


# Malicious Uniform Resource Locator Detection Using Wolf Optimization Algorithm and Random Forest Classifier



Kayode S. Adewole , Muiz O. Raheem, Oluwakemi C. Abikoye, Adeleke R. Ajiboye, Tinuke O. Oladele, Muhammed K. Jimoh, and Dayo R. Aremu

**Abstract** Within the multitude of security challenges facing the online community, malicious websites play a critical role in today's cybersecurity threats. Malicious URLs can be delivered to users via emails, text messages, pop-ups or advertisements. To recognize these malicious websites, blacklisting services have been created by the web security community. This method has been proven to be inefficient. This chapter proposed meta-heuristic optimization method for malicious URLs detection based on genetic algorithm (GA) and wolf optimization algorithm (WOA). Support vector machine (SVM) as well as random forest (RF) were used for classification of phishing web pages. Experimental results show that WOA reduced model complexity with comparable classification results without feature subset selection. RF classifier outperforms SVM based on the evaluation conducted. RF model without feature selection produced accuracy and ROC of 0.972 and 0.993, respectively, while RF model that is based on WOA optimization algorithm produced accuracy of 0.944 and ROC of 0.987. Hence, in view of the experiments conducted using two well-known phishing datasets, this research shows that WOA can produce promising results for phishing URLs detection task.

---

K. S. Adewole (✉) · M. O. Raheem · O. C. Abikoye · A. R. Ajiboye · T. O. Oladele · D. R. Aremu  
Department of Computer Science, University of Ilorin, Ilorin, Nigeria  
e-mail: [adewole.ks@unilorin.edu.ng](mailto:adewole.ks@unilorin.edu.ng)

M. O. Raheem  
e-mail: [raheem069.mo@gmail.com](mailto:raheem069.mo@gmail.com)

O. C. Abikoye  
e-mail: [abikoye.o@unilorin.edu.ng](mailto:abikoye.o@unilorin.edu.ng)

A. R. Ajiboye  
e-mail: [ajibabdulraheem@gmail.com](mailto:ajibabdulraheem@gmail.com)

T. O. Oladele  
e-mail: [tinuoladele@gmail.com](mailto:tinuoladele@gmail.com)

D. R. Aremu  
e-mail: [draremu2006@gmail.com](mailto:draremu2006@gmail.com)

M. K. Jimoh  
Department of Educational Technology, University of Ilorin, Ilorin, Nigeria  
e-mail: [jimoh.km@unilorin.edu.ng](mailto:jimoh.km@unilorin.edu.ng)

**Keywords** Phishing detection · Meta-heuristic · Genetic algorithm · Wolf optimization · Machine learning

## 1 Introduction

The significance of the world wide web (WWW) has constantly been expanding. These days the internet is an integral part of everybody’s daily activities and has contributed tremendously in information sharing across the globe. Technology grows with huge speed, which makes the user to utilize it in a smarter way. As technology advances, motives for usage also grow vastly. Numerous attacks are exhibited over the network; one of them is phishing in which the attacker impersonates himself as genuine to hijack the user’s credentials. Unfortunately, technological advancement combined with new sophisticated attack has increased tremendously and the number of victims is growing [1]. Such attack incorporates rogue websites that sell fake products, monetary extortion by deceiving users into uncovering delicate information, which inevitably leads to stealing of money or personality, or notwithstanding introducing malicious software on the network. There exist a broad range of methods for carrying out such assaults; for instance, social engineering, drive-by exploits, watering hole, phishing, SQL injection, man-in-the-middle, loss/theft of gadgets, denial of service and many others [2]. To engage in phishing attack, attacker can disguise uniform resource locator (URL) to appear as legitimate to the visitors of the website.

Resources and other documents on the web are accessed through URLs. URL is the worldwide location with two major elements: the protocol identifier and the resource name. The protocol identifier represents the protocol used to access the web resource, while resource name depicts the domain name or IP address where the web resource is located. These two components are separated with a colon and double forward slashes, as shown in Fig. 1.

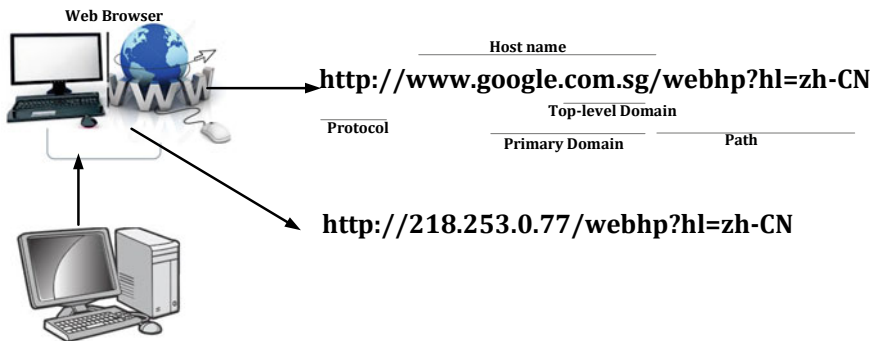


Fig. 1 Sample URL [2]

