a model becomes too specialized in fitting the training data, leading to poor performance on new, unseen data. Therefore, the testing accuracy (or validation accuracy) measures how well a model generalizes to new, unseen data. It is calculated by dividing the number of correctly predicted instances in a separate testing/validation dataset (not used during training) by the total number of instances in that dataset. A high testing accuracy indicates that the model can make accurate predictions on data it has not encountered before, suggesting good generalization. Testing accuracy is a crucial metric as it provides an estimate of how well the model is expected to perform in real-world scenarios where new data is encountered. Thus, the proposed model attains the highest testing accuracy of 98% as against the classical MLP algorithms which achieved the highest testing accuracy of 93%. This has shown how well the proposed model fits the training data. Hence, the proposed optimization has addressed the problem of overfitting seen in the classical MLP approach since the training accuracy is lower than the testing accuracy suggesting how well the proposed model generalizes to new, unseen data. However, for the classical MLP method, the training accuracy was higher than testing accuracy as a result of overfitting. It's important to monitor both metrics during model development to ensure that the model neither underfits (low training accuracy) nor overfits (high training accuracy but low testing accuracy) the data. Balancing these two aspects is essential for building models that perform well in practice.

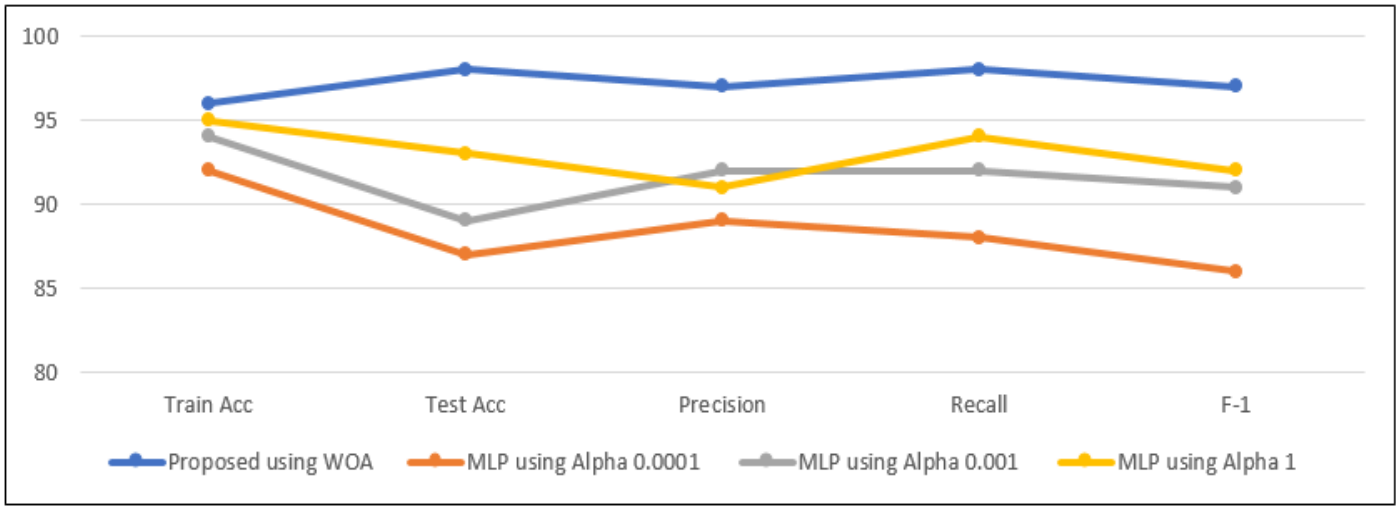

Fig 4 Overall Results for all Methods on Different Metrics

The accuracy can be misleading in some cases. precision and recall help us further understand how strong the accuracy shown holds true for a particular problem. In the context of phishing attack detection, "precision" is a crucial evaluation metric that measures the accuracy of positive predictions made by a classification model. It helps answer the question, "Of all the instances predicted as phishing attacks, how many were phishing attacks?" In other words, precision assesses the model's ability to make correct positive predictions and avoid false positives. A higher precision score indicates that the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1175

model is good at avoiding false alarms, meaning that when it predicts a phishing attack, it is more likely to be correct. In the context of phishing attack detection, high precision is essential because false positives (incorrectly flagging legitimate emails or websites as phishing) can be disruptive and harmful. In our case, the proposed model achieved a precision score of 97%. This is better when compared to all the three classical MLP methods which attain the highest precision of 92%. By achieving the best precision score, this has demonstrated the model's ability to correctly identify phishing attacks while minimizing false alarms.

