




## Article

# Evolutionary Algorithm with Deep Auto Encoder Network Based Website Phishing Detection and Classification

Hamed Alqahtani <sup>1</sup>, Saud S. Alotaibi <sup>2</sup>, Fatma S. Alrayes <sup>3</sup>, Isra Al-Turaiki <sup>4</sup>, Khalid A. Alissa <sup>5</sup>, Amira Sayed A. Aziz <sup>6</sup>, Mohammed Maray <sup>7</sup> and Mesfer Al Duhayyim <sup>8,\*</sup>

- <sup>1</sup> Department of Information Systems, College of Computer Science, Center of Artificial Intelligence, Unit of Cybersecurity, King Khalid University, Abha 62529, Saudi Arabia; hsqhtani@kku.edu.sa
  - <sup>2</sup> Department of Information Systems, College of Computing and Information System, Umm Al-Qura University, Mecca 24382, Saudi Arabia; ssotaibi@uqu.edu.sa
  - <sup>3</sup> Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; falrayes@pnu.edu.sa
  - <sup>4</sup> Department of Information Technology, College of Computer and Information Sciences, King Saud University, P.O. Box 145111, Riyadh 4545, Saudi Arabia; ialtraiki@ksu.edu.sa
  - <sup>5</sup> SAUDI ARAMCO Cybersecurity Chair, Networks and Communications Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; kaalissa@iau.edu.sa
  - <sup>6</sup> Department of Digital Media, Faculty of Computers and Information Technology, Future University in Egypt, New Cairo 11835, Egypt; amirabdelaziz@fue.edu.eg
  - <sup>7</sup> Department of Information Systems, College of Computer Science, King Khalid University, Abha 62529, Saudi Arabia; mmarey@kku.edu.sa
  - <sup>8</sup> Department of Computer Science, College of Sciences and Humanities-Aflaj, Prince Sattam Bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia
- \* Correspondence: m.alduhayyim@psau.edu.sa



**Citation:** Alqahtani, H.; Alotaibi, S.S.; Alrayes, F.S.; Al-Turaiki, I.; Alissa, K.A.; Aziz, A.S.A.; Maray, M.; Al Duhayyim, M. Evolutionary Algorithm with Deep Auto Encoder Network Based Website Phishing Detection and Classification. *Appl. Sci.* **2022**, *12*, 7441. <https://doi.org/10.3390/app12157441>

Academic Editors: Suhui Luo and Kamran Shaukat

Received: 27 May 2022

Accepted: 18 July 2022

Published: 25 July 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Abstract:** Website phishing is a cyberattack that targets online users for stealing their sensitive data containing login credential and banking details. The phishing websites appear very similar to their equivalent legitimate websites for attracting a huge amount of Internet users. The attacker fools the user by offering the masked webpage as legitimate or reliable for retrieving its important information. Presently, anti-phishing approaches necessitate experts to extract phishing site features and utilize third-party services for phishing website detection. These techniques have some drawbacks, as the requirement of experts for extracting phishing features is time consuming. Many solutions for phishing websites attack have been presented, such as blacklist or whitelist, heuristics, and machine learning (ML) based approaches, which face difficulty in accomplishing effectual recognition performance due to the continual improvements of phishing technologies. Therefore, this study presents an optimal deep autoencoder network based website phishing detection and classification (ODAE-WPDC) model. The proposed ODAE-WPDC model applies input data pre-processing at the initial stage to get rid of missing values in the dataset. Then, feature extraction and artificial algae algorithm (AAA) based feature selection (FS) are utilized. The DAE model with the received features carried out the classification process, and the parameter tuning of the DAE technique was performed using the invasive weed optimization (IWO) algorithm to accomplish enhanced performance. The performance validation of the ODAE-WPDC technique was tested using the Phishing URL dataset from the Kaggle repository. The experimental findings confirm the better performance of the ODAE-WPDC model with maximum accuracy of 99.28%.

**Keywords:** cybersecurity; internet of things; cloud computing; computational models; deep learning; metaheuristics; phishing detection; website phishing

## 1. Introduction

Cybercrime can be defined as crime that targets networks or computers. Computer crimes are covered by a wide range of potentially criminal actions. Phishing is regarded as

most frequently employed attack over social networks. With these assaults, the phisher endeavors to obtain personal data from the user to be utilized dishonestly toward users [1,2]. In the current digital business scenario, many corporations are making use of the ever-evolving changes of cyberspace, owing to the development of the internet day by day, particularly because of the impacts of COVID-19 which has pushed every person to highly utilize internet in every field. As the largest computer network [3], the internet is a serious platform for the success of business and its growth, as most marketable trades are held online [4]. In spite of the ease linked with online transactions from businesses as well as users, there occurs an online menace called phishing. Phishing indulges in making a well-designed website (WS) that imitates prevailing authentic commercial WSs for deceiving users and illegally acquiring their login credentials and documents, which alleviates phishers in obtaining accessibility to the legitimate financial data of users [5]. Inappropriately, the phishing impact was fatal because legal users who were affected were prone to find theft and data breaches and do not have a faith in electronic banking and online trade. Phishing commonly appears through an email which is sent to users, from trustworthy resources, which urges them in adjusting their login credentials by following or clicking a hyperlink in these emails [6].

Phishing is symbolically the same as fishing in water bodies; however, rather than catching fish, invaders attempt to obtain the confidential information of users. Phishing WSs seem to be same as the corresponding legal WSs for alluring great numbers of internet users. The current advancements in the detection of phishing have resulted in the progress of several novel techniques on the basis of visual similarity [7]. In recent decades, the usage of deep learning (DL), computational technique, and machine learning (ML) have grown exponentially in evolving solutions for several fields, particularly education, medicine, finance, and cybersecurity. Whereas such applications of ML methods have proven advantageous in several domains, they also have several disadvantages, such as adversarial attacks, a lack of benchmark datasets, the cost of architecture, imbalanced datasets, and the inability to learn from small datasets. Conversely, innovative techniques, namely DL, generative adversarial networks, one-shot learning, and continuous learning, were applied successfully for sorting several responsibilities in such domains. Thus, it becomes important to implement such novel techniques in life-critical missions and measure the success of less conventional techniques utilized in such domains [8].

This study presents an optimal deep autoencoder network based website phishing detection and classification (ODAE-WPDC) model. The proposed ODAE-WPDC model applies input data pre-processing at the initial stage to get rid of missing values in the dataset. Then, feature extraction and artificial algae algorithm (AAA) based feature selection (FS) are utilized. The DAE model with the received features carries out the classification process, and the parameter tuning of DAE technique is performed using the invasive weed optimization (IWO) algorithm to accomplish enhanced performance. The IWO is a derivative-free real parameter optimization technique that mimics the ecological behavior of colonizing weeds. The performance validation of the ODAE-WPDC methodology was tested utilizing benchmark Kaggle repository. In short, the paper's contributions can be summarized as follows.

- Propose an intelligent model using metaheuristic and deep learning model to identify phishing websites via feature selection and classification processes;
- Employ AAA based feature subset selection process to reduce curse of dimensionality;
- Apply IWO with DAE classifier and the hyperparameter tuning process using the IWO algorithm helps in achieving enhanced performance;
- Validate the performance of the proposed model on the Phishing URL dataset from the Kaggle repository.

## 2. Related Works

Numerous works related to cybersecurity-based solutions are available in the literature [9,10]. The authors in [11] concentrate on implementing a DL structure for detecting

phishing WSs. This work initially designs two kinds of features for web phishing, such as original and interaction features. The detection method dependent upon DBN is then projected. In [12], it can be projected a manner for detecting malicious URL addresses with accuracy, utilizing CNNs. In contrast to the preceding mechanism, whereas URL or traffic statistics or web contents are analyzed, it can be analyzed only the URL text. Therefore, this technique is faster and detects zero-day attacks. Do et al. [13] establish the model of phishing and DL from the context of cybersecurity. Afterward, classifications of phishing detection and DL techniques are offered for classifying the recent works into several types. Then, taking the presented classification as baseline, this research widely analyzes the recent DL approaches and examines their benefits and drawbacks.