Malicious URLs have turned into a typical means to encourage cybercrimes, which include drive-by-download and spamming. Numerous attackers endeavour to utilize malicious sites to distribute malicious projects or compromise users' data. According to Kaspersky Lab, there has been increase in browser-based attacks in 2012 ranging between 946,393,693 and 1,595,587,670. However, 87.36% of these attacks were utilized maliciously. The Anti-Phishing Working Group additionally states that phishing attacks that make use of malicious links expanded from 93,462 to 123,486 during the second half of the year 2012. It has been observed by Lin et al. [3] that out of the millions of URLs utilized every day, malicious URLs are short-lived so as to avoid blacklist-based detection. Early detection method for malicious URLs utilized blacklist-based approach. This approach depends heavily on repositories of already categorized web pages. Blacklist-based method has the problem of generality owing to the fact that any URL that is not listed in the repositories might not be detected [4]. Conversely, machine learning methods have played significant roles and have also been used to build intelligent frameworks that distinguish malicious web pages from genuine ones. For example, Gupta [5] used pattern matching algorithm with word segmentation to pinpoint malicious web pages. Naïve Bayes and sequential minimal optimization (SMO) approach have been studied in the work of Aydin and Baykal [6]. Li et al. [7] proposed supervised boosting decision tree approach to detect phishing URL. Wang et al. [8] proposed a hybrid classification approach based on static and dynamic analyses for malicious website detection and Adewole et al. [9] discovered the possibility of phishing detection using hybrid rule-based method through a combination of two commonly used rule induction algorithms: JRip and Projective Adaptive Resonance Theory (PART). Notwithstanding, numerous researches have employed machine learning to deploy intelligent frameworks for malicious URLs detection, however, employing meta-heuristics approach with classification techniques to build a more accurate system to efficiently detect malicious web pages still remains an open research issue. Therefore, this chapter investigates the performance of two meta-heuristic optimization algorithms based on genetic algorithm (GA) and wolf optimization algorithm (WOA). Support vector machine (SVM) and random forest (RF) algorithms have been used as classifiers to evaluate the performance of the features selected from the two meta-heuristic algorithms. These algorithms were selected in this study based on their outstanding performances as reported in the literatures [6, 15, 16, 20].

The subsequent sections are arranged as follows: Sect. 2 focuses on related studies on malicious URLs detection, Sect. 3 discusses the methodology of the proposed framework and Sect. 4 presents the results of the various experiments conducted in this study. The last section, Sect. 5 concludes the chapter and presents the future direction of the study.

## 2 Related Works

Several studies have been conducted to detect malicious websites. This section discusses related studies on malicious URLs detection. For instance, Xuan and Yongzhen [10] developed malicious URLs detection system using two-dimensional barcodes and hash function. In their approach, the researchers extracted eigenvalues of malicious and benign links. The system generates black and white list library for the URLs extracted. Based on the match rules produced, the authors presented safety tips for users in accordance with these rules.

Lexicon-based approach has been studied in the literature to detect malicious websites. For instance, Darling et al. [11] employed lexical analysis of URLs to categorize websites according to the level of maliciousness. The main idea is to identify the classification model based on lexical analysis that could be employed in real time to detect malicious URLs. In addition, Lee and Kim [12] focused on detection of malicious URLs in a twitter data stream. Authors concentrated on discovering frequently distributed URLs to uncover the deviousness of associated link redirect chains. Tweets from Twitter timeline were experimented upon to develop a classification model for phishing URLs detection. Experimental result reveals that the classification approach was capable of accurately identifying suspicious links in a tweet. Gupta [5] employed algorithm for pattern matching on word segmentation to pinpoint phishing URL. Naïve Bayes and SMO approach have been studied in the work of Aydin and Baykal [6]. Li et al. [7] developed supervised boosting decision tree method to detect phishing URL. Wang et al. [8] proposed a hybrid classification approach based on static and dynamic analyses for malicious website detection.

Also, models for spam message and spam account detection on Twitter have been studied extensively in the literature [13]. In addition, Bhardwaj, Sharma and Pandit [14] proposed artificial bee colony algorithm for identifying malicious links on the web. Furthermore, a study carried out by Adewole et al. [9] applied a hybrid rule-based technique to identify malicious URLs. The research showed that PART algorithm is superior to JRip when deployed for phishing URLs detection task. Thus, their study concluded that the hybrid rule induction method that combined the rules generated from the two induction algorithms performed better than both PART and JRip in terms of accuracy.

Babagoli et al. [18] proposed a method for phishing website detection that utilizes meta-heuristic-based nonlinear regression algorithm coupled with feature selection technique. The authors evaluated the proposed approach using dataset that comprises 11055 phishing and legitimate web pages. Twenty (20) features were focused on to build the phishing detection system. Sohrabi and Karimi [19] proposed spam comments detection model from Facebook social network. Sahingoz et al. [20] proposed natural language processing (NLP) features to train classification algorithm for real-time anti-phishing detection system. Seven classification algorithms were used to evaluate the performance of the NLP-based features. The study observed that RF algorithm produced the best result with an accuracy of 97.98% for phishing URLs detection.

Although a number of machine learning models have been investigated to detect phishing URLs, however, investigation based on WOA and GA for feature optimization with SVM and RF classifiers is the main focus of this research.

### 3 Methodology

This section discusses the methodology employed to build the proposed model for phishing URL detection. It describes the approach for data collection as well as the optimization algorithms that were used for features optimization. Summarily, Fig. 2