However, there is typically a trade-off between precision and recall (sensitivity) in machine learning. Increasing precision often comes at the cost of lower recall, meaning that the model may miss some actual phishing attacks in an attempt to avoid false positives. Achieving a balance between precision and recall is important, and it depends on the specific goals and requirements of the phishing detection system. Precision doesn't take into account the cases where the model missed positive instances (false negatives), which is where recall comes into play. In situations where both false positives and false negatives have different implications, precision and recall need to be balanced to find an optimal model performance. Therefore, the recall score is analyzed in the next subsection.

Recall is a critical metric in phishing attack detection, as it measures the model's ability to correctly identify all phishing attacks, thus reducing the chances of missing genuine threats. When evaluating a phishing detection system, it is essential to consider recall along with other metrics. However, there is often a trade-off between recall and precision in machine learning. Increasing recall can lead to more false positives (non-phishing instances incorrectly classified as phishing), which may result in more false alarms. Balancing recall and precision are important, and the specific balance depends on the goals and requirements of the phishing detection system. From Fig. 9 above, the proposed system achieved the best recall of 98%. as against the other baseline methods. This performance was superior when compare to the highest recall value of 94% achieved by all the classical MLP methods. By achieving a higher recall score the proposed model indicates that the network is good at capturing a higher proportion of actual phishing attacks, minimizing the chances of missing genuine threats. In the context of phishing attack detection, high recall is crucial because failing to detect a phishing attack can have serious consequences, including data breaches and financial losses. However, precision and recall are often combined into a single metric called the F1-score, which provides a balance between the two.

As stated earlier, F-Measure provides a single score that balances both the concerns of precision and recall in one number. In statistical analysis of binary classification, the F1 score (also F-score or F-measure) is a measure of a test's accuracy. It is calculated from the precision and recall of the test, where the precision is the number of correctly identified positive results divided by the number of all positive results, including those not identified correctly, and the recall is the number of correctly identified positive results divided by the number of all samples that should have been identified as positive. In each case a higher value shows how confident the classification accuracy or performance can be relied upon.

From Figure 4 above, the proposed system achieved the highest F-score of 97% as against the other classical approaches. Therefore, by achieving higher values both in terms of accuracy, precision recall and F-score as shown in Figure 17, the proposed model has further cemented its overall superiority in classifying the cases of phishing attacks from the network datasets as compared to the state-of-the-art MLP methods. The success of this approach relies on the WOA to reliably prevent premature convergence toward local optima and find the best optimal values for deep neural network's weights and biases. The results proved that the WOA can address the overfitting issues in the existing studies by local optima avoidance and improving the convergence speed. The high local optima avoidance is due to the high exploration of this algorithm. The random selection of prey in each selection is the main mechanism that assisted this algorithm in avoiding the many local solutions in the problem of training DNNs. Another mechanism is the enemy-encircling approach of WOA, which requires the search agents to search the space around the prey. The superior convergence speed of a WOA-based trainer originates from the saving of the best prey and adaptive search around it. The search agents in WOA tend to search more locally around the prey proportional to the number of iterations. The WOA-based trainer inherits this feature from the WOA and manages to outperform all the classical MLP algorithms. This has shown how well the proposed model fits the training data. Hence, the proposed optimization has addressed the problem of overfitting seen in the classical MLP approach since the training accuracy is lower than the testing accuracy suggesting how well the proposed model generalizes to new, unseen data. The success of this approach relies on the WOA to reliably prevent premature convergence toward local optima and find the best optimal values for deep neural network's weights and biases. The results proved that the WOA can address the overfitting issues in the existing studies by local optima avoidance and improving the convergence speed.

V. CONCLUSION

The escalating frequency of phishing attacks in today's digital landscape has led to significant losses for individuals, including personal information and assets. This study introduces an effective method for identifying malicious websites, crucial in combating phishing attempts. The proposed Whale Optimization Algorithm (WOA) approach for training deep networks was evaluated using phishing attack datasets from Kaggle on MATLAB 2021a. Comparative analysis with classical approaches based on decision support accuracy was conducted using standard evaluation metrics.

