World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 5.924

A NEW DEFENSE MECHANISM AGAINST SMISHING ATTACKS USING GRAY WOLF OPTIMIZER

***[1]Marwan H. Alsammarraie and [2]Mohamad A. Alfayomi**

[1]Software Engineering Department, Faculty of Information Technology, Isra University.
[2]Professor, Computer Science Department, Faculty of Information Technology, Isra University.

Article Received on 21/04/2020 **Article Revised on 11/05/2020** **Article Accepted on 01/06/2020**

***Corresponding Author**
Marwan H. Alsammarraie
Software Engineering Department, Faculty of Information Technology, Isra University.

SUMMARY

Recently, the phishing attack is one of the critical threats against the Organizations, Internet users, service provider, cloud computing and many other fields in daily life. In the phishing attack, the intruder attempts to defraud the users and leak or steal the credential information, including personal information such as bank account, passwords etc., by sending a fooled email or SMS to redirect the user to an untrusted website. Various methods have been proposed in terms of filtering and detect different types of phishing attacks, however, the researchers and security information experts still studying to find a solution to assure the internet security from phishing and other attacks. Viewing SMS phishing messages are mostly short text and become a relatively low number associated with legitimate messages, new features for quick writing and oversampling technique for imbalanced data utilized to SMS phishing detection. In this research, a novel framework of the SMS phishing detection presented. The proposed method combines feature extraction, oversampling, optimization algorithm for feature selection and classification. The general framework for SMS phishing detection is consists of Data input, Data preprocessing, Feature extraction, Oversampling. Then, Feature optimization using binary Gray Wolf Optimizer Algorithm, Classification using support vector machine (SVM), and results and output.

1. INTRODUCTION

term phishing can define as an identity fraud that takes benefit of developed systems and

applications targeting vulnerabilities due to human nature. The phishing process starts by sending the phisher an SMS or email to the ordinary user the appears to that massage from a legitimate sender. These emails and SMS contain links, which leads to a phisher malicious webpage where users asked to provide credentials information or to download and install malware or spyware on mobile or computer (Gupta, Tewari, Jain, Agrawal, & Applications, 2017). The motivation of the phisher behind sending and make scams are several reasons such as financial earnings, identity theft, or notoriety (Almomani et al., 2013).

The phishing attack is considered as one of the main criminal mechanisms that involve both social engineering attacks and technical subterfuge attacks to steal users' information (i.e., personal identity (ID)) and financial account credentials (Tong, ZHENG, WU, WANG, & Engineering, 2018). As stated in the recent reports of Anti-Phishing Working Group (APWG), the number of phishes recognized agents the websites at the beginning of the year 2019 was 162,155, which is around 46% from the whole recognized phishes (180,577) at the end of the year 2018, figure 1 show the number of phishing sites in 2019 (Group, 2019)

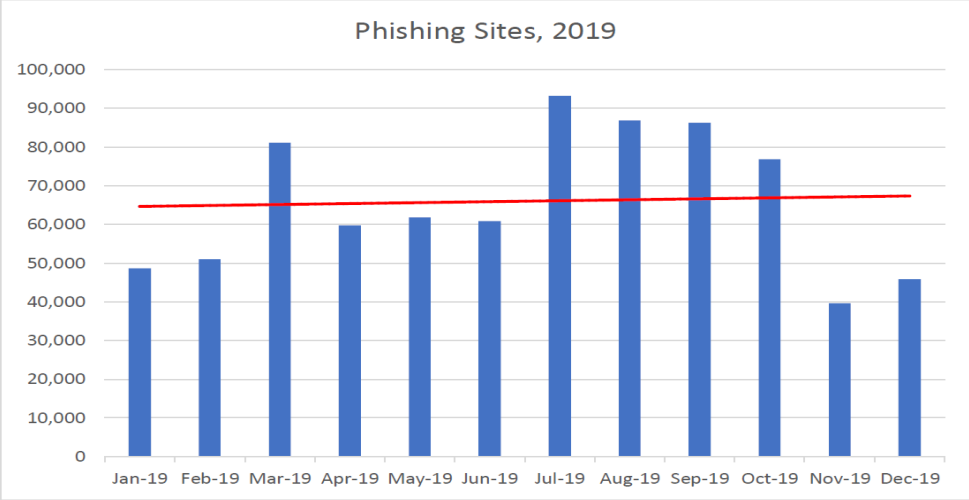

Figure 1: Number of phishing sites in 2019.

The number of the phishing attack show that the Software as a service (SaaS) on the cloud and the webmail sites are the highest target to attack by phishing. Numerous security organizations reported that phishing attacks on social media overgrowing and increased double in 2019.

However, the assaults against the cloud storage and files hosting website not popular yet, figure 2 illustrates the most target sectors in 2019 (Group, 2019).

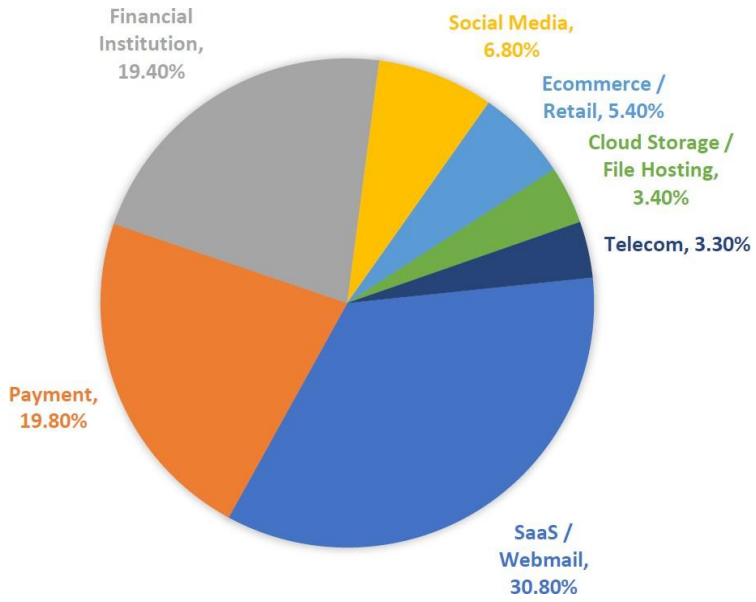

Figure 2: The most target sectors in 2019.