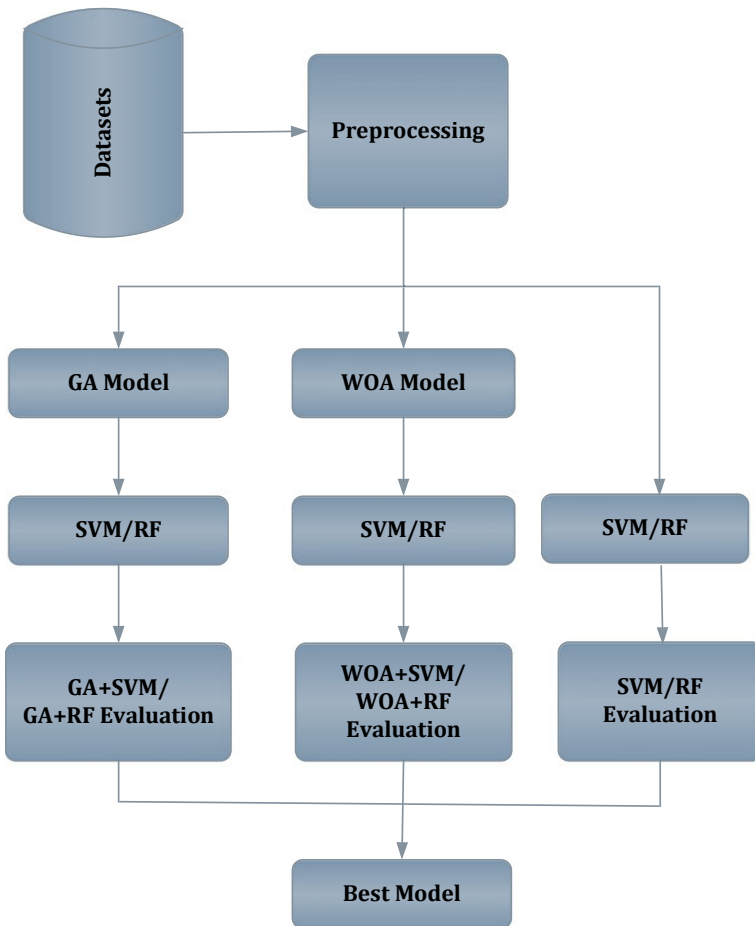


Fig. 2 Proposed framework for phishing URLs detection

**Table 1** Description of the two datasets utilized in the study

Dataset name	No. of features	Attributes characteristics	No. of instances	Class distribution
Dataset1	10	Integer	1,353	Malicious (702), genuine (548), suspicious(103)
Dataset2	30	Integer	11,055	Malicious (4898), genuine (6157)

shows the proposed framework in this study to detect malicious web pages. The subsequent sections highlight the components of the proposed framework and the techniques deployed to achieve them.

### ***3.1 Method of Data Collection and Preparation***

This study examined two publicly available datasets for malicious URLs detection. The datasets were obtained from UCI machine learning repository. First dataset, henceforth referred to as Dataset1, is accessible at '<https://archive.ics.uci.edu/ml/machine-learning-databases/00379/>', which has a total of 1,353 URLs instances. This dataset has ten (10) attributes for analysis. The second dataset, henceforth referred to as Dataset2, is accessible at '<https://archive.ics.uci.edu/ml/machine-learning-databases/00327/>', which has a total of 11,055 URLs instances. This dataset has 30 attributes for analysis. Table 1 depicts the composition of these datasets. Detailed reports of the various features in the datasets can be found in [9].

### ***3.2 Feature Subset Selection***

Feature selection, as a data preprocessing approach, has been proven to be powerful and efficient in the preparation of data with high dimensionality for various data mining and machine learning issues. The goals of feature selection include constructing less complicated and more comprehensible models, enhancing machine mining model performance, and preparing clean and understandable data of high quality. In order to select a subset of features of high quality from the two datasets considered in this study, two meta-heuristic optimization algorithms were studied, which are GA and WOA algorithms. The subsequent sections discussed the two algorithms in detail.

### 3.3 Meta-Heuristics Algorithms

As discussed in the previous sections, this study investigated two meta-heuristic algorithms: GA and WOA based on their optimal performance as testified in the literature.

**Genetic Algorithm.** GA is a meta-heuristic search algorithm inspired by Charles Darwin's theory of natural evolution. Its operation mimics the natural selection process and the algorithm has gained wider usage for solving optimization problems over the years. GA selects fittest individuals for reproduction so as to yield offspring of the next generation. The algorithm terminates if it does not produce offspring that are significantly different from the previous generation. This means that the population has converged on this iteration and a set of solutions to the problem has been identified. In relation to feature subset selection, GA searches the best combination of features that will provide improved results in the solution space. GA has several stages which are demonstrated in Algorithm 1.

---

#### Algorithm1: Genetic Algorithm

---

**[Start]** Generate random population of  $n$  chromosomes (appropriate solutions for the problem)

**[Fitness]** Calculate the fitness  $f(x)$  of all chromosome  $x$  in the population

**[New population]** Generate a new population by reiterating the subsequent phases till the new population is complete

**[Selection]** Select two parent chromosomes from a population according to their fitness (the better fitness, the more chance to be selected)

**[Crossover]** With a crossover, probability crosses over the parents to form a new offspring (children). If no crossover was achieved, offspring is an exact copy of parents.

**[Mutation]** With a mutation, probability mutates a new offspring at each locus (position in chromosome).

**[Accepting]** Place new offspring in a new population

**[Replace]** Use new generated population for a further run of algorithm

**[Test]** If the end condition is satisfied, **stop**, and return the best solution in current population

**[Loop]** Go to step **[Fitness]**

---

**Wolf Optimization Algorithm.** The wolf optimization algorithm (WOA) is one of the bio-inspired meta-heuristics algorithms based on wolf preying behaviour. One of its distinguishing characteristics is the concurrent possession of individual local search capability as well as flocking movement [15]. Therefore, the individual wolf in WOA searches autonomously by memorizing its particular attribute and unites with its peer when the peer is in a better location. Using this approach, long-range inter-communication amongst the wolves that characterize the searching points for candidate solutions is removed since wolves stalk their target in stillness. Also,

the swarming behaviour of WOA, unlike most bio-inspired algorithms, is delegated to each individual wolf rather than to a single leader, as opposed particle swarm optimization and Firefly. WOA operates as if there are multiple leaders swarming from different directions to the best solution, instead of one direction for optimum solution by a single flock. WOA is summarized in Algorithm 2.