The authors in [14] examine a novel technique for identifying phishing WSs utilizing hyperlinks accessible from the source code of HTML webpage from the equivalent WS. This feature is utilized for training the supervised DNN approach with Adam optimizing to differentiate fraudulent WSs from genuine WSs. The presented DL approach with Adam optimizer utilizes a listwise method for classifying phishing as well as genuine WSs. Odeh et al. [15] propose the recent methods for phishing WS recognition utilizing the ML approaches. The popularly studied methods are concentrated on classical ML approaches. Ada Boosting, SVM, RF, and NB are the powerful ML approaches studied in the works. This review work also recognizes DL-based approaches with optimum efficiency to detect phishing WSs related to the conventional ML approaches. Makkar and Kumar [16] examine a cognitive spammer structure that eliminates spam pages if the search engines compute the webpage rank score. The structure identifies web spam with the assistance of the LSTM network by training the link features. In [17], a real-time anti-phishing model that utilizes seven distinct classifier approaches and NLP based features is presented. The model has the subsequent differentiating property in other studies in analyses: language independence, utilization of massive size of legitimate and phishing datasets, real-time implementation, recognition of novel WSs, independence in third-party service, and utilization of feature-rich classifications.

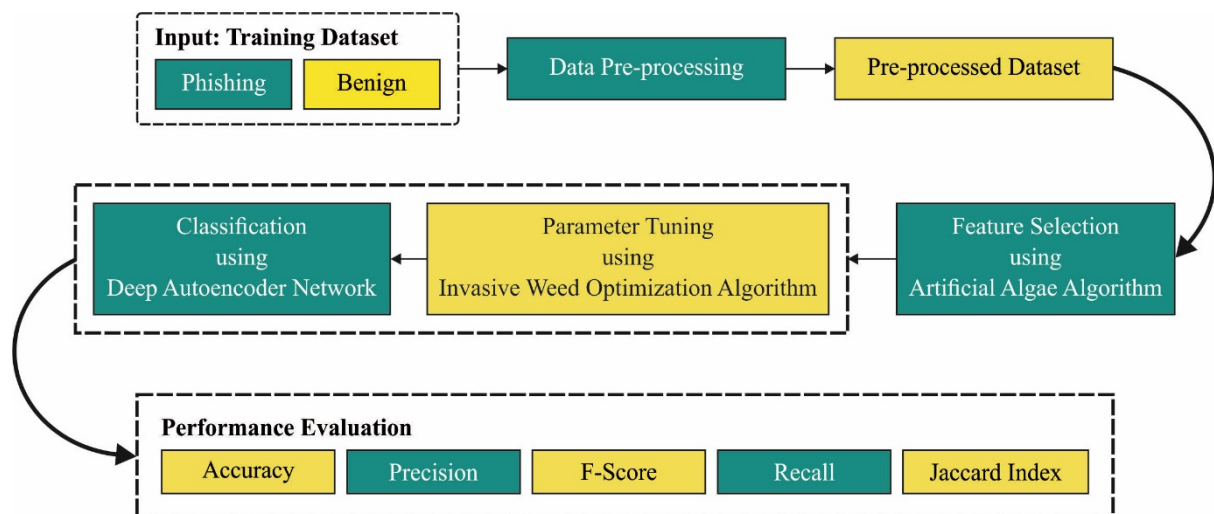
Lee et al. [18] propose an effective phishing page detection model by the use of multiple models, where every model is trained by the insertion of (controlled) noises in a subset of arbitrarily elected features from entire set of features. Ghaleb et al. [19] introduce a 2-stage ensemble learning approach with the integration of random forest (RF) based pre-classification and multilayer perceptron (MLP) based decision making. The trained MLP classification model substitutes the majority voting method of the three trained RF models to make decisions. Kondracki et al. [20] present the initial examination of the man-in-the-middle (MITM) phishing toolkit. With the detailed investigation of the toolkit, the implicit network level characteristics are identified, which can be employed for the detection process. In addition, an ML-based classification model is derived to find the existence of toolkits for online communication purposes. Noah et al. [21] introduce an anti-phishing model named PhisherCop, which is based on the stochastic gradient descent (SGD) and a support vector classifier (SVC) model. The authors in [22] introduce the Crawlphish model to automatically detect and categorize client-side cloaking utilized by recognized phishing websites. The authors also present a taxonomy of eight distinct kinds of evasion over three high-level classes.

ML-based phishing website detection utilizes ML models for the detection of manually extracted phishing website URL features. The efficacy of the recognition process can be enhanced by this approach. It necessitates experts in the extraction of URL features manually, designing a training set for phishing website detection, and, lastly, utilizing supervised learning approaches for phishing website detection. To resolve the manual feature extraction process, the DL models are found to be useful. At the same time, the choice of proper DL model is a difficult process. In particular, when phishers alter the attacking strategies for leveraging the system susceptibilities and the users' unawareness, the selection of the proper model can result in unpredicted outcomes, resulting in a waste of effort and eventually affecting the model's accuracy and efficiency. On the other hand,

the fine-tuning procedure of DL models is another challenging problem that needs to be resolved. Motivated to solve this problem, in this work, the IWO algorithm is applied to fine tune the DAE parameters to accomplish maximum detection accuracy.

### 3. The Proposed Model

In this study, a novel ODAE-WPDC model is introduced for the recognition and classification of WS phishing to achieve cybersecurity. At the primary stage, the proposed ODAE-WPDC model applies input data pre-processing at the initial stage to get rid of missing values in the dataset. This is followed by feature extraction, and the AAA based FS process is utilized. Finally, the IWO with DAE model is applied for the classification process. Figure 1 depicts the block diagram of the ODAE-WPDC approach.



**Figure 1.** Block diagram of ODAE-WPDC approach.

#### 3.1. Data Pre-Processing

This is the initial processing of data for preparing them for initial processing or further examination. It removes the feature which has missing values or null values. The significant features compared with phishing WS URLs are removed with this phase. At this point, features such as URL length, abnormal URL, statistical report, and so on, are extracted for phishing URL recognition.

#### 3.2. Design of AAA Based FS Technique

Once the raw data are pre-processed and features are extracted, the AAA-FS model is utilized to choose feature subsets. In 2015, Uymaz et al. [23] presented AAA, a bio-inspired metaheuristic optimized technique to overcome real-time and continuous optimization issues. It is a stimulation for the search activity of microalgae. Every individual is regarded as an artificial algal community (AAC) from the population-based technique; also, every AAC resembles a solution from the problem space. The life cycle encompasses mitotic reproduction, altering the dominant species, and environmental adaptation. The adaptation stage, the reproduction or evolutionary stage, and the helical movement phase are the three stages of AAA. The evolutionary/reproduction stage is exploited for replenishing the community cell by resurrecting algae by mitotic division when they have enough light and nutrients in the environment. Algae perform a movement named helical motion. The algae population exists in liquid atmosphere and congregates nearer to the liquid surface

wherever there is a sufficient light source. The algae cell uses their flagellum (organelle) for helical motion [24]. Figure 2 depicts the flowchart of AAA and explained in Algorithm 1.