2. Related Works

Different studies proposed for SMS phishing detection systems, which can be categorized into two main types the study of phishing detection algorithm and the second type is the improvement of the phishing detection system. The investigation on the detection algorithm is intended to enhance the accuracy of the detection system by the machine learning algorithms and several statistical learning approaches. The phishing detection system is designed to implement in mobile phones to protect SMS messages phishing. On the other hand, the previous researches use two types of features the non-content and content features. The non-content feature related to SMS components (i.e. timestamp, message size) (Xu, Xiang, Yang, Du, & Zhong, 2012). The content feature focus on the accuracy of the phishing system, such as function words and special characters.

In general, the researches studies of the SMS phishing constraint on the investigation of the detection algorithm. (Uysal, Gunal, Ergin, & Gunal, 2013) Investigates on filtering the SMS to extract the spam messages by investigating the impact of feature extraction and selection methods on Turkish and English. The feature set of the filtering structure contains a group of features constructs from a bag of words (BoW) method and a set of structural features (SF) unique to the spam issue. The information-theoretic feature selection method used to classify the BoW features. Then different mixtures of SF and Bow filled within broadly used pattern classification approaches to classify SMS. The result demonstrates that the proposed mixture method of BoW and SF shows (Gómez Hidalgo, Bringas, Sánz, & an outperformance in

classification performance on the dataset García, 2006) propose to use the Bayesian filtering approach to detect and block the spam messages. The English and Spanish language used to build sets of SMS spam. To examine the effects of spam on the language sets, several Machine learning approaches, and messages design methods tested. The result shows a significant performance of Bayesian filtering in terms of effectiveness. A new smartphone spam group formed by non-encoded and existing messages dataset presented by (Almeida, Hidalgo, & Yamakami, 2011). Furthermore, proposed statistics associating to the designed corpus, as symbols repetitions and since the corpus created by subsets of messages obtained from similar origins. The Support Vector Machine (SVM) and various machine learning algorithms are compared to classify the spam SMS. The SVM algorithm shows a better performance comparing with other algorithms. (Karami, Zhou, & Technology, 2014) Interduce a lexical-semantic and employ passive content-based features to detect the static SMS spams. The efficiency of the proposed method validated using different classification methods. The result shows that the proposed method enhances SMS spam detection performance. An analysis of the spam filtering approaches for the spam SMS messages introduced by (Mathew & Issac, 2011). Several filtering methods (i.e., Lazy IBK, Attribute Selected Classifier, and Bayesian Logic Regression) of SMS spam compared to recognize the best performing method in the SMS text to optimizes the spam detection for SMS. The Bayesian Logic Regression shows the best performance among different algorithms to detect spam. (Zainal, Sulaiman, Jali, & Security, 2015) Propose to use the Weka and RapidMiner to classify and clustering the spam messages along with different algorithms such as SVM for classification and K-Means for clustering. The suggested tools employ on SMS spam datasets to classify and cluster the spams. The result demonstrates that the best classifying algorithm is SVM comparing with other algorithms such as Naïve Bayesian, on the other hand, the best clustering algorithm is K-means comparing to other algorithms like k-Nearest Neighbour algorithm.

Some researcher focuses on development application to work as SMS phishing detection. An SMS manager and SMS content detection based on Ontology controller for SMS method. The Ontology algorithm utilized to analyze and classify the spam SMS. The proposed method examined on different cases, the result shows satisfying and support the implementing the proposed work (Balubaid & Manzoor, 2015). (Sethi & Bhootna, 2014) introduce the Bayesian classifying method to detect and prevent SMS spams. The authors build two groups of SMS spam with proper size and some particular words, then examined on several messages' description methods and Machine Learning methods, in terms of efficiency. A service-side

based solution implements the graph data mining to detecting the spams SMS proposed by (Xu et al., 2012). Moreover, authors study techniques to identify spam based on features that include temporary and graph-topology data but eliminate content. SVM and K-NN classification algorithms employed to detect the spams. The SVM algorithms show a better performance to detect spams.

For the content feature, various studies try to employ content features. (Uysal, Gunal, Ergin, & Gunal, 2012) introduce a new framework using two feature selection methods based on information accumulation and chi-square metrics to find the discriminative features describing the SMS messages. Then, Two Bayesian classifiers implemented on the discriminative feature to find out the spam SMS messages. Furthermore, a mobile application for Android phones is built to filter the spams in the real-time base. This filter works silently without distributing the user. The proposed work evaluated on extensive SMS messages. The evaluation result demonstrates that the proposed framework shows accurate classification spam messages. Identify the several threats against mobile phones and attitudes of users with those threats is a critical issue. (Yeboah-Boateng, Amanor, & Sciences, 2014) examines various phishing attacks on mobile phones and the user attitudes dealing with online phone services. Lastly, a taxonomy of decoying and alluring proposed by the authors, which contain words utilized in phishing assaults, could be a valuable benchmark for clients to defend toward becoming a victim. In this paper (Warade, Tijare, & Sawalkar, 2014), the SMS spam detection system proposed by lookup in the call record data and SMS messages. The system will examine the relationship between the user and the message sender. If there is no relation between the user and the sender, and the message contains spam, then the system will reject the message. (Junaid & Farooq, 2011) proposes an SMS spam detection system can detect the spams on the access layer of the smartphone. Spam messages examine to distinguish the feature of spam messages through the hexadecimal format of the SMS. Then, these features provided to a classifier to filter the spams such as Naive Bayes Algorithm, K Nearest Neighbor (IBk), Fuzzy AdaBoost (Fuzzy-AB) and sUpervised Classifier System (UCS). The UCS algorithm shows the best performance in spam detection. Based on Naïve Bayesian Classifier (Joo et al., 2017) present an S-Detector which classifies the words, then classify the Smishing messages from the general one. And this is primarily utilized to clarify by using a statistical learning approach.

3. RESEARCH METHOD

Viewing SMS phishing messages are mostly short text and become a relatively low number

associated with legitimate messages, new features for quick writing and oversampling technique for imbalanced data are utilized to SMS phishing detection. In this section, a novel framework of the SMS phishing detection is presented, as shown in Figure 4. The proposed method combines feature extraction, oversampling, optimization algorithm for feature selection and classification.