---

**Algorithm 2: Wolf Optimization Algorithm**

---

Objective function  $f(x)$ ,  $x=(x_1, x_2, \dots, x_d)^T$   
 Initialize the population of wolves,  $x_i(i=1, 2, \dots, W)$   
 Define and initialize parameters:  
 $r$  = radius of the visual range  
 $s$  = step size by which a wolf moves at a time  
 $\alpha$  = velocity factor of wolf  
 $p_a$  = a user-defined threshold [0..1], it defines how commonly an enemy appears  
 WHILE ( $t < \text{generations}$  && *stopping criteria not met*)  
   FOR  $i = 1 : W$   
     Prey\_new\_food\_initiatively();  
     Generate\_new\_location();  
     //Check whether the next location suggested by the random generator is new.  
     Otherwise, repeat generating random location.  
     IF( $\text{dist}(x_i, x_j) < r$  &&  $x_j$  is better as  $f(x_i) < f(x_j)$ )  
       ELSE IF  
          $x_i = \text{prey\_new\_food\_passively}()$ ;  
       END IF  
       Generate\_new\_location();  
       IF( $\text{rand}() > p_a$ )  
          $x_i = x_i + \text{rand}() + v$ ; // escape to a new position.  
       END IF  
     END FOR  
 END WHILE

---

### 3.4 Classification

In order to separate phishing website from legitimates ones, two classification algorithms were employed based on SVM and random forest (RF). These algorithms have been widely used in security domain and have shown significant classification performance [4, 13]. The classifiers take as input a dataset containing the class of each piece of data instance to enable the computer to learn the pattern that exists among the instances in the dataset. This pattern is then used to predict the class of new data samples. In this study, the target attribute of the Dataset1 is divided into three categories: malicious, suspicious and genuine. In the case of Dataset2, the target attribute is binary in nature, which involves malicious and genuine cases. Therefore, the goal of each classifier is to extract pattern that reveals the specific group or class each data instance is related within a given dataset.



**Support Vector Machine.** Support vector machine (SVM) is one of the most popular classifiers that has been employed in several domains. SVM utilizes ‘kernel trick’ approach to solve a nonlinearly separable problem through mapping of points into a higher-dimensional space. SVM solves the issues of overfitting that are inherent in some learning algorithms. The main idea of SVM is to compute the optimal separating hyperplane between the classes in the dataset by maximizing the margin between the classes’ closest points. The maximum margin hyperplane is the one that provides the highest separation between the classes considered. In two-dimensional space, this hyperplane is a line that divides a plane into two distinctive parts corresponding to the classes in a binary classification task. SVM can solve both classification and regression tasks and can handle several types of variables. The separating hyperplanes can be defined as:

$$w_i x_i + b \geq +1, \text{ when } y_i = +1 \tag{1}$$

$$w_i x_i + b \leq -1, \text{ when } y_i = -1 \tag{2}$$

where  $w$  is the weight,  $x$  is the input,  $y$  is the output and  $b$  is bias.

**Random Forest.** Random forest (RF) is a type of decision tree algorithms that are based on ensemble technique. RF produces an ensemble of classifiers based on different decision trees using random feature selection and bagging technique during the training phase. The decision tree generates two categories of nodes, namely, the leaf node labelled as a class and the interior node represented with a feature. During training phase, a diverse subset of training samples is chosen with a replacement to train each decision tree. Entropy is applied to compute the information gain contributed by each feature. Let  $D$  represents the dataset with the labelled instances and  $C$  as the class such that  $C = \{C_1, C_2, C_3, \dots, C_j\}$ , where  $j$  is the number of classes considered. In this study, the value of  $j$  is set to 2 or 3 depending on the specific dataset used as earlier discussed. Thus, the information needed to identify the class of an instance in the dataset  $D$  is denoted as  $Info(D) = Entropy(P)$ , where  $P$  is the class probability distribution such that:

$$P = \left\{ \frac{|C1|}{|D|}, \frac{|C2|}{|D|}, \frac{|C3|}{|D|}, \dots, \frac{|Cj|}{|D|} \right\} \tag{3}$$

By partitioning  $D$  based on the value of a feature  $F$  according to subsets  $\{D_1, D_2, D_3, \dots, D_n\}$ ,  $Info(F,D)$  according to  $F$  is computed as:

$$Info(F, D) = \sum_{i=1}^n \frac{|D_i|}{|D|} Info(D_i) \tag{4}$$

The corresponding information gain after obtaining the value of  $F$  is computed as:

$$\text{Gain}(F, D) = \text{Info}(D) - \text{Info}(F, D) \quad (5)$$

Then the *GainRatio* is defined as:

$$\text{GainRatio}(F, D) = \frac{\text{Gain}(F, D)}{\text{SplitInfo}(F, D)} \quad (6)$$

where *SplitInfo*( $F, D$ ) denotes the information due to the splitting of  $D$  according to the feature  $F$ . Random forest uses the majority voting of all the individual decisions to obtain the final decision of the classifier [1].

### 3.5 Cross-Validation

Cross-validation is a statistical technique that divides data into two parts: one used to train a model and the other used to validate the model. This method is to evaluate and compare learning algorithms [17]. Cross-validation process uses a single parameter called  $k$ . The parameter represents the number of partitions in which a given dataset can be divided. Based on this, the process is frequently called  $k$ -fold cross-validation. For instance,  $k = 10$  becomes 10-fold cross-validation. In this study, 10-fold cross-validation method is used to train the proposed models because this approach has been widely accepted in the literature to avoid model overfitting and to produce better transparent model for phishing web page detection.