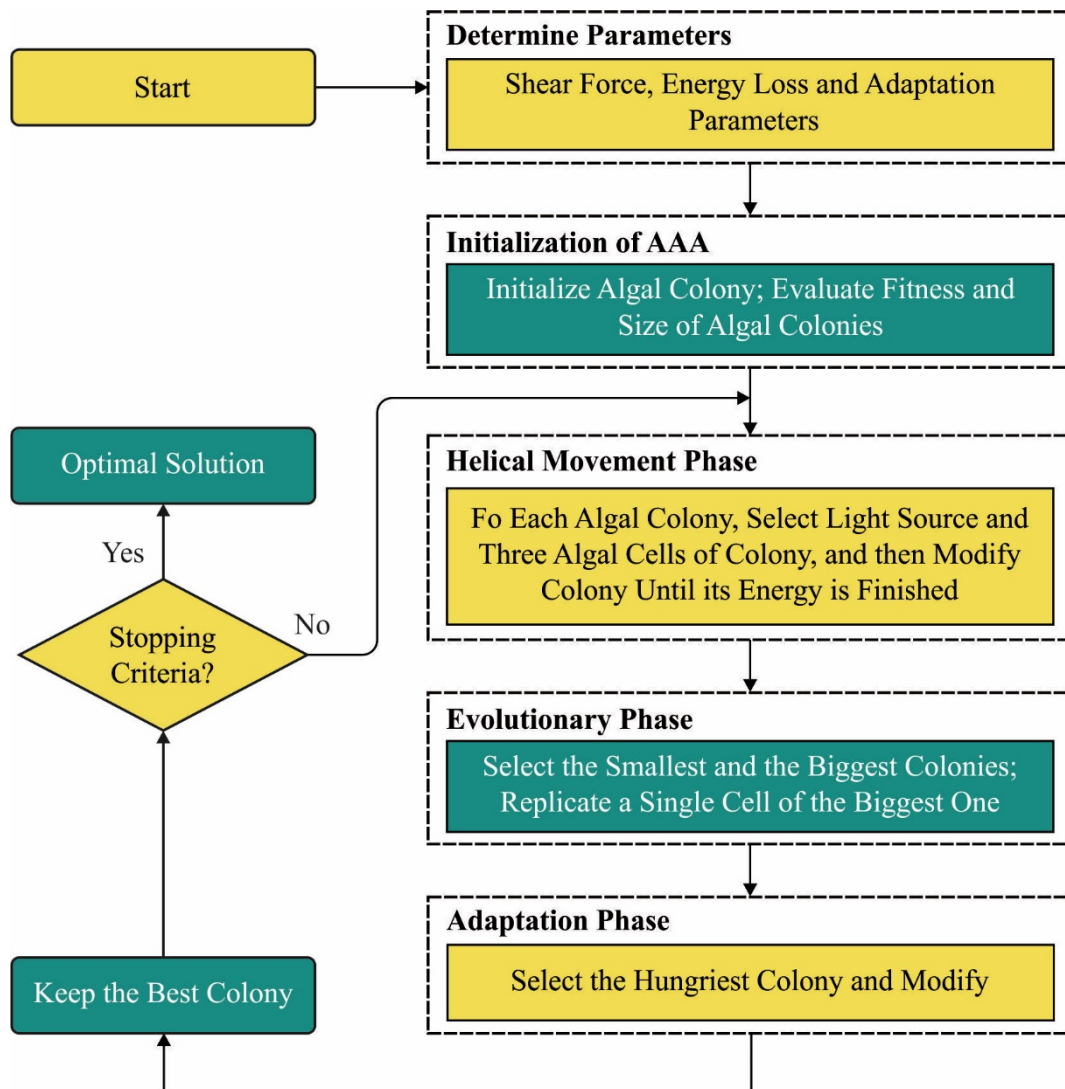
---

**Algorithm 1:** Pseudocode of AAA

---

Initialization: Generate  $N$  population of algae colonies  
Determine fitness  $f(x_i), i = 1, 2, \dots, N, D$   
where  $x_i$  = algae colony,  $N$  = number of algae colonies, and that the  $D$  = problem dimensionality  
while termination condition is unsatisfied do  
  for  $i = 1$  to  $n$  do  
    while energy of  $i^{th}$  colony not done do  
      Employ helical movement stage  
    end while  
  end for  
  Employ evolutionary/reproduction stage  
  Employ adaptation stage  
end while

---



**Figure 2.** Flowchart of AAA.



The fitness function (FF) utilized in the presented AAA-FS system was planned to contain a balance between the amount of chosen features from all the solutions (minimal) and the classifier accuracy (maximal) reached by utilizing these chosen features; Equation (1) demonstrates the FF for evaluating the solution.

$$\text{Fitness} = \alpha \gamma_R(D) + \beta \frac{|R|}{|C|} \quad (1)$$

whereas  $\gamma_R(D)$  implies the classifier error rate of provided classier (the K-nearest neighbor (KNN) technique is utilized).  $|R|$  refers to the cardinality of the chosen subset and  $|C|$  signifies the entire amount of features from the dataset.  $\alpha$ , and  $\beta$  are two parameters equivalent to the significance of classifier quality and subset length.  $\alpha \in [1, 0]$  and  $\beta = 1 - \alpha$ .

### 3.3. Process Involved in DAE Classification

When the features are selected, they can be fed into the DAE classification approach. An SAE is also known as DAE, which is the original deep network that comprises AE using several hidden layers and generates sensitive power [25]. For the classifier issue, the softmax classification is widely selected by the resultant layer. Next, the recreation of input instances with lesser error is a popular method. The trained set is provided by

$$(X, Y) = \left\{ \left( x^{(n)}, y^{(n)} \right) \middle| n = 1, 2, \dots, N \right\} \quad (2)$$

In Equation (2),  $y^{(n)}$  indicates a sample trademark  $x^{(n)}$ . The number of instances is represented as  $N$ . For each instance of trainable dataset  $x^{(n)}$ , the code encoded using  $h^{(n)} = f(x^{(n)})$  later decodes  $h^{(n)}$  for reconstructing with  $x^{?(n)} = g(h^{(n)})$ , and  $f$  and  $g$  are the encoder and decoder variables. This is resolved by diminishing errors among the inputs and reconstructions.

$$h^{(n)} = s(Wx^{(n)} + b) \quad (3)$$

$$x^{?(n)} = s(Wh^{(n)} + b?) \quad (4)$$

The sigmoid function is represented as  $s(\cdot)$ , a trained dataset using energy utilization as follows:

$$(\theta) = \frac{1}{N} \sum_{n=1}^N \frac{1}{2} \|x^{(n)} - x^{?(n)}\|_2^2 \quad (5)$$

Parameter absence in  $s$  and  $\theta$  from linear conversion. The standard auto-counter is fundamental for the model of DAE that encodes  $x^{(n)}$  to hidden notation  $h^{(n1)}$  that is provided to the following input port of DAE. The recurrence of the process of the consequential layer for  $l = 1, \dots, L$ , where  $L$  characterizes the number of hidden layers from DAE. The resultant layer is involved in the topmost hidden layer for monitoring the trained procedure. All the layers produce the best outcomes because of training the design parameter. Fine-tuning is commonly utilized from NN as a global optimization technique; hence, it enhances the DAE accuracy. The deviation of true labels from output values is decreased by the fine-tuning process. The representation of the square error cost depends on ideal samples stated in the following:

$$J(W, b; x^{(n)}, y^{(n)}) = \frac{1}{2} \|y^{(n)} - y^{?(n)}\|_2^2 \quad (6)$$

The energy function  $J(W, b)$  forces the results to be nearer to the true label throughout the whole preparation and determines the procedure of fine-tuning.

$$J(W, b) = \frac{1}{N} \sum_{n=1}^N J(W, b; x^{(n)}, y^{(n)}) \quad (7)$$

From the equation,  $(W, b) = \{ (W^{(l)}, b^{(l)}) | 1 = 1, 2, \dots, L \}$  are encoder constraints of the whole layer. The initialization of the parameter is the initial phase of the DL technique, thus minimizes the constraint updating through energy function with a stochastic technique to complete the DAE tuning.

### 3.4. Hyperparameter Optimization

At the final stage, the IWO algorithm assists in attaining maximum outcome by the use of the IWO-based hyperparameter tuning process. The IWO algorithm is a bio-simulated mathematical optimization technique that mimics the natural behaviors of weeds [26]. IWO has lots of benefits, namely very strong robustness, simplicity of structure, and requiring fewer parameters; it is utilized for solving linear, nonlinear, general, and multidimensional optimization problems. It is assumed to be effective in converging to the most suitable solution using fundamental characteristics, namely growth, seeding, and competition in a weed colony.

**Initial population:** Firstly, the population is distributed in a random fashion through the  $D$ -dimension solution space, as weeds are created at random.

**Reproduction:** The number of seeds generated by all the weeds is estimated based on fitness. Every seed has a probability of reproducing; also, the reproduction rate ranges from higher to lesser depends upon an optimal-to-worse-fit seed. Then, the seed develops into a wild plant able to generate new units, and it is formulated as follows:

$$ot_n = \frac{f - f_{worst}}{f_{best} - f_{worst}} (S_{max} - S_{min}) + S_{min} \quad (8)$$

In Equation (8),  $f$  denotes the fitness of the weed.  $f_{worst}$  and  $f_{best}$  indicate the worse and optimal fitness of the present population, correspondingly.  $S_{min}$  and  $S_{max}$  refer to the lesser and higher counts of seeds.