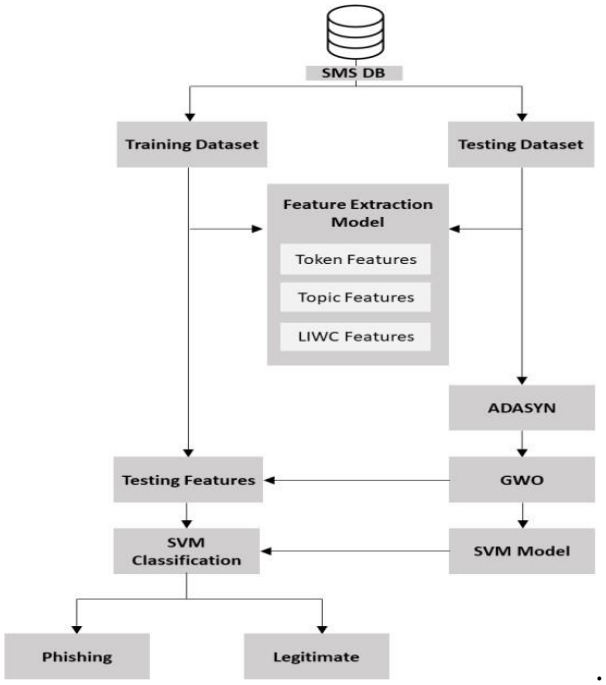

Figure 3: The methodology of SMS phishing detection.

3.1 Framework for SMS phishing detection

The general framework for SMS phishing detection is consists of seven main steps: Data input, Data preprocessing, Feature extraction, Oversampling, Feature optimization using binary Gray Wolf Optimizer Algorithm, Classification using support vector machine (SVM), and Result output. dataset according to several splits or parts. Three types of features are involved in the pre-processing steps called token features, topic features, and LIWC features, which are extracted in the feature extraction level, which will be introduced in detail in the following sections. One of the current conventional oversampling methods for trading with the imbalanced examples problem called Adaptive Synthetic Sampling Approach (ADASYN) (He, Bai, Garcia, & Li, 2008; He, Garcia, & engineering, 2009). ADASYN is utilized to support phishing examples and legitimate examples.

Oversampling is essential for SMS phishing detection because of the imbalanced SMS data in real life. Binary Gray Wolf Optimizer (BGWO) algorithm is employed to feature selection

optimization steps to extract optimal features and decrease feature dimensions. Finally, the support vector machine (SVM) is utilized to classify whether it is a phishing message or a legitimate message.

3.2 Dataset

In the paper, we decide to use the dataset created by (Almeida et al., 2011) this dataset is widely used in machine learning studies, and published in UCI dataset. Moreover, it contains more than 5574 messages (747 spam messages and 4827 legitimate messages) in the non-encoded form in the English language. In addition, 425 SMS as a spam SMS text was extracted from the internet. The web site used to collect this data is the Grumbletext, which is a famous UK website that the users used to claim and report the spam messages. Furthermore, the data set contain random 3.375 a non-spam message, which is known as ham messages. Another 450 legitimate SMS inserted and more messages were added as shown in Table1

Table 1: Dataset statics.

Type of message	Number of messages	The percentage of messages
Hams	4,827	86.60 %
Spams	747	13.40 %
Total	5,574	100.00 %

3.3 Feature detection for SMS phishing

Three models of feature extraction used, first, the token features which collected from the function word and the message structure. Secondly, the topic features will focus on SMS properties by utilizing the Biterm topic approach (Yan, Guo, Lan, & Cheng, 2013). Finally, the Linguistic Inquiry and Word Count (LIWC) features adapted for its outperformance (Karami et al., 2014).

3.3.1 Token features

Token features introduced containing function word features and structure features and by extracting relevant kinds of literature. The structure features are properties of characters, for both sentences and words in SMS (Cheng, Chandramouli, & Subbalakshmi, 2011). In this work, the structure features included the number of words, characters, the up characters, and the special character "!". (Uysal et al., 2013). The Function word features obtain by showing the top fifty one- gram, two-gram, and three-gram word lists among the spam messages datasets. Some small word (i.e: 'to', 'a', 'you have', and 'this is') are neglected. For this, the function words will initially select the verb, adjectives, nouns, and phrases. Features related to the URL also

chosen (i.e. 'ur', 'uk', 'www') which are essential features for phishing detection (Almeida et al., 2011; Xu et al., 2012). The following table 1 shows the primary elements of the different grams. Table 2 shows the token features, structure features, and function feature words.

Table 2: Initial elements of function words.

Kind	Words
One-gram	txt, text, ur, reply, call, free, now, stop, mobile, www, claim, cash, please, urgent, uk, only.
Two-gram	your mobile, have won, to claim, call now, call from, please call, co uk, won a, account statement, or cash, private your, statement for, your account, a prize, win a, call identifier, code expires, identifier code.
Three-gram	call identifier code, have won a, account statement for, identifier code expires, statement for shows, you have won, private your. account, your account statement, attempt to contact, are awarded with, thanks for your

Table 3: Token features.

Features	Features
Structure features	Number of the following feature: character, up character, !, words.
Function words features	stop, text, uk, statement, www, reply, please, urgent, cash, txt, claim, ur, mobile, identifier, expires, code, private, thanks, award, contact, only, win, call, account, won, free, now, prize.

3.3.2 Topic features

A topic model is a statistical representation employed to obtain the latent semantic construction in a series of texts which is generally employed in natural language processing (NLP). General topic models (e.g. Latent Dirichlet Allocation (LDA) and SVM) are applied in Email phishing discovery most commonly (Aleroud et al., 2017). As a variety of small text, SMS messages vary from Emails and the other types of long texts. Immediately using those topic models on SMS phishing discovery does not control well on account of the difficult data sparsity in small texts. Biterm topic model (BTM) shows the word co-occurrence designs and handles the aggregated guides in the whole corpus for learning points to address the problem of sparse word co-occurrence models at the level of the texts (Yan et al., 2013). The occurrence probability of the topic of each message is reached by BTM, which is applied as topic features in this work. Ten-fold cross-validation approach is used to manage the most suitable number of problems, and finally, 50 topics are chosen through experiments using the SVM.