### 3.6 Evaluation Metric

Evaluation metrics are the methods used in determining the performance of machine learning models. For this research, the models were evaluated using parameters such as accuracy, sensitivity (recall), specificity, precision, F-measure and receiver operating characteristics (ROC). These metrics are briefly discussed as follows:

- i. Accuracy: This is the fraction of predictions that the model gets right. Mathematically, accuracy can be calculated by:

$$\text{Accuracy} = \frac{t_p + t_n}{t_p + t_n + f_p + f_n} \quad (7)$$

- ii. Sensitivity: Sensitivity is a measure of the proportion of actual positive cases that got predicted as positive or (true positive). Sensitivity is also termed as Recall. Therefore, in this case, it refers to the model ability to detect phishing URL correctly. Mathematically, sensitivity is calculated by:

$$\text{Sensitivity} = \frac{t_p}{t_p + f_n} \quad (8)$$

- iii. **Specificity:** This is defined as the proportion of actual negatives, which got predicted as the negative (or true negative). In essence, specificity measures the model ability to correctly detect web pages that are actually legitimate (i.e. not phishing web pages). It can be calculated mathematically by:

$$\text{Specificity} = \frac{t_n}{t_n + f_p} \quad (9)$$

- iv. **Precision:** This metric represents the proportion of the data instances that the model predicts to be relevant which is truly relevant. It is the number of true positives divided by the number of true positives plus the number of false positives. It is calculated mathematically by:

$$\text{Precision} = \frac{t_p}{t_p + f_p} \quad (10)$$

- v. **F-measure:** This is the weighted harmonic mean of precision and recall. It is calculated as follows:

$$F - \text{measure} = \frac{2PR}{(P + R)} \quad (11)$$

Considering the equations above, true positive ( $t_p$ ) is the number of phishing URLs that were correctly identified as phishing, false positive ( $f_p$ ) is the number of legitimate URLs that were incorrectly detected as phishing. True negative ( $t_n$ ) is the number of legitimate URLs that were correctly identified as legitimate, while false negative ( $f_n$ ) is the number of phishing URLs that were incorrectly detected as legitimate.

## 4 Results and Discussion

This section explains the process employed in detecting malicious URLs using selected meta-heuristic algorithms for feature selection and SVM and RF for classification. It discusses the experiments performed, simulation tool as well as the result analysis. To evaluate the performance of each of the selected meta-heuristics algorithms, various experiments were carried out using Dataset1 and Dataset2. The experiment was performed on Windows 10 operating system, having a random-access memory (RAM) of 4 GB and 2.50 GHz Intel Core i5 CPU with 500 GB hard disk. Finally, cross-validation using 10-fold was employed to assess the performance of the selected meta-heuristic algorithms on the two phishing datasets.

## 4.1 Modelling and Interpretation

The experiments were conducted using WEKA 3.8.2 version, which is a simulation tool with different machine learning algorithms for predictive tasks. It has the capability for data preparation, classification, regression, clustering, associate rule mining and visualization. WEKA is a popular tool for data mining. It is an open-source and freely available platform-independent software. It has flexible facilities for scripting experiments.

**Classification performance based on SVM.** Table 2 presents the classification results of SVM based on all the features in the two datasets that were analysed in this study. From this result, SVM is able to achieve performance accuracy of 86.60% and 93.8% for Dataset1 and Dataset2, respectively. The false positive was 0.109 for Dataset1 and 0.066 for Dataset2. The results of other metrics considered were also promising, which shows the significance of the model for distinguishing phishing web pages from legitimate ones.

**Classification performance based on RF.** The results obtained based on RF algorithm without feature selection is summarized in Table 3. RF produced better results across the evaluation metrics used in this study. For instance, the accuracy of RF algorithm is 89.4% on Dataset1 and 97.2% on Dataset2. As shown in the table, ROC of the proposed RF model for two datasets was estimated at 96.3% and 99.3%, respectively. This shows the capability of the proposed framework to effectively detect phishing

**Table 2** Classification based on SVM only

	Dataset1	Dataset2
Accuracy	0.860	0.938
TP rate	0.860	0.938
FP rate	0.109	0.066
Precision	0.843	0.938
Recall	0.860	0.938
F-measure	0.846	0.938
ROC area	0.900	0.936

**Table 3** Classification based on RF only

	Dataset1	Dataset2
Accuracy	0.894	0.972
TP rate	0.894	0.972
FP rate	0.081	0.031
Precision	0.894	0.972
Recall	0.894	0.972
F-measure	0.894	0.971
ROC area	0.963	0.993

web pages. In addition, false alarm was reduced across the two phishing datasets. The importance of the RF model to produce relevant results is very significant as demonstrated by the results obtained with the precision metric.

**Classification performance based on GA and SVM.** GA was used for feature selection on Dataset1 and Dataset2, each having ten (10) and thirty (30) features, respectively, as earlier highlighted. GA selected five (5) optimal features for Dataset1 and nine (9) optimal features for Dataset2. With the reduced features for modelling, the proposed framework based on GA was able to achieve very promising results without compromising the model performance as shown in Table 4. Using the minimal number of features as selected from the GA algorithm produced accuracy of 83.7% and 93.3% for Dataset1 and Dataset2, respectively. This result reveals that the proposed approach is able to reduce model complexity while still retain better performance.

**Classification performance based on GA and RF.** Based on the selected features from GA, RF model produced improved results on Dataset2. The model accuracy dropped slightly on Dataset1; however, the ROC result is better than the SVM model with GA selected features. Table 5 summarized the results based on GA and RF algorithms. From this result, an accuracy of 82.3% and 94.4% was obtained on Dataset1 and Dataset2, respectively. This result implied that GA is a good feature subset selection algorithm for developing a model to detect malicious web pages.