**Spatial distribution:** The seed generated is distributed in a random fashion through the  $D$ -dimension search space, usually an arbitrary number taking a mean corresponding to zero with a variance. By scattering the seeds arbitrarily, it can be guaranteed that they are nearer to the parental plant. However, the standard deviation (SD) ( $\sigma$ ) would decrease from a primary value ( $\sigma_{init}$ ) to last value ( $\sigma_{final}$ ). Then, it equated to the following.

$$\sigma_{cur} = \frac{(iter_{max} - iter)^n}{(iter_{max})^n} (\sigma_{init} - \sigma_{final}) + \sigma_{final} \quad (9)$$

In Equation (9),  $iter_{max}$  denotes the maximal iteration count,  $\sigma_{cur}$  denotes the SD at present step,  $\sigma_{init}$  signifies the 1st SD,  $\sigma_{final}$  represents the final SD, and  $n$  indicates the modulation index.

**Competitive exclusion:** Here, the weed number in a colony exceeds the maximal population count with rapid reproductions. Next, the created seed is permitted for propagating to search spaces. Next, lower fitness weeds are detached for attaining the maximal population allowable from the colony. This process is continued till the maximal iteration or ending condition is accomplished. The weeds using the optimum fitness are preferred as the most suitable solution as illustrate in Algorithm 2.

**Algorithm 2:** Pseudocode of IWO technique

---

```

Begin {
  Initializing population of weeds, set parameters;
  Current_iteration = 1;
  While (Current_iteration < Max_iteration) do
  {
    Estimate an optimum and worse fitness from the populations
    Estimate the SD std depends on iteration
    For all the weeds w from the population W
    {
      Calculate the amount of seeds for w depending on their fitness
      Choose the seeds in the possible solution nearby the parent weed w from a neighborhood with
      standard distribution containing mean = 0 and SD = std;
      Increase seeds created to population W
      If (|W| > Max_SizePopulation)
      {
        Sorting the population w based on its fitness
        W = SelectBetter (weed, seed, Max_SizePopulation)
      } End if
    } End for
    Current_iteration = Current_iteration + 1;
  } End while
} End

```

---

The IWO system develops a FF for achieving maximal classifier efficacy. It solves a positive integer for defining the best performance of candidate results.

$$\begin{aligned}
 \text{fitness}(x_i) &= \text{Classifier Error Rate}(x_i) \\
 &= \frac{\text{number of misclassified samples}}{\text{Total number of samples}} * 100
 \end{aligned}
 \quad (10)$$

#### 4. Results and Discussion

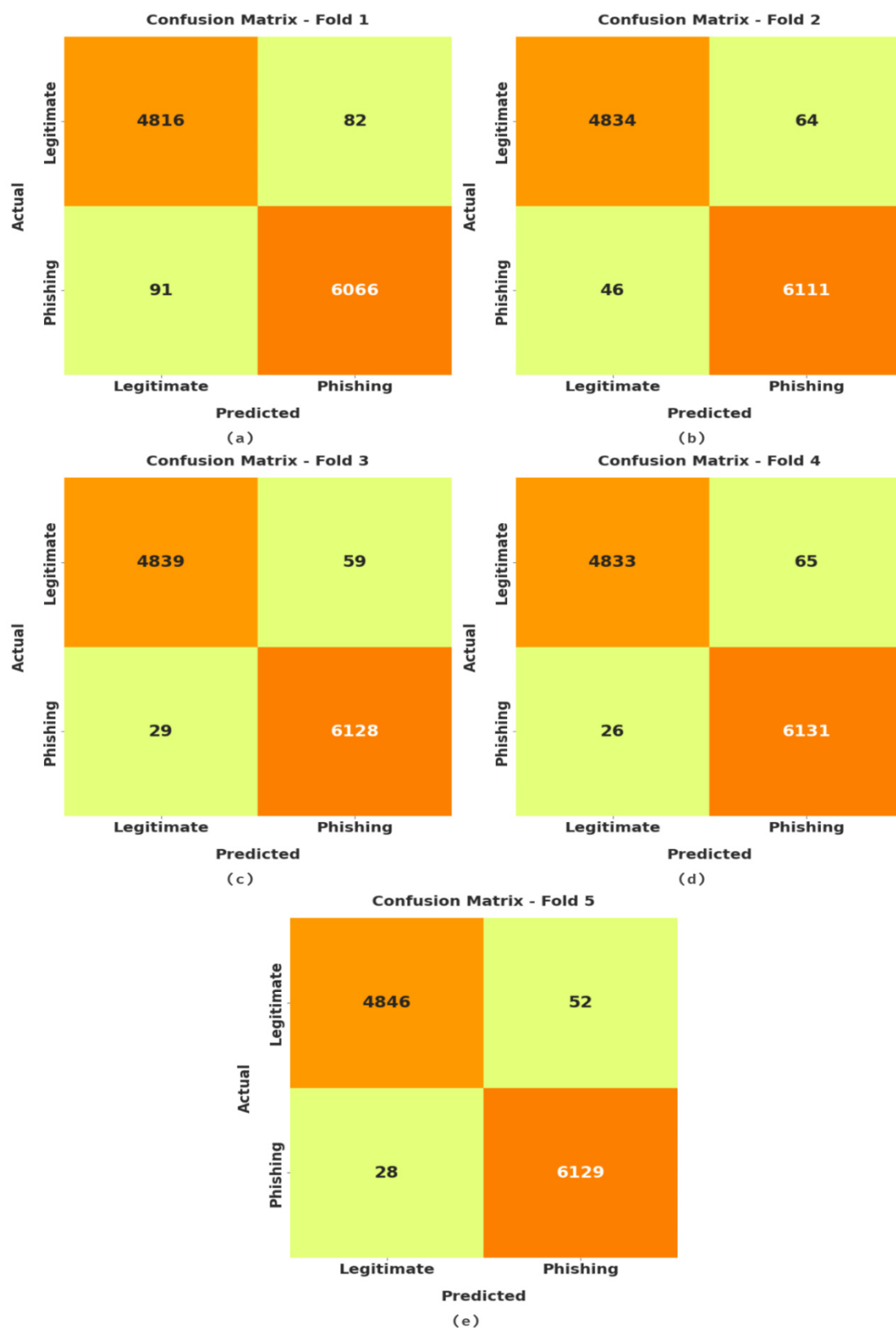
The experimental validation of the ODAE-WPDC model is tested using a dataset from the Kaggle repository [27]. The dataset holds 4898 samples under a legitimate class and 6157 samples under a phishing class as depicted in Table 1. The results are examined in terms of distinct measures, such as accuracy, precision, recall, F-score, and Jaccard index. For effective detection performance, the values of these measures should be high.

**Table 1.** Dataset details.

Class Name	No. of URLs
Legitimate	4898
Phishing	6157
Total Number of URL's	11,055

Figure 3 illustrates the confusion matrices produced by the ODAE-WPDC model under distinct folds. On fold-1, the ODAE-WPDC model recognizes 4816 samples under the legitimate class and 6066 samples under the phishing class. On fold-3, the ODAE-WPDC approach recognizes 4839 samples under the legitimate class and 6128 samples under the phishing class. Additionally, on fold-4, the ODAE-WPDC system recognizes 4833 samples under the legitimate class and 6131 samples under the phishing class. At last, on fold-5, the ODAE-WPDC methodology recognizes 4846 samples under the legitimate class and 6129 samples under the phishing class.





**Figure 3.** Confusion matrices of ODAE-WPDC approach: (a) Fold-1, (b) Fold-2, (c) Fold-3, (d) Fold-4, and (e) Fold-5.

Table 2 and Figure 4 illustrate a brief classification result of the ODAE-WPDC approach under varying folds. The experimental outcomes indicate that the ODAE-WPDC model

has resulted in maximum performance under all folds. For sample, with fold-1, the ODAE-WPDC model offers an average  $accu_y$  of 98.44%,  $prec_n$  of 98.41%,  $reca_l$  of 98.42%,  $F_{score}$  of 98.41%, and  $J_{index}$  of 96.88%. Simultaneously, with fold-2, the ODAE-WPDC approach has an accessible average  $accu_y$  of 99%,  $prec_n$  of 99.01%,  $reca_l$  of 98.97%,  $F_{score}$  of 98.99%, and  $J_{index}$  of 98%. Concurrently, with fold-3, the ODAE-WPDC method has an obtainable average  $accu_y$  of 99.20%,  $prec_n$  of 99.23%,  $reca_l$  of 99.16%,  $F_{score}$  of 99.19%, and  $J_{index}$  of 98.40%. Along with that, with fold-4, the ODAE-WPDC system presents an average  $accu_y$  of 99.18%,  $prec_n$  of 99.21%,  $reca_l$  of 99.13%,  $F_{score}$  of 99.17%, and  $J_{index}$  of 98.34%. At last, with fold-5, the ODAE-WPDC approach has an obtainable average  $accu_y$  of 99.28%,  $prec_n$  of 99.29%,  $reca_l$  of 99.24%,  $F_{score}$  of 99.27%, and  $J_{index}$  of 98.54%.