3.3.3 Linguistic Inquiry and Word Count Feature

Linguistic Inquiry obtains Linguistic Inquiry and Word Count (LIWC) features and Word Count

(LIWC) tool, which is a simple text analysis application that calculates words in psychologically meaningful categories (Tausczik, Pennebaker, & psychology, 2010). LIWC can parse text content quantitatively and measure the percentage of distinctive words classes in the text such as causal terms, sensitive terms, cognitive terms and the other psychological roles. LIWC is extensively employed in the area of natural language processing and science. Literature (Karami et al., 2014) firstly adopts LIWC features in SMS phishing discovery and produces promising performance. Ninety-three LIWC features are used in this work.

3.4 Oversampling approach for imbalanced data

Mobile safety records in China means there are approximately 159.53 billion SMS reports in the first part of 2017, among which 0.18 billion messages are phishing messages. There are quite a few phishing examples related to general text information. The vast difference in the data implies that SMS phishing discovery is an imbalanced individual problem. Imbalanced samples can guide to a set of problems. The information received in minority status is very restricted, and it is hard to excavate rules inside. Many classification algorithms apply the divide and conquer technique, and few rules of youth class result in low distribution accuracy. On the other view, inappropriate text bias systems tend to classify samples as the majority class when uncertainty endures. Consequently, SMS phishing detection flow will be approximately low utilizing conventional process without trading with the problem of imbalanced examples.

There are many ways for managing class imbalance, such as weighted loss function, under sampling plan, oversampling system, etc. Weighted loss function approach is to establish a weight for the loss function so that the lack of discriminant errors for opposition class is higher than that of the majority group. The under-sampling system is to increase the classification achievement of the minority group by decreasing the majority class examples. The difficulty of the under-sampling method is that some vital information of the majority group is lost. The oversampling way is to reduce or reduce the imbalance of data by attaching some samples of the minority group. The oversampling method leads to over fitting sometimes. Synthetic minority oversampling technique (SMOTE) is the most popular applied oversampling method for handling class imbalance. This work utilises Adaptive Synthetic Sampling Approach (ADASYN), which is an expansion of SMOTE on its superior performance.

ADASYN algorithm is suggested to use to overcome the weakness of SMOTE algorithm which is smitten increases the appearance of overlapping between groups because it produces the same number of synthetic data examples for each first minority pattern without considering next-

door- neighbour cases (Wang et al., 2010). The chief idea of the ADASYN algorithm is to apply a density population as a model to automatically determine the number of synthetic units that require to be created for each minority example by adaptively adjusting the weights of various minority examples to repay for the skewed arrangements.

3.5 Feature selection method based on binary GWO algorithm

In this part, the motivation of the proposed method is first presented. Then, the mathematical model is presented.

Grey Wolf Optimizer (GWO) is motivated by grey wolves as in (Mirjalili, Mirjalili, & Lewis, 2014). The GWO algorithm simulates the management authority and hunting tool of grey wolves in life. 4 kinds of grey wolves such as alpha, beta, delta, and omega are operated for assuming the leadership authority as shown in Figure 5. Also, the three primary levels of hunting, searching for prey, encircling prey, and attacking prey, are performed.

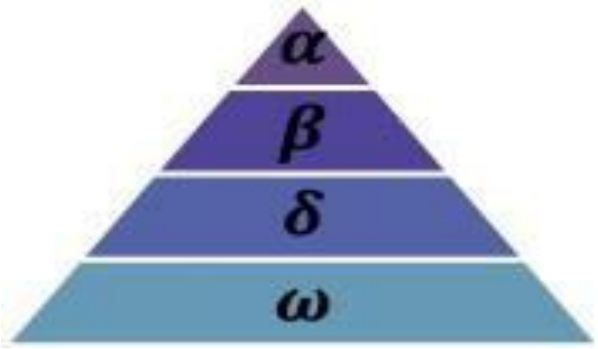

Figure 3: Hierarchy of grey wolf.

3.5.1 Inspiration

A grey wolf goes to the Canidae group. Grey wolves are recognized as apex predators, meaning that they are at the head of the meals chain. Grey wolves often fancy being in a pack (Mirjalili et al., 2014). The pseudo code of the GWO algorithm is presented in Figure 4.

set the maximum number of iterations L
Initialize the population $X_i (i = 1, 2, \ldots, n)$
Initialize a, A, and C
Calculate the fitness of wolves
X_α = the best search agent
X_β = the second best search agent
X_δ = the third best search agent
while $(t < L)$ **do**
  for each search agent **do**
    Update the position of the current search agent
  end for
  Update a, A, and C
  Calculate the fitness of all search agents
  Update X_α , X_β and X_δ
  $t = t + 1$
end while
return X_α

Figure 4: The pseudo code of the GWO algorithm.

The social authority of wolves, collection hunting, is another unusual social behavior of grey wolves. The main phases of grey wolf hunting are as follows:

Tracking, chasing, and threatening the prey.
Pursuing, encircling, and harassing the prey until it stops moving. Attack towards the prey. These steps are shown in Figure 5.

Figure *5:* Hunting behavior of grey wolves.

In this work, this hunting method and the cultural authority of grey wolves are

mathematically presented in order to design binary GWO and perform the optimization process. More details are in (Mirjalili et al., 2014).

3.5.2 Mathematical Model

In this section, we will present the mathematical model and the main outline of the GWO algorithm. The modeling of Social:

This algorithm designed to make the alpha (α) wolves an appreciate solution. Then, the second and the third solutions considered to be beta (β) and delta (δ). The rest of the considered solutions are omega (ω), as illustrated in figure 6.

Surround the prey

During the hunting, the grey wolves surround the prey. which can be modeled as in Eq.1.

…… E.q. $1D = |C.X_p(t) - X(t)|$

…… E.q. $2X(t+1) = X_p(t) - A.D$

Where t refers to the current iteration, the variables A and C are coefficient vectors, the X and XP is the position vector of a grey wolf and prey, respectively.

We can calculate the vector A and C as follow:

$E.q.\ 3A = 2a.r_1 - a$

$E.q.\ 4C = 2a.r_2$

Where the variables of a reduced from 2 to 0 linearly throughout iterations, the components r1 and r2 are chosen randomly to represent the vectors in [0, 1].