**Table 4** Classification based on GA and SVM

	Dataset1	Dataset2
Accuracy	0.837	0.933
TP rate	0.837	0.933
FP rate	0.129	0.072
Precision	0.792	0.933
Recall	0.837	0.933
F-measure	0.811	0.933
ROC area	0.866	0.931

**Table 5** Classification based on GA and RF

	Dataset1	Dataset2
Accuracy	0.823	0.944
TP rate	0.823	0.944
FP rate	0.135	0.059
Precision	0.804	0.944
Recall	0.823	0.944
F-measure	0.811	0.944
ROC area	0.935	0.986

**Table 6** Classification based on WOA and SVM

	Dataset1	Dataset2
Accuracy	0.837	0.933
TP rate	0.837	0.933
FP rate	0.129	0.072
Precision	0.792	0.933
Recall	0.837	0.933
F-measure	0.811	0.933
ROC area	0.866	0.931

**Table 7** Classification based on WSA + RF

	Dataset1	Dataset2
Accuracy	0.823	0.944
TP rate	0.823	0.944
FP rate	0.135	0.059
Precision	0.804	0.944
Recall	0.823	0.944
F-measure	0.811	0.944
ROC area	0.935	0.987

**Classification performance based on WOA and SVM.** Wolf optimization algorithm (WOA) was used for feature subset selection on both datasets. The results were similar to those obtained in GA. WOA also selected five (5) optimal features for Dataset1 and nine (9) attributes for Dataset2. The results are summarized in Table 6.

**Classification performance based on WOA and RF.** Since the number of features selected by the two meta-heuristic algorithms considered in this study is the same, WOA with RF algorithm produced similar results when compared with GA with RF algorithm. These results are also summarized in Table 7 with an accuracy of 82.3% and 94.4% for Dataset1 and Dataset2, respectively. These results show that the two meta-heuristic algorithms considered in this study have produced promising results comparable to the results obtained without feature subset selection. This approach reduced the model complexity and guaranteed an improved prediction time when deployed in a real-life environment.

## 4.2 Models Comparison Based on SVM as a Classifier

Figures 3 and 4 show the comparison of the results of the models based on SVM algorithm for phishing URLs detection on Dataset1 and Dataset2, respectively. The meta-heuristic algorithms have really demonstrated comparable results considering the results obtained with the evaluation metrics.

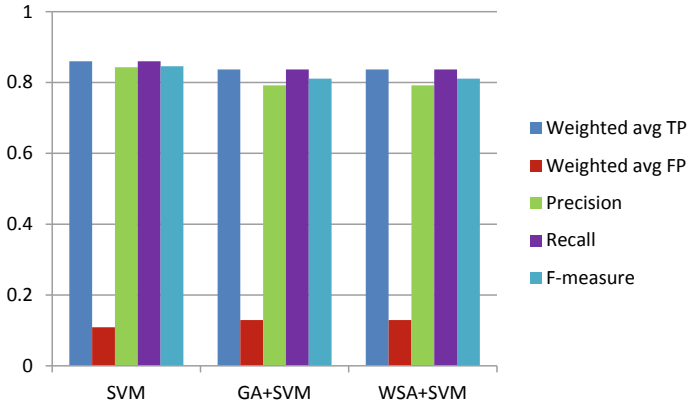


Fig. 3 Comparison of the SVM models based on Dataset1

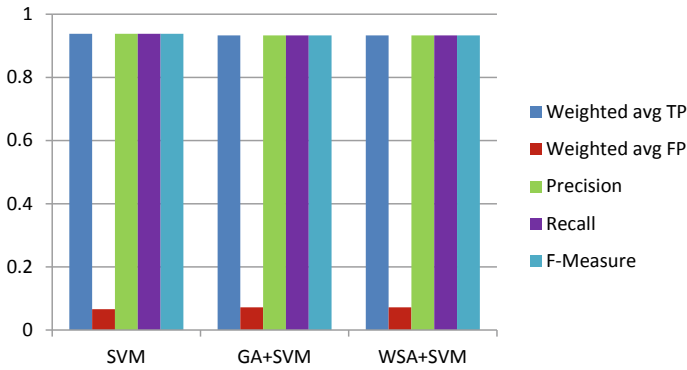


Fig. 4 Comparison of the SVM models based on Dataset2

Furthermore, the time taken by each model based on SVM classifier with and without feature subset selection revealed that the models based on meta-heuristic algorithms produced in complexity as demonstrated by their training time in seconds. However, the WOA and SVM model took the least time, having 0.16 and 8.72 s for Dataset1 and Dataset2, as shown in Figs. 5 and 6, respectively.

### 4.3 Models Comparison Based on RF as a Classifier

Similarly, Figs. 7 and 8 show the performance of the different RF models on Dataset1 and Dataset2, respectively. As shown in these figures, RF models based on the two meta-heuristic algorithms produced comparable results when compared with the RF model without feature subset selection.