**Table 2.** Result analysis of ODAE-WPDC approach with various measures and folds.

Class Labels	Accuracy	Precision	Recall	F-Score	Jaccard Index
<b>Fold 1</b>					
legitimate	98.44	98.15	98.33	98.24	96.53
phishing	98.44	98.67	98.52	98.59	97.23
<b>Average</b>	<b>98.44</b>	<b>98.41</b>	<b>98.42</b>	<b>98.41</b>	<b>96.88</b>
<b>Fold 2</b>					
legitimate	99.00	99.06	98.69	98.88	97.78
phishing	99.00	98.96	99.25	99.11	98.23
<b>Average</b>	<b>99.00</b>	<b>99.01</b>	<b>98.97</b>	<b>98.99</b>	<b>98.00</b>
<b>Fold 3</b>					
legitimate	99.20	99.40	98.80	99.10	98.21
phishing	99.20	99.05	99.53	99.29	98.58
<b>Average</b>	<b>99.20</b>	<b>99.23</b>	<b>99.16</b>	<b>99.19</b>	<b>98.40</b>
<b>Fold 4</b>					
legitimate	99.18	99.46	98.67	99.07	98.15
phishing	99.18	98.95	99.58	99.26	98.54
<b>Average</b>	<b>99.18</b>	<b>99.21</b>	<b>99.13</b>	<b>99.17</b>	<b>98.34</b>
<b>Fold 5</b>					
legitimate	99.28	99.43	98.94	99.18	98.38
phishing	99.28	99.16	99.55	99.35	98.71
<b>Average</b>	<b>99.28</b>	<b>99.29</b>	<b>99.24</b>	<b>99.27</b>	<b>98.54</b>

Figure 5 provides an average  $accu_y$  inspection of the ODAE-WPDC methodology under distinct folds. The figure implies that the ODAE-WPDC model has gained effectual outcomes under every fold. For instance, with fold-1, the ODAE-WPDC model has obtained an average  $accu_y$  of 98.44%. Additionally, with fold-2, the ODAE-WPDC approach has reached an average  $accu_y$  of 99%. With fold-3, the ODAE-WPDC system has attained an average  $accu_y$  of 99.20%. In addition, with fold-4, the ODAE-WPDC approach has obtained an average  $accu_y$  of 99.18%. At last, with fold-5, the ODAE-WPDC methodology has gained an average  $accu_y$  of 99.28%.

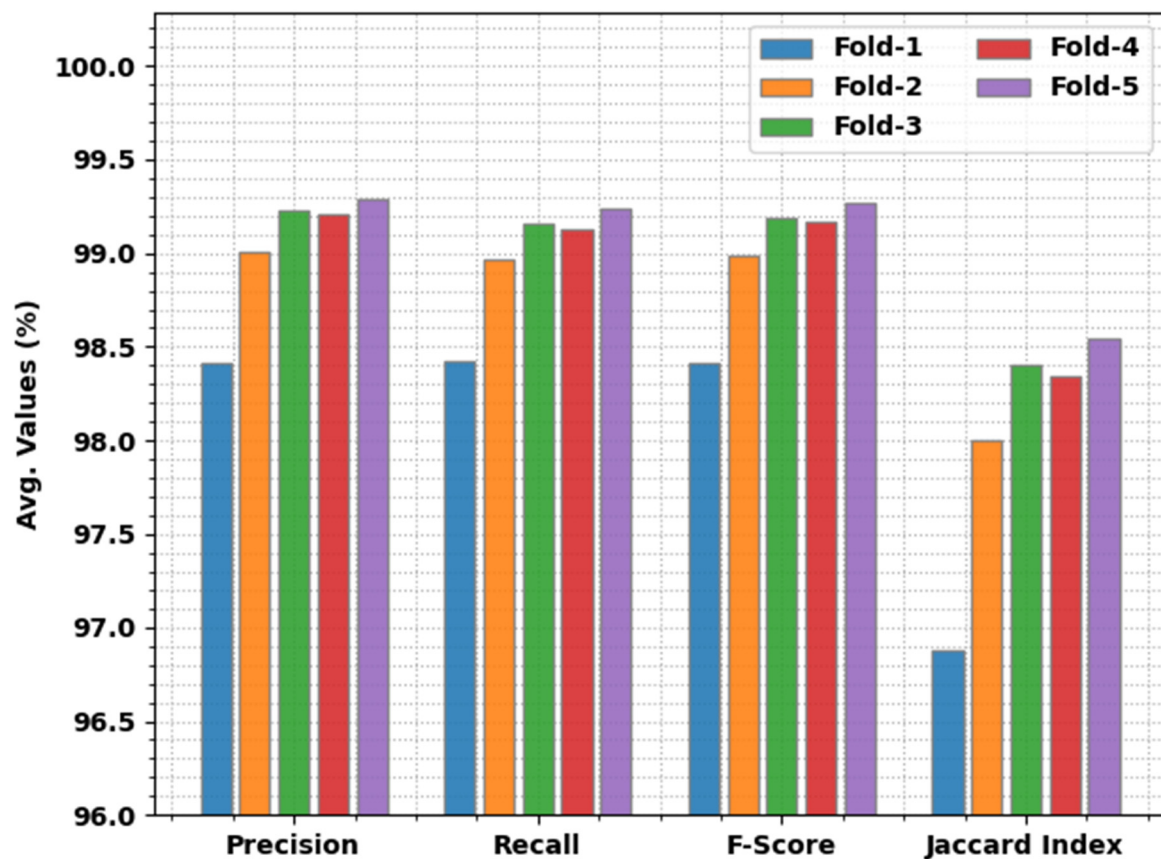


Figure 4. Average analysis of ODAE-WPDC approach with various measures and folds.