Figure 9 shows the effects of E.q. 1 and E.q. 2, these two equations represent a couple of dimensional location vector. As illustrated in the figure, the wolf in the location (X, Y) will update its location according to the prey location (X^*, Y^*). Several locations around the optimal agent reached concerning the current location by changing the value of A and C. For example, the wolf can move to the location (X^*- X, Y), by changing the values to A= (1, 0), C= (1, 1). Figure 10 demonstrated the wolf updated it is location in 3D space.

r1 and r1 which are random vectors enable the wolves to move to any location between the spots depicted in figure 3. Thus, the wolves can move to a new location in space surrounding the prey randomly by using E.q 1 and E.q. 2.

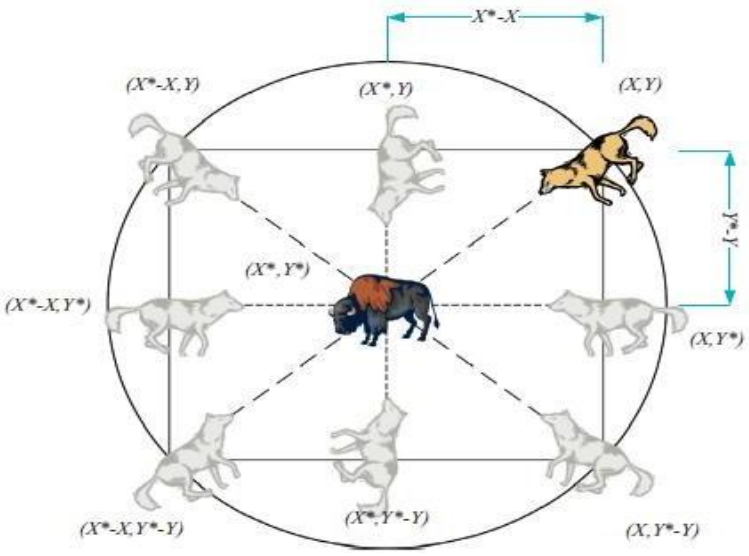

Figure 6: The effects of E.q. 1 and E.q. 2.

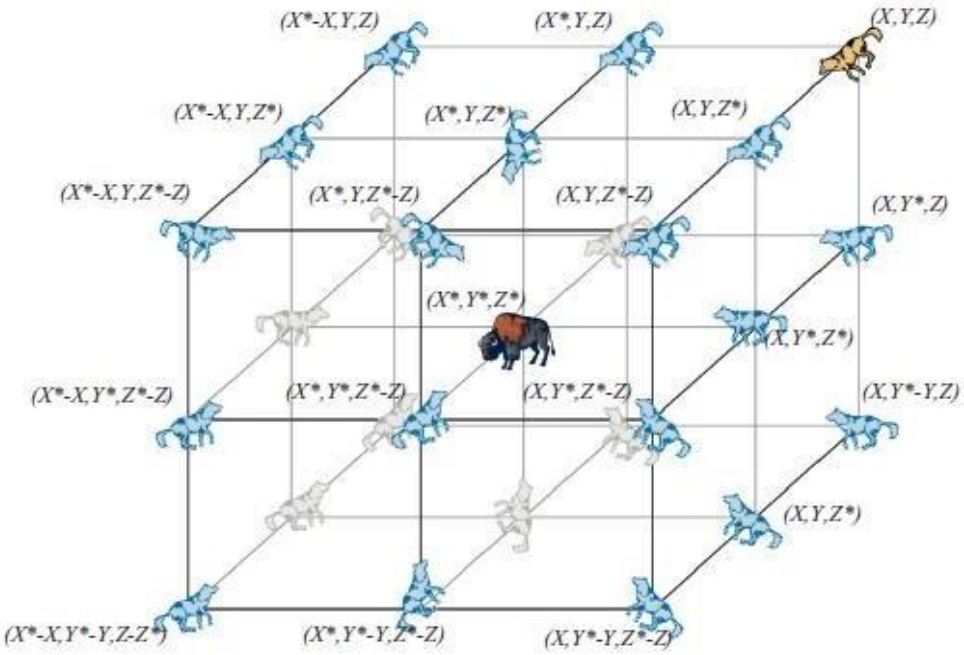

Figure 7: The wolf updated it is location in 3D space.

Hunting

Grey wolves can find the position of the prey and surrounding them, which in this algorithm can be managed by alpha. Besides, the beta and delta help in the hunting. This procedure can be formulated mathematically can be presented as follow:

5.| $E.q\ D_\alpha = |C_1.X_\alpha - X|,\ D_\beta = |C_2.X_\beta - X|,\ D_\delta = |C_3.X_\delta - X$

$E.q.6 X_1 = X_\alpha - A_1.(D_\alpha),\ X_2 = X_\beta - A_2.(D_\beta),\ X_3 = X_\delta - A_3.(D_\delta)$

Figure 11 demonstrates how is the agent update the new location regarding alpha, beta, and

delta. Note that a final location is a random place inside a circle, that created by locations of the alpha, beta, and delta. Thus, alpha, beta, and delta determine the location of the prey, and the rest of the wolves move in random positions

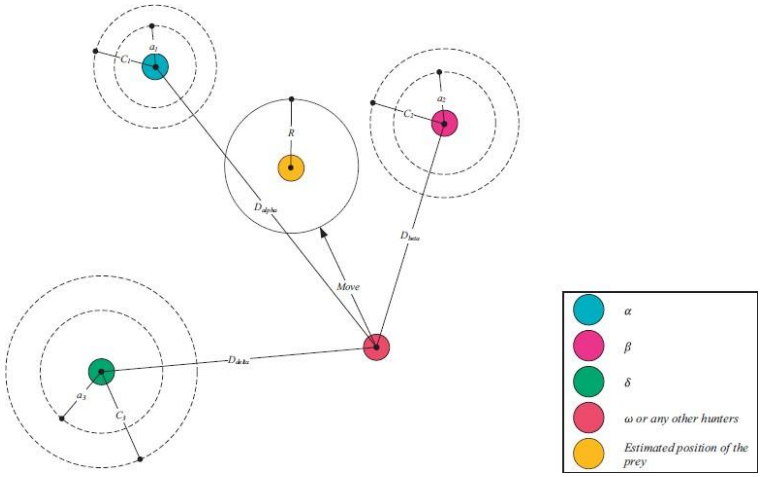

Figure 8: Updating the location in GWO

4. EXPERIMENTS AND RESULTS

In this part, several experiments will conduct, and experimental results are listed. Three types feature in this work are analyzed through BGWO feature optimization method. Also, the SMS phishing detection results are compared with previous researches.