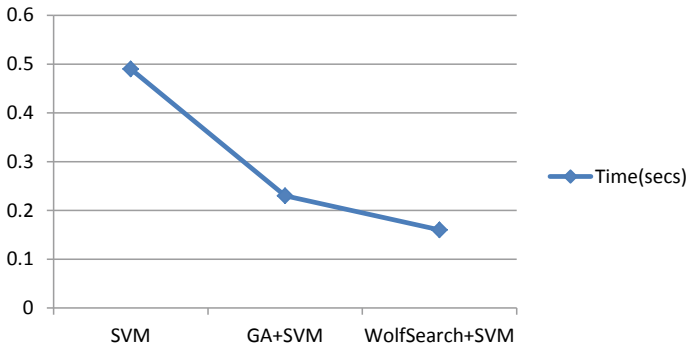


Fig. 5 Comparison of time taken for Dataset1 with SVM models

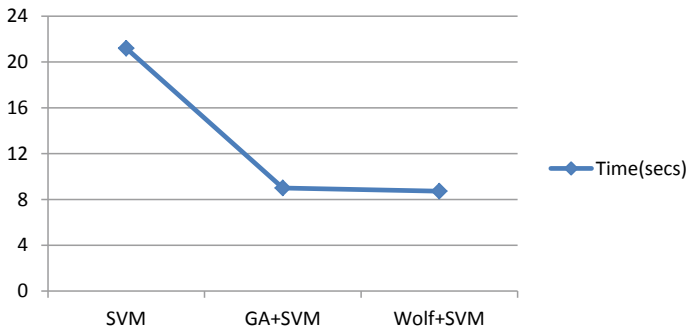


Fig. 6 Comparison of time taken for Dataset2 with SVM models

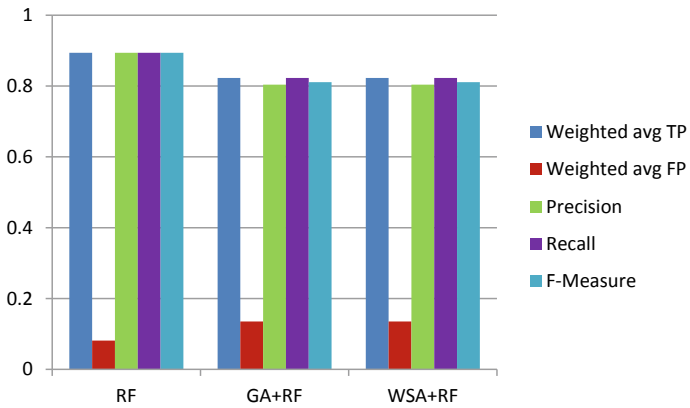


Fig. 7 RF models comparison based on Dataset1



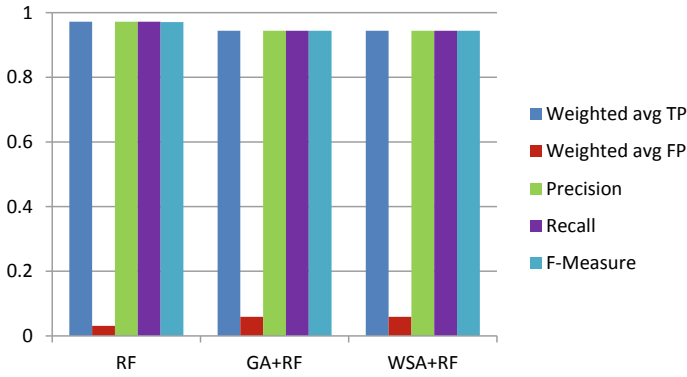


Fig. 8 RF models comparison based on Dataset2

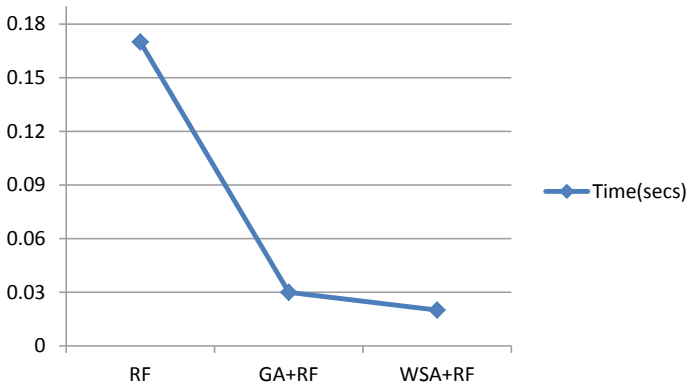
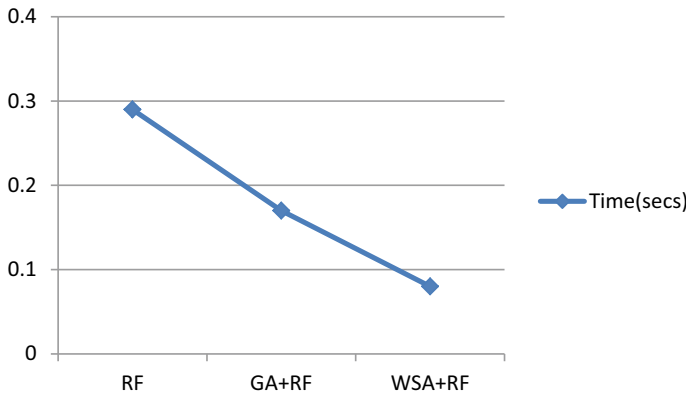


Fig. 9 Comparison of time taken for Dataset1 with RF models

Similarly, it was observed that the time taken by the WOA algorithm on the two datasets was reduced when compared with GA and RF model without feature subset selection (see Figs. 9 and 10). This finding reveals that WOA algorithm is a better candidate to produce a model with less complexity when feature dimensionality reduction is being considered to build a prototype of phishing URLs detection system. WOA and RF model took the least time, having 0.02 and 0.08 s for Dataset1 and Dataset2, respectively.

#### 4.4 Comparison with Existing Models

This section shows the comparison of the results of the proposed models in this study with the existing model that have been developed in the literature. Table 8



**Fig. 10** Comparison of time taken for Dataset2 with RF models

**Table 8** Baseline comparison with the existing model based on Dataset2

Approaches	Models	TPR	FPR	Accuracy	Precision	Recall	F-Measure	ROC
Proposed	<b>RF</b>	<b>0.972</b>	<b>0.031</b>	<b>0.972</b>	<b>0.972</b>	<b>0.972</b>	<b>0.971</b>	<b>0.993</b>
Proposed	<b>WOA + RF</b>	<b>0.944</b>	<b>0.059</b>	<b>0.944</b>	<b>0.944</b>	<b>0.944</b>	<b>0.944</b>	<b>0.987</b>
Aydin and Baykal [6]	SMO	0.938	0.066	0.938	0.938	0.938	0.938	0.936

summarizes the results of the various models under consideration. As discussed in the previous section, Naïve Bayes and SMO approach were studied in the work of [6]. From this table, the proposed models were able to outperform the state-of-the-art producing promising results across the different evaluation metrics considered in this study. In order to ensure objectivity in the models’ comparison in this section, the SMO experiment in [6] was conducted and the results reported in Table 8 for comparison with the proposed models in this study.