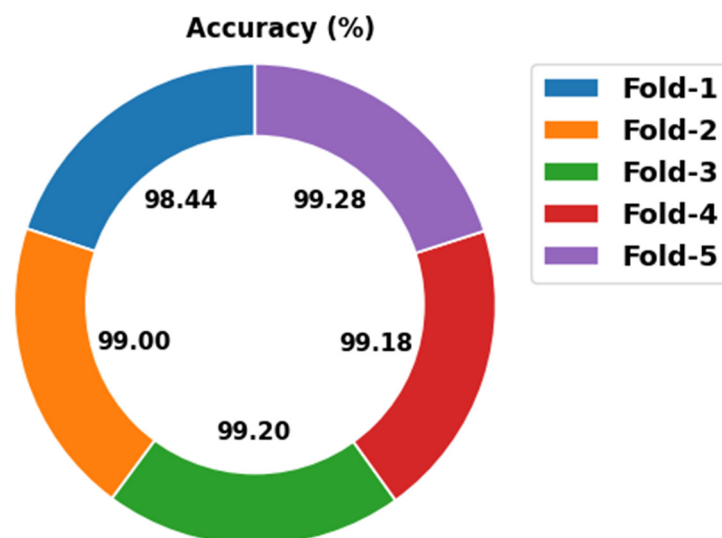
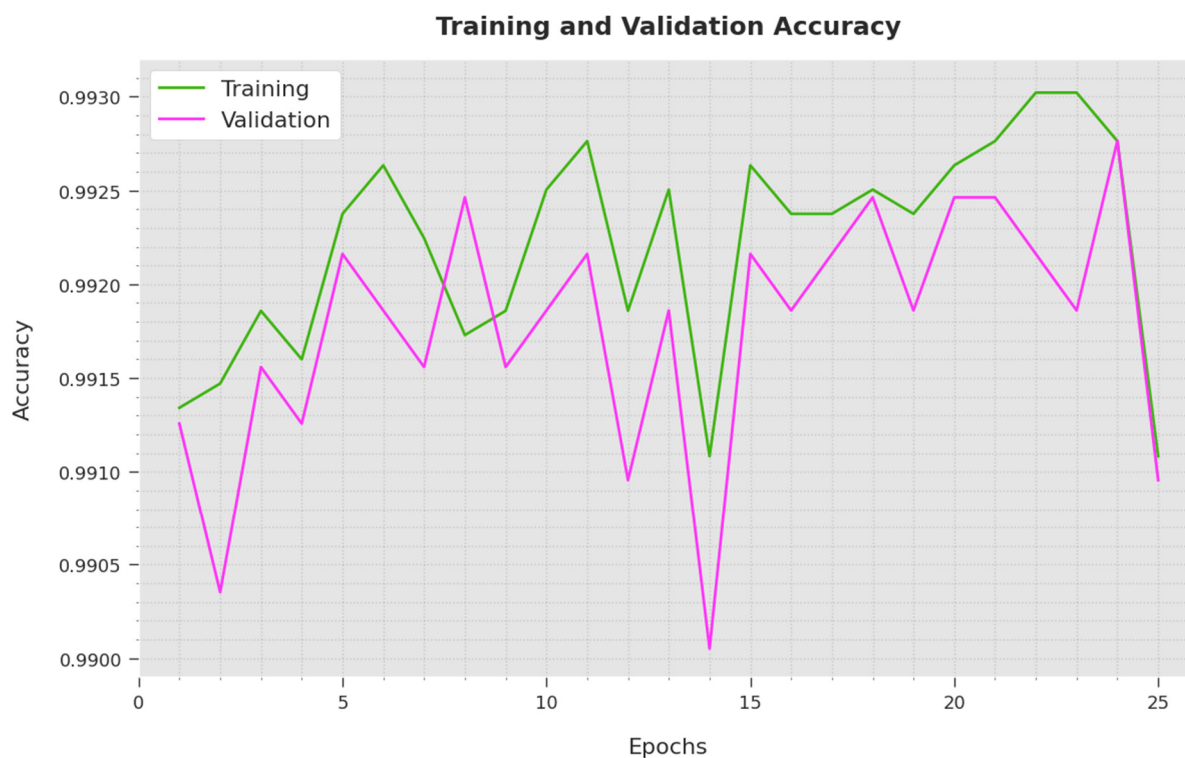


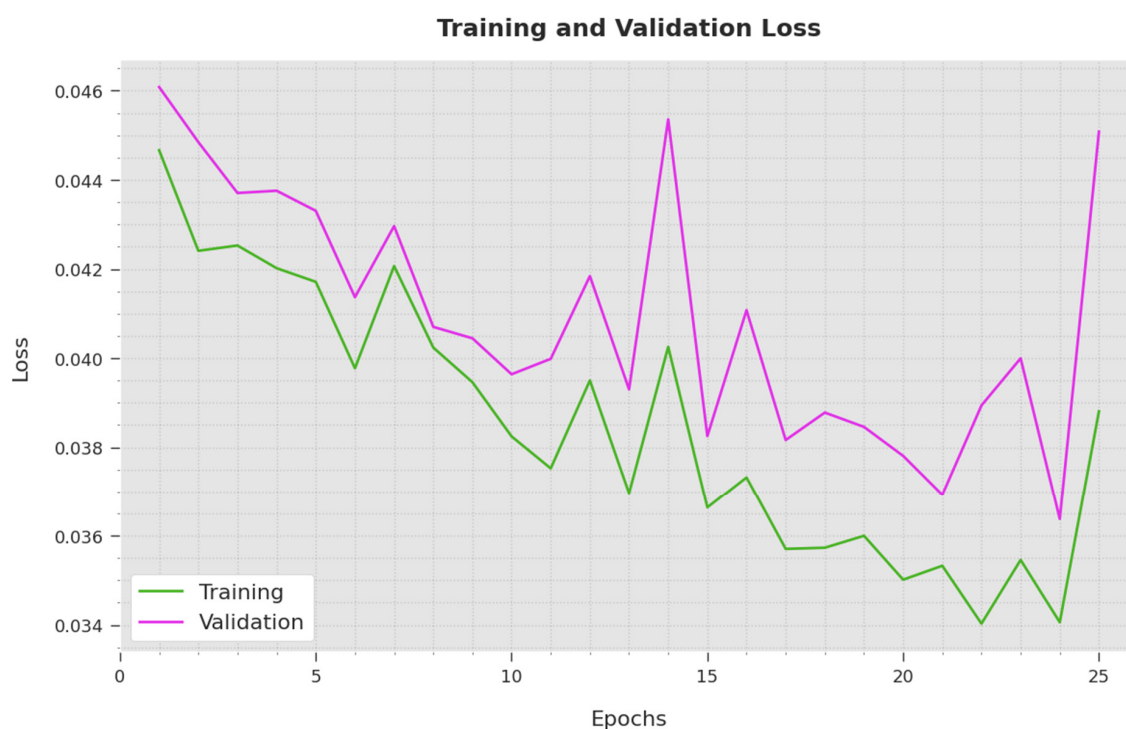
Figure 5. Average accuracy analysis of ODAE-WPDC approach with distinct folds.

The training accuracy (TA) and validation accuracy (VA) attained by the ODAE-WPDC system on test dataset is demonstrated in Figure 6. The experimental outcomes imply that the ODAE-WPDC algorithm has gained maximal values of TA and VA. Specifically, the VA seems to be higher than TA.



**Figure 6.** TA and VA analysis of ODAE-WPDC approach.

The training loss (TL) and validation loss (VL) achieved by the ODAE-WPDC approach on test dataset are established in Figure 7. The experimental outcomes infer that the ODAE-WPDC system has accomplished the least values of TL and VL. Specifically, the VL seems to be lower than TL.



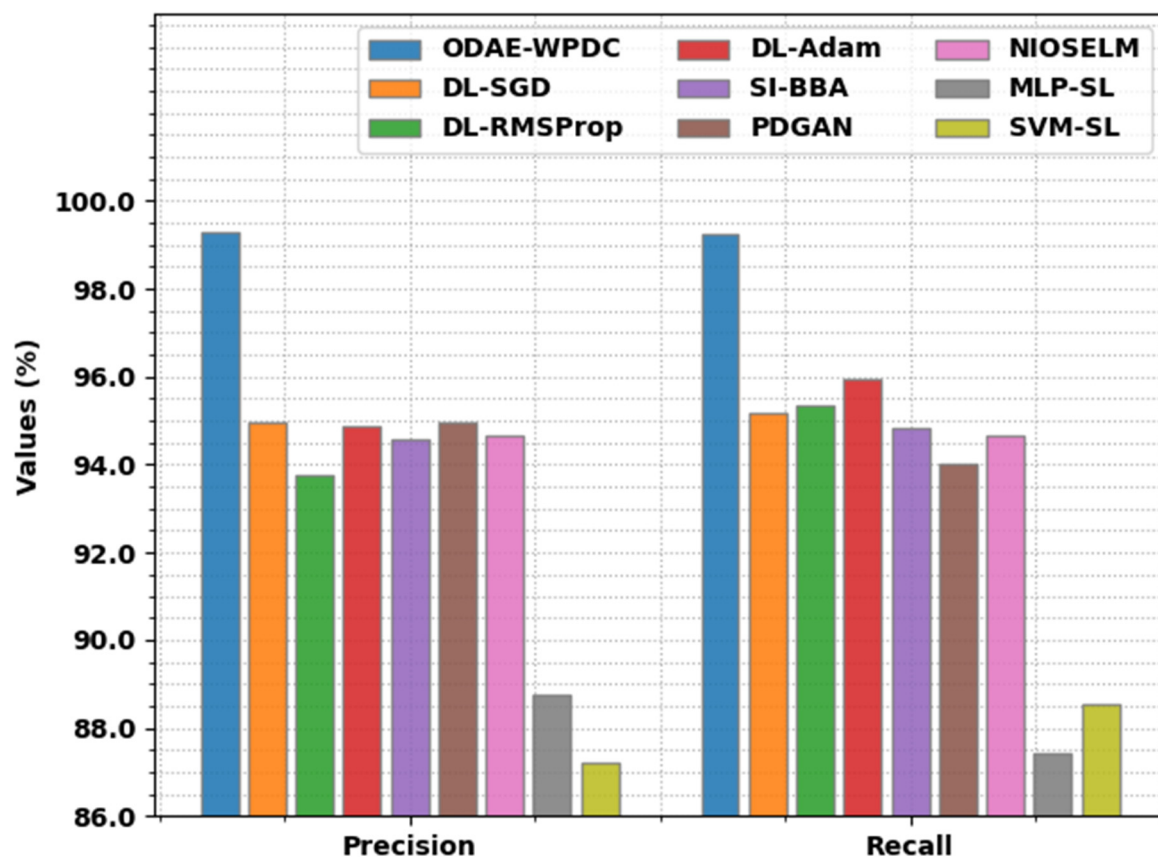
**Figure 7.** TL and VL analysis of ODAE-WPDC approach.