Three experiments are produced to demonstrate the effectiveness and feasibility of the proposed method in this work. Firstly, SVM is employed to classify phishing and legitimate messages on its excellent performance. Then, ADASYN data pre-processing approach for imbalanced data is used to SMS phishing detection system.

Finally, the BGWO algorithm is used for feature optimization to improve the rapidity and validity of the proposed method. The dataset presented previously is applied in the experiments. Seven standard measurements including accuracy (ACC), False Positives Rate (FPR), True Positives Rate (TPR), precision, recall, F1-measure and Matthews Correlation Coefficient (MCC) are scheduled for evaluating the performance of proposed SMS phishing detection method.

To compare the obtained results with previous obtained results from others, different separations between training and testing datasets are employed in this work such as 3:7, 5:1, 4:1, and 3:1 as well as 10-fold cross-validation. The experimental parameters are specified as follows: the

termination condition of the BGWO algorithm is that the evolution creation is equal to the maximum iteration number. All the results are the average of 10 times happened experiments.

Experimental parameters are selected as a following:

The SVM algorithm assigned to t=50, The initial result of the GWO is s=20, and the highest number of the iteration assigned to be I=100. Thus, The GWO algorithm will terminate when the evaluation result equal to the highest number of the iteration. Furthermore, in the results we take the average of 10 repeated attempts in the experimental result. We use the MATLAB 2019a to apply all the experiments presented in this thesis.

Table 12 demonstrated that the GWO and ADASYN approach enhances the accuracy of Smishing detection at various levels despite the several separations between the datasets and training. The SVM algorithm was implemented to get the first part of the result. the optimal accuracy of 98.58% conducted with the separation of 4:1. Then the ADASYN shows the second part of the result with optimal accuracy at 98.75 and accomplished with the separation of 5:1. Finally, the GWO algorithm conduct the optimal accuracy at 99.25% and accomplished with separation at 5:1.

From the Result demonstrated in the table, the proposed method shows an outperformance in detecting the phishing comparing with other methods such as (Almeida et al., 2011; Tong et al., 2018). In addition, the proposed approach shows an improvement in the true positive rate and the recall values with 98.19% with 3:7 separation. This result designates that the proposed approach shows great performance in classifying the SMS phishing.

Table 4: The Expermintal results.

Separation	Approach	Accuracy (%)	TPR	FPR	Precisi on	Recall	F1-Measure	MCC
10-fold cross	SVM	98.48183	0.95369	0.06386	0.99012	0.94603	0.96959	0.94056
	ADASYN-	98.67940	0.960942	0.053	0.9894	0.96045	0.97105	0.94782
validation	SVM			41	2			
	ADASYN-GWO-SVM	98.84718	0.972593	0.04538	0.98785	0.97100	0.97743	0.95631
3:7	SVM	97.82676	0.93785	0.09012	0.98853	0.94106	0.95401	0.91853
	ADASYN-GWO	98.50077	0.94583	0.06341	0.98053	0.94210	0.96012	0.92190
	ADASYN-GWO-SVM	98.25967	0.953810	0.06742	0.98044	0.95078	0.96384	0.92917

5:1	SVM	98.24785	0.94991	0.07298	0.99067	0.94098	0.96687	0.93503
	ADASY-SVM	98.93468	0.96934	0.04578	0.98804	0.96085	0.97853	0.95146
	ADASYN-GWO-SVM	99.00925	0.98105	0.04919	0.98749	0.97630	0.98339	0.96329
4:1	SVM	98.458387	0.95271	0.07820	0.99120	0.95051	0.97941	0.94015
	ADASYN-SVM	98.69167	0.96643	0.05055	0.98200	0.96150	0.97352	0.94238
	ADASYN-GWO-SVM	98.77146	0.967308	0.05276	0.98161	0.96978	0.97865	0.95019
3:1	SVM	98.78888	0.95683	0.06637	0.98950	0.94853	0.96940	0.93047
	ADASYN-SVM	98.98720	0.96874	0.05798	0.98904	0.95958	0.97933	0.93275
	ADASYN-GWO-SVM	98.77482	0.97760	0.05359	0.98832	0.96916	0.97702	0.94080

With 98.70% of accuracy, the LIWC show significant features accuracy, and the topic features show a 98.66% accuracy. Despite, the F1 and Recall values are chosen by the Topic features. This means that the covered topic possibility distribution of SMS has high efficiency in phishing detection.

Table 5: The Experimental results for each type of feature.

Features	Accuracy (%)	TPR	FPR	Precision	Recall	F1-Measure	MCC
LIWC features	98.70427	1.3743	0.09272	1.0043	1.01134	0.94595	98.70427
Topic features	98.66843	1.38562	0.08207	1.01562	1.01191	0.94529	98.66843
Token features	97.93289	1.357	0.09977	0.987	0.99548	0.9205	97.93289

GWO algorithm is applied to decrease the number of feature measures and enhance the computational performance in this thesis. Table 7 illustrates the optimization result of the feature with the 10-fold cross approach. From the 179 features, we choose 87.4 which is nearly half of all feature's numbers.

The result show enhancement in the final result of phishing detection with half of all features as shown in table 4. For the Token, Topic and LIWC features, the average chosen feature is 14.5, 27.7 and 49, respectively. The performance of these types, each type is selected at a different rate. The maximum selected rate is 53.26% is introduced in the topic features, then the LIWC with 52.12% The result of the classification and rate illustrated in table 7. The results demonstrate that the Topic and LIWC features have significant performance,

accordingly, the more related features are selected by the GWO algorithm. But the Token features have low accuracy, and that the reason for selected a small number of features. Overall, the GWO algorithm chose the optimal sequence of the features and present promising achievements in detecting phishing SMS.