The experimental findings demonstrate the superiority of the proposed model, achieving a testing accuracy of 98% compared to classical MLP algorithms with a maximum of 93% testing accuracy. This indicates the proposed model's robustness in generalizing to new data, addressing the overfitting issue observed in traditional MLP approaches. Moreover, the proposed system achieved the highest precision (97%), recall (98%), and F-score (97%), further confirming its

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1175

effectiveness in classifying phishing attacks compared to conventional methods.

While the study yielded promising results, it was limited to phishing attack datasets. Future research should explore the proposed model's applicability to other critical cyber-attacks such as zero-day attacks and man-in-the-middle attacks. Enhancing the model's generalization across various network intrusion scenarios would further bolster its effectiveness in cybersecurity contexts.

ACKNOWLEDGMENT

We extend our gratitude to our supervisors, Dr. B. I. Yau and Dr. Usman Ali, for their invaluable guidance and support throughout this research, contributing significantly to its success.

REFERENCES

[1]. Weldon, K.a., et al., Petroleum prices prediction using data mining techniques--A Review. arXiv preprint arXiv:2211.12964, 2022.
[2]. Guo, J. Oil price forecast using deep learning and ARIMA. in 2019 International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI). 2019. IEEE.
[3]. Xu, Z., et al., Using econometric and machine learning models to forecast crude oil prices: Insights from economic history. Resources Policy, 2023. 83: p. 103614.
[4]. An, J., Oil price predictors: Machine learning approach. 2019.
[5]. ArunKumar, K., et al., Comparative analysis of Gated Recurrent Units (GRU), long Short-Term memory (LSTM) cells, autoregressive Integrated moving average (ARIMA), seasonal autoregressive Integrated moving average (SARIMA) for forecasting COVID-19 trends. Alexandria engineering journal, 2022. 61(10): p. 7585-7603.
[6]. Kim, G.I. and B. Jang, Petroleum Price Prediction with CNN-LSTM and CNN-GRU Using Skip-Connection. Mathematics, 2023. 11(3): p. 547.
[7]. Shu-rong, L. and G. Yu-lei. Crude oil price prediction based on a dynamic correcting support vector regression machine. in Abstract and applied analysis. 2013. Hindawi.
[8]. Rosli, N., R. Ibrahim, and I. Ismail, Intelligent prediction system for gas metering system using particle swarm optimization in training neural network. Procedia Computer Science, 2017. 105: p. 165-169.
[9]. Gao, S. and Y. Lei, A new approach for crude oil price prediction based on stream learning. Geoscience Frontiers, 2017. 8(1): p. 183-187.
[10]. Gumus, M. and M.S. Kiran. Crude oil price forecasting using XGBoost. in 2017 International conference on computer science and engineering (UBMK). 2017. IEEE.
[11]. Huang, L. and J. Wang, Global crude oil price prediction and synchronization based accuracy evaluation using random wavelet neural network. Energy, 2018. 151: p. 875-888.
[12]. Folorunso, S., A. Taiwo, and O. Olabanjo, A predictive model for estimating petroleum consumption using machine learning approach. Lautech journal of engineering and technology, 2018. 12(2): p. 80-87.
[13]. Bristone, M., R. Prasad, and A.A. Abubakar, CPPCNDL: Crude oil price prediction using complex network and deep learning algorithms. Petroleum, 2020. 6(4): p. 353-361.
[14]. Cen, Z. and J. Wang, Crude oil price prediction model with long short term memory deep learning based on prior knowledge data transfer. Energy, 2019. 169: p. 160-171.
[15]. An, J., A. Mikhaylov, and N. Moiseev, Oil price predictors: Machine learning approach. International Journal of Energy Economics and Policy, 2019. 9(5): p. 1.
[16]. Shambulingappa, H., Crude oil price forecasting using machine learning. International Journal of Advanced Scientific Innovation, 2020. 1(1): p. 1-11.
[17]. Zhang, T., et al., Multi-step-ahead crude oil price forecasting based on two-layer decomposition technique and extreme learning machine optimized by the particle swarm optimization algorithm. Energy, 2021. 229: p. 120797..