Finally, a detailed comparative study of the algorithm with other algorithms on WS phishing detection is given in Table 3 [28,29]. The experimental findings state that the ODAE-WPDC methodology has gained maximal performance over the other models.

**Table 3.** Comparative analysis of ODAE-WPDC approach with recent algorithms.

Methods	Accuracy	Precision	Recall	F-Score
ODAE-WPDC	99.28	99.29	99.24	99.27
DL-SGD	94.64	94.97	95.17	94.50
DL-RMSProp	92.84	93.77	95.34	95.52
DL-Adam	94.69	94.87	95.93	95.27
SI-BBA	94.93	94.59	94.84	94.78
PDGAN	94.12	94.96	94.02	92.21
NIOSELM	93.40	94.65	94.66	90.86
MLP-SL	87.80	88.75	87.41	74.75
SVM-SL	83.37	87.22	88.54	75.21

Figure 8 illustrates a comparative  $prec_n$  and  $reca_l$  inspection of the ODAE-WPDC system with recent models. The figure implies that the ODAE-WPDC approach has resulted in enhanced performance in terms of  $prec_n$  and  $reca_l$ . With regard to  $prec_n$ , the ODAE-WPDC system has obtained improved  $prec_n$  of 99.29%, whereas the DL-SGD, DL-RMSProp, DL-Adam, SI-BBA, PDGAN, and NIOSELM models have gained  $prec_n$  of 94.97%, 93.77%, 94.87%, 94.59%, 94.96%, and 94.65%, respectively. In addition, in terms of  $reca_l$ , the ODAE-WPDC model has obtained higher  $reca_l$  of 99.24% whereas the DL-SGD, DL-RMSProp, DL-Adam, SI-BBA, PDGAN, and NIOSELM methods have achieved  $reca_l$  of 95.17%, 95.34%, 95.93%, 94.84%, 94.02%, and 94.66%, correspondingly.



**Figure 8.**  $prec_n$  and  $reca_l$  analysis of ODAE-WPDC approach with existing methodologies.



Figure 9 showcases a comparative  $accu_y$  and  $F_{score}$  examination of the ODAE-WPDC methodology with recent techniques. The figure exposes that the ODAE-WPDC system has resulted in enhanced performance with regard to  $accu_y$  and  $F_{score}$ . Interm of  $accu_y$ , the ODAE-WPDC system has obtained enhanced  $accu_y$  of 99.28%, whereas the DL-SGD, DL-RMSProp, DL-Adam, SI-BBA, PDGAN, and NIOSELM algorithms have reached  $accu_y$  of 94.64%, 92.84%, 94.69%, 94.93%, 94.12%, and 93.40%, correspondingly. With regard to  $F_{score}$ , the ODAE-WPDC system has obtained higher  $F_{score}$  of 99.27%, whereas the DL-SGD, DL-RMSProp, DL-Adam, SI-BBA, PDGAN, and NIOSELM systems have reached  $F_{score}$  of 94.50%, 95.52%, 95.27%, 94.78%, 92.21%, and 90.86%, correspondingly.

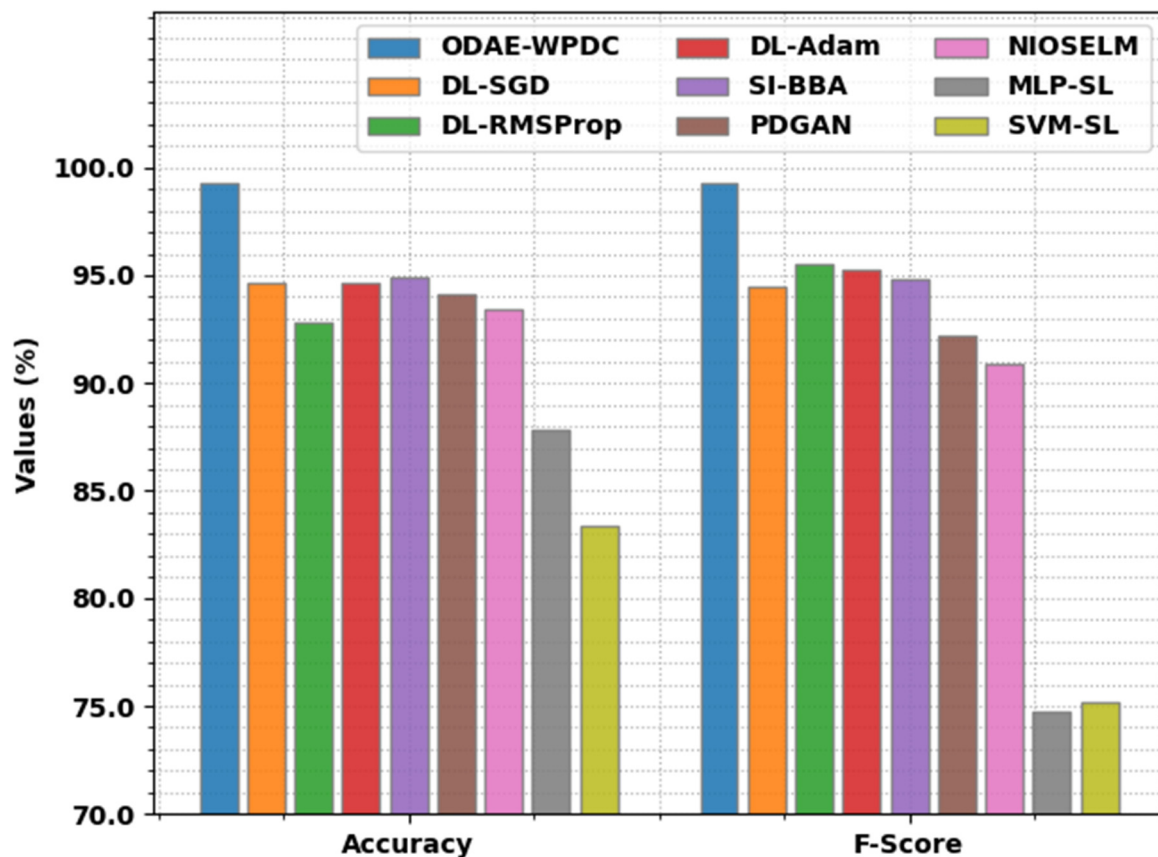


Figure 9.  $Accu_y$  and  $F_{score}$  analysis of ODAE-WPDC approach with existing methodologies.

From the detailed results and discussion, it is clear that the ODAE-WPDC model has shown effectual phishing WS detection and classification performance.

## 5. Conclusions

In this study, a novel ODAE-WPDC model was introduced for the recognition and classification of WS phishing to accomplish cybersecurity. At the primary stage, the proposed ODAE-WPDC model applies input data pre-processing at the initial stage to get rid of missing values in the dataset. This is followed by feature extraction, and the AAA based FS process is utilized. Finally, the IWO with the DAE model is applied for the classification process, where the IWO algorithm assists in attaining maximum outcome. The performance validation of the ODAE-WPDC model is tested utilizing the benchmark Kaggle repository. The experimental findings confirm the better performance of the ODAE-WPDC model over recent DL models. Thus, the presented ODAE-WPDC model can be utilized for security in the digital era. In future, the presented ODAE-WPDC model can be extended to the design of a weighted ensemble voting process.