Table 6: The Feature optimization result.

Feature Type	Number of all Feature	Average chosen Number	Rate
All features	179	87.4	48.82%
Token features	33	14.5	43.93%
Topic features	52	27.7	53.26%
LIWC features	94	49	52.12%

To show the effectiveness of the presented approach, we compare our results with four different previous studies proposed SMS phishing detection methods using the same dataset. In (Almeida et al., 2011) present an approach achieve accuracy of 97.64% and 34% selected samples to toning the training and select 70% for testing and compare with other classification approaches (Karami et al., 2014)achieves a 99.21% accuracy and select a 480 feature. However, this study presents a new topic and token feature for SMS in combination with an oversampling approach and optimization algorithm for features.

The proposed method in this thesis achieves 99.25% accuracy by using only an average of 87.4 of features. Besides, our work shows better performance in the topic and token features at 98.66% and 97.93% compared with (Karami et al., 2014) which achieves 94.69% and 97.99%.

Enaitz et al. (Ezpeleta, Garitano, Zurutuza, & Hidalgo, 2017)present an approach to analyzing the SMS messages, the method achieves 99.01%, compared with our approach which achieves a better performance of 99.25% accuracy.

Finally, Tong, W. U., et al, propose an approach for the SMS phishing detection, and with nearly similar data to our work, the proposed method achieves 99.01%, with the significant performance we achieve a 99.25% of accuracy (Tong et al., 2018).

By comparison, the GWO algorithm proposed in this algorithm shows an outperformance, high accuracy, and efficient approach. Figure 12 illustrates a comparison of accuracy results between different approaches.

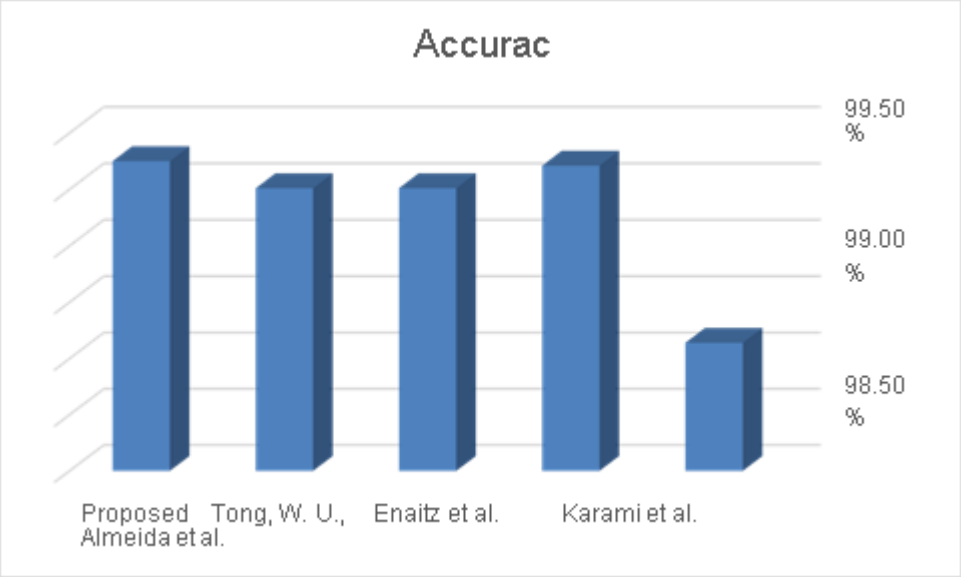

Figure *9:* Comparison between the proposed work and other methods.

In this paper, we introduce a Smishing detection approach using the oversampling and feature selection optimization algorithm to analyze the imbalanced data issue and distinguish between several types of features. Thus, we introduce three features with 32 and 50 for token and topic feature respectively, and LIWC with 93 features. Further, the SMS phishing detection systems suffer from imbalanced data, to solve this problem we propose an Adaptive Synthetic Sampling approach. Then, to reduce the size of the features and investigating to get the optimal features, the Gray Wolf algorithm (GWO) is employed.

To verify the proposed detection method three exterminates are developed using the Support Vector Machine (SVM) for classification to evaluate the performance of the introduced approach. The results show an outperformance for the proposed method with the combination of the GWO algorithm and the ADASYN method and show an improvement in detected the Smishing accuracy among the several features types. High accuracy is accomplished by this approach with 99.25% accuracy among 5 to 9 for training data and 1 to 6 samples for the data testing. The topic and LIWC features show superior performance up to 98.70% of accuracy in a single sample feature.

For more than half of the features that were selected the GWO algorithm accomplish a better performance in the accuracy of detection the Smishing. The topic and LIWC features show better achievements comparing with the token features. Consequently, the proposed approach against Smishing attacks using a gray wolf optimizer shows promising performance.

REFERENCES

1. Abdelhamid, N., Ayesh, A., & Thabtah, F. J. E. S. w. A. Phishing detection based associative classification data mining, 2014; *41*(13): 5948-5959.
2. Aleroud, A., Zhou, L. J. C., & Security. Phishing environments, techniques, and countermeasures: A survey, 2017; *68*: 160-196.
3. Almeida, T. A., Hidalgo, J. M. G., & Yamakami, A. *Contributions to the study of SMS spam filtering: new collection and results.* Paper presented at the Proceedings of the 11th ACM symposium on Document engineering, 2011.
4. Almomani, A., Gupta, B., Atawneh, S., Meulenberg, A., Almomani, E. J. I. c. s., & tutorials. A survey of phishing email filtering techniques, 2013; *15*(4): 2070-2090.
5. Balubaid, M. A., & Manzoor, U. J. a. p. a. Ontology based SMS controller for smart phones, 2015.
6. Chan, P. P., Yang, C., Yeung, D. S., & Ng, W. W. J. N. Spam filtering for short messages in adversarial environment, 2015; *155*: 167-176.
7. Chaudhari, A. S. J. R. M. T., Dept. of Mathematics, & Computer Science, E. U. o. T. Security analysis of SMS and related technologies, 2015.
8. Cheng, N., Chandramouli, R., & Subbalakshmi, K. J. D. I. Author gender identification from text, 2011; *8*(1): 78-88.
9. Choudhary, N., & Jain, A. K. *Towards filtering of SMS spam messages using machine learning based technique.* Paper presented at the International Conference on Advanced Informatics for Computing Research, 2017.
10. Costa, G., Ortale, R., & Ritacco, E. J. A. T. o. I. S. X-class: Associative classification of xml documents by structure, 2013; *31*(1): 1-40.
11. Croft, N. J., Olivier, M. S. J. I., & Africa, C. S. A. R. G. S. (2007). A silent SMS denial of service (DoS) attack. *29*.
12. easydns.com. Phishing attacks using SMS text messages. Retrieved from https://easydns.com/blog/2015/07/11/phishing-attacks-using-sms-text-messages/, 2015.
13. Egele, M., Stringhini, G., Kruegel, C., & Vigna, G. *Compa: Detecting compromised accounts on social networks.* Paper presented at the NDSS, 2013.
14. Ezpeleta, E., Garitano, I., Zurutuza, U., & Hidalgo, J. M. G. Short Messages Spam Filtering Combining Personality Recognition and Sentiment Analysis. *International Journal of Uncertainty, Fuzziness and Knowledge- Based Systems*, 2017; *25*(Suppl. 2): 175-189.
15. Goel, D., Jain, A. K. J. C., & Security. Mobile phishing attacks and defence mechanisms:

State of art and open research challenges, 2018; *73*: 519-544.

16. Gómez Hidalgo, J. M., Bringas, G. C., Sánz, E. P., & García, F. C. *Content based SMS spam filtering.* Paper presented at the Proceedings of the 2006 ACM symposium on Document engineering, 2006.
17. Group, A. P. W. *PHISHING ACTIVITY TRENDS REPORTS*. Retrieved from, 2019.
18. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf.
19. Gupta, B. B., Tewari, A., Jain, A. K., Agrawal, D. P. J. N. C., & Applications. Fighting against phishing attacks: state of the art and future challenges, 2017; *28*(12): 3629-3654.
20. He, H., Bai, Y., Garcia, E. A., & Li, S. *ADASYN: Adaptive synthetic sampling approach for imbalanced learning.* Paper presented at the 2008 IEEE international joint conference on neural networks (IEEE world congress on computational intelligence), 2008.
21. He, H., Garcia, E. A. J. I. T. o. k., & engineering, d. Learning from imbalanced data, 2009; *21*(9): 1263-1284.
22. Islam, M. R., Abawajy, J., & Warren, M. *Multi-tier phishing email classification with an impact of classifier rescheduling.* Paper presented at the 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009.
23. Jakobsson, M. J. C. F., & Security. Two-factor inauthentication–the rise in SMS phishing attacks, 2018; *2018*(6): 6- 8.
24. Ji, H., & Zhang, H. J. C. C. Analysis on the content features and their correlation of web pages for spam detection, 2015; *12*(3): 84-94.
25. Joo, J. W., Moon, S. Y., Singh, S., & Park, J. H. J. T. S. S-Detector: an enhanced security model for detecting Smishing attack for mobile computing, 2017; *66*(1): 29-38.
26. Junaid, M. B., & Farooq, M. *Using evolutionary learning classifiers to do MobileSpam (SMS) filtering.* Paper presented at the Proceedings of the 13th annual conference on Genetic and evolutionary computation, 2011.
27. Karami, A., Zhou, L. J. P. o. t. A. S. f. I. S., & Technology. Exploiting latent content based features for the detection of static sms spams, 2014; *51*(1): 1-4.
28. Kessem, L. J. S. o. S. Rogue mobile apps, phishing, malware and fraud.Khonji, M., Iraqi, Y., Jones, A. J. I. C. S., & Tutorials. (2013). Phishing detection: a literature survey, 2012; *15*(4): 2091- 2121.
29. Lambert, A. Analysis of spam.Lee, J., Cho, D., & Lee, J. (2011). An integrity verification method for secure application on the smartphone. *The Korean Institute of Information Technology*, 2003; *9*(10): 223-228.
30. Lemos, R. Phishing Attacks Increasingly Focus on Social Networks, Studies Show." eWeek.

In: July, 2014.

31. Lord, S. J. N. S. (2003). Trouble at the Telco: when GSM goes bad, *2003;* (1): 10-12.
32. Marforio, C., Masti, R. J., Soriente, C., Kostiainen, K., & Capkun, S. J. a. p. a. Personalized security indicators to detect application phishing attacks in mobile platforms, 2015.
33. Mathew, K., & Issac, B. *Intelligent spam classification for mobile text message.* Paper presented at the Proceedings of 2011 International Conference on Computer Science and Network Technology, 2011.
34. Mirjalili, S., Mirjalili, S. M., & Lewis, A. J. A. i. e. s. Grey wolf optimizer, 2014; *69*: 46-61.
35. Pannu, M., Bird, R., Gill, B., & Patel, K. *Investigating vulnerabilities in gsm security.* Paper presented at the 2015 International Conference and Workshop on Computing and Communication (IEMCON), 2015.
36. Reaves, B., Scaife, N., Tian, D., Blue, L., Traynor, P., & Butler, K. R. *Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways.* Paper presented at the 2016 IEEE Symposium on Security and Privacy (SP), 2016.
37. Sethi, G., & Bhootna, V. J. I. J. C. S. I. T. SMS spam filtering application using Android, 2014; *5*(3): 4624-4626.
38. Tausczik, Y. R., Pennebaker, J. W. J. J. o. l., & psychology, s. The psychological meaning of words: LIWC and computerized text analysis methods, 2010; *29*(1): 24-54.
39. Tong, W., ZHENG, K.-f., WU, C.-h., WANG, X.-j. J. D. T. o. C. S., & Engineering. SMS Phishing Detection Using Oversampling and Feature Optimization Method. (iece), 2018.
40. Uysal, A. K., Gunal, S., Ergin, S., & Gunal, E. S. *A novel framework for SMS spam filtering.* Paper presented at the 2012 International Symposium on Innovations in Intelligent Systems and Applications, 2012.
41. Uysal, A. K., Gunal, S., Ergin, S., & Gunal, E. S. J. E. i. E. The impact of feature extraction and selection on SMS spam filtering, 2013; *19*(5): 67-72.
42. Wang, C., Zhang, Y., Chen