## 5 Conclusion

In this study, the performance of two meta-heuristic algorithms, GA and WOA, was examined for feature subset selection towards identifying malicious web pages. Due to the high exploration capability of features selection of the two meta-heuristic algorithms, they demonstrated promising results when compared with models without feature subset selection. SVM and RF classifiers were considered to develop effective classification models for the proposed framework. From the results obtained, the models based on RF outperformed SVM model using performance metrics such as accuracy, sensitivity, specificity, recall, precision, F-measure and ROC. The results of RF and WOA with RF models were compared with existing state-of-the-art model,

and the outcome revealed that the proposed models in this study gave better performance when compared with the state-of-the-art. Furthermore, this study observed that WOA meta-heuristic optimization algorithm gave the least running time and reduced model complexity when compared with other models developed in this study. Although the performance of the models without feature subset selection is better, however, models based on meta-heuristic optimization were able to reduce complexity with a slight reduction in the accuracy. In future, the authors intend to investigate other feature categories that may improve the performance of the models for phishing detection. In addition, other feature selection methods need to be investigated.

## References

1. Priya, R.: An ideal approach for detection of phishing attacks using naïve bayes classifier. *Int. J. Comput. Trends Technol. (Technology)* **40**, 84–87 (2016)
2. Sahoo, D., Liu, C., Hoi, S.C.: Malicious URL detection using machine learning: a survey, arXiv preprint [arXiv:1701.07179](https://arxiv.org/abs/1701.07179) (2017)
3. Lin, M.-S., Chiu, C.-Y., Lee, Y.-J., Pao, H.-K.: Malicious URL filtering—A big data application. In: 2013 IEEE International Conference on Big Data, pp. 589–596 (2013)
4. Vanhoenshoven, F., Nápoles, G., Falcon, R., Vanhoof, K., Köppen, M.: Detecting malicious URLs using machine learning techniques. In: 2016 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1–8 (2016)
5. Gupta, S.: Efficient malicious domain detection using word segmentation and BM pattern matching. In: 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1–6 (2016)
6. Aydin, M., Baykal, N.: Feature extraction and classification phishing websites based on URL. In: 2015 IEEE Conference on Communications and Network Security (CNS), pp. 769–770 (2015)
7. Li, Y., Yang, Z., Chen, X., Yuan, H., Liu, W.: A stacking model using URL and HTML features for phishing webpage detection. *Future Gener. Comput. Syst.* **94**, 27–39 (2019)
8. Wang, R., Zhu, Y., Tan, J., Zhou, B.: Detection of malicious web pages based on hybrid analysis. *J. Inform. Secur. Appl.* **35**, 68–74 (2017)
9. Adewole, K.S., Akintola, A.G., Saliyu, S.A., Faruk, N., Jimoh, R.G.: Hybrid rule-based model for phishing URLs detection. In: International Conference for Emerging Technologies in Computing, pp. 119–135 (2019)
10. Xuan, J., Yongzhen, L.: The detection method for two-dimensional barcode malicious URLs based on the hash function. In: 2016 3rd International Conference on Information Science and Control Engineering (ICISCE), pp. 702–705 (2016)
11. Darling, M., Heileman, G., Gressel, G., Ashok, A., Poornachandran, P.: A lexical approach for classifying malicious URLs. In: 2015 international conference on high performance computing & simulation (HPCS), pp. 195–202 (2015)
12. Lee, S., Kim, J.: Warningbird: A near real-time detection system for suspicious urls in twitter stream. *IEEE transactions on dependable and secure Comput.* **10**, 183–195 (2013)
13. Adewole, K.S., Han, T., Wu, W., Song, H., Sangaiah, A.K.: Twitter spam account detection based on clustering and classification methods. *J. Supercomput.*, 1–36 (2018)
14. Bhardwaj, T., Sharma, T.K., Pandit, M.R.: Social engineering prevention by detecting malicious URLs using artificial bee colony algorithm. In: Proceedings of the Third International Conference on Soft Computing for Problem Solving, pp. 355–363 (2014)

15. Tang, R., Fong, R., Yang, X.-S., Deb, S.: Wolf search algorithm with ephemeral memory. In: Seventh International Conference on Digital Information Management (ICDIM 2012), pp. 165–172 (2012)
16. Chu, Z., Gianvecchio, S., Wang, H., Jajodia, S.: Detecting automation of twitter accounts: are you a human, bot, or cyborg? *IEEE Trans. Dependable Secure Comput.* **9**(6), 811–824 (2012)
17. Refaeilzadeh, P., Tang, L., Liu, H.: Cross-validation. *Encyclopedia of database systems*, pp. 532–5382 (2009)
18. Babagoli, M., Aghababa, M.P., Solouk, V.: Heuristic nonlinear regression strategy for detecting phishing websites. *Soft. Comput.* **23**, 4315–4327 (2019)
19. Sohrabi, M.K., Karimi, F.: A feature selection approach to detect spam in the Facebook social network. *Arabian J. Sci. Eng.* **43**, 949–958 (2018)
20. Sahingoz, O.K., Buber, E., Demir, O., Diri, B.: Machine learning based phishing detection from URLs. *Expert Syst. Appl.* **117**, 345–357 (2019)