## 6. Limitations and Future Scope

In future, we would like to verify the performance of the proposed model on other datasets and experiments with more novel features and their influence. A major drawback of our model is that it cannot identify whether the URL is active or not; therefore, it is essential to verify whether the URL is active or not before detection for ensuring the detection performance. At the same time, the computational complexity of the proposed model can be analyzed in future. Additionally, few attackers utilize URLs that are not impersonations of other websites, and such URLs will not be identified. In addition, the robust nature of the proposed model can be tested against adversarial attacks which are commonly utilized by malicious parties. In the future, we plan to exploit novel models for automatic extraction of other features to detect phishing sites, such as web code features, web text features, and web icon features.

**Author Contributions:** Conceptualization, H.A.; Investigation, S.S.A. and M.M.; Methodology, H.A. and S.S.A.; Project administration, M.A.D.; Resources, F.S.A.; Software, F.S.A., I.A.-T. and M.M.; Supervision, I.A.-T.; Validation, K.A.A. and A.S.A.A.; Writing—original draft, H.A., K.A.A. and A.S.A.A.; Writing—review & editing, K.A.A., A.S.A.A. and M.A.D. All authors have read and agreed to the published version of the manuscript.

**Funding:** The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Large Groups Project under grant number (61/43). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R319), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (22UQU4210118DSR09).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Data sharing not applicable to this article as no datasets were generated during the current study.

**Conflicts of Interest:** The authors declare that they have no conflict of interest. The manuscript was written with contributions of all authors. All authors have approved the final version of the manuscript.

**Ethics Approval:** This article does not contain any studies with human participants performed by any of the authors.

## References

1. Shahrivari, V.; Darabi, M.M.; Izadi, M. Phishing Detection Using Machine Learning Techniques. *arXiv* **2020**, arXiv:2009.11116.
2. Al-Qarafi, A.; Alrowais, F.; Alotaibi, S.S.; Nemri, N.; Al-Wesabi, F.N.; Al Duhayyim, M.; Marzouk, R.; Othman, M.; Al-Shabi, M. Optimal Machine Learning Based Privacy Preserving Blockchain Assisted Internet of Things with Smart Cities Environment. *Appl. Sci.* **2022**, *12*, 5893. [\[CrossRef\]](#)
3. Crawford, M.; Khoshgoftar, T.M.; Prusa, J.D.; Richter, A.N.; Al Najada, H. Survey of review spam detection using machine learning techniques. *J. Big Data* **2015**, *2*, 23. [\[CrossRef\]](#)
4. Nugraha, A.F.; Tama, D.A.; Istiqomah, D.A.; Ramadhani, S.T.A.; Kusuma, B.N.; Windarni, V.A. Feature Selection Technique for improving classification performance in the web-phishing detection process. *Conf. Ser.* **2022**, *4*, 25–31. [\[CrossRef\]](#)
5. Varshney, G.; Misra, M.; Atrey, P.K. A survey and classification of web phishing detection schemes. *Secur. Commun. Netw.* **2016**, *9*, 6266–6284. [\[CrossRef\]](#)
6. Adebowale, M.A.; Lwin, K.T.; Hossain, M.A. Intelligent phishing detection scheme using deep learning algorithms. *J. Enterp. Inf. Manag.* **2020**. [\[CrossRef\]](#)
7. Jain, A.K.; Gupta, B.B. A machine learning based approach for phishing detection using hyperlinks information. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 2015–2028. [\[CrossRef\]](#)
8. Alam, T.M.; Shaukat, K.; Hameed, I.A.; Khan, W.A.; Sarwar, M.U.; Iqbal, F.; Luo, S. A novel framework for prognostic factors identification of malignant mesothelioma through association rule mining. *Biomed. Signal Process. Control.* **2021**, *68*, 102726. [\[CrossRef\]](#)
9. Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Chen, S.; Liu, D.; Li, J. Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies* **2020**, *13*, 2509. [\[CrossRef\]](#)

10. Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Xu, M. A survey on machine learning techniques for cyber security in the last decade. *IEEE Access* **2020**, *8*, 222310–222354. [\[CrossRef\]](#)
11. Yi, P.; Guan, Y.; Zou, F.; Yao, Y.; Wang, W.; Zhu, T. Web phishing detection using a deep learning framework. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 4678746. [\[CrossRef\]](#)
12. Wei, W.; Ke, Q.; Nowak, J.; Korytkowski, M.; Scherer, R.; Woźniak, M. Accurate and fast URL phishing detector: A convolutional neural network approach. *Comput. Netw.* **2020**, *178*, 107275. [\[CrossRef\]](#)
13. Do, N.Q.; Selamat, A.; Krejcar, O.; Herrera-Viedma, E.; Fujita, H. Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions. *IEEE Access* **2022**. [\[CrossRef\]](#)
14. Lakshmi, L.; Reddy, M.P.; Santhaiah, C.; Reddy, U.J. Smart phishing detection in web pages using supervised deep learning classification and optimization technique adam. *Wirel. Pers. Commun.* **2021**, *118*, 3549–3564. [\[CrossRef\]](#)
15. Odeh, A.; Keshta, I.; Abdelfattah, E. Machine learning techniques for detection of website phishing: A review for promises and challenges. In Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 27–30 January 2021; pp. 0813–0818.
16. Makkar, A.; Kumar, N. An efficient deep learning-based scheme for web spam detection in IoT environment. *Future Gener. Comput. Syst.* **2020**, *108*, 467–487. [\[CrossRef\]](#)
17. Sahingoz, O.K.; Buber, E.; Demir, O.; Diri, B. Machine learning based phishing detection from URLs. *Expert Syst. Appl.* **2019**, *117*, 345–357. [\[CrossRef\]](#)
18. Lee, J.; Ye, P.; Liu, R.; Divakaran, D.M.; Chan, M.C. Building robust phishing detection system: An empirical analysis. *NDSS MADWeb* 2020. [\[CrossRef\]](#)
19. Ghaleb, F.A.; Alsaedi, M.; Saeed, F.; Ahmad, J.; Alasl, M. Cyber Threat Intelligence-Based Malicious URL Detection Model Using Ensemble Learning. *Sensors* **2022**, *22*, 3373.
20. Kondracki, B.; Azad, B.A.; Starov, O.; Nikiforakis, N. Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security 2021, Virtual Event, Korea, 15–19 November 2021; pp. 36–50.
21. Noah, N.; Tayachew, A.; Ryan, S.; Das, S. Poster: PhisherCop-An Automated Tool Using ML Classifiers for Phishing Detection. In Proceedings of the 43rd IEEE Symposium on Security and Privacy (IEEE S&P 2022), San Francisco, CA, USA, 23–26 May 2022.
22. Zhang, P.; Oest, A.; Cho, H.; Sun, Z.; Johnson, R.C.; Wardman, B.; Sarker, S.; Kapravelos, A.; Bao, T.; Wang, R.; et al. Crawlphish: Large-scale analysis of client-side cloaking techniques in phishing. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24–27 May 2021; pp. 1109–1124.
23. Uymaz, S.A.; Tezel, G.; Yel, E. Artificial algae algorithm (AAA) for nonlinear global optimization. *Appl. Soft Comput.* **2015**, *31*, 153–171. [\[CrossRef\]](#)
24. Kocer, H.G.; Uymaz, S.A. A Modified Artificial Algae Algorithm For Large Scale Global Optimization Problems. *Int. J. Intell. Syst. Appl. Eng.* **2018**, *6*, 306–310. [\[CrossRef\]](#)
25. Raja, P.S. Brain tumor classification using a hybrid deep autoencoder with Bayesian fuzzy clustering-based segmentation approach. *Biocybern. Biomed. Eng.* **2020**, *40*, 440–453. [\[CrossRef\]](#)
26. Srinivas, S.T.P. Application of improved invasive weed optimization technique for optimally setting directional overcurrent relays in power systems. *Appl. Soft Comput.* **2019**, *79*, 1–13.
27. Available online: <https://www.kaggle.com/akashkr/phishing-url-eda-and-modelling/data> (accessed on 12 March 2022).
28. Rendall, K.; Nisioti, A.; Mylonas, A. Towards a multi-layered phishing detection. *Sensors* **2020**, *20*, 4540. [\[CrossRef\]](#) [\[PubMed\]](#)
29. Kumar, P.P.; Jaya, T.; Rajendran, V. SI-BBA—A novel phishing website detection based on Swarm intelligence with deep learning. *Mater. Today Proc.* 2021, *in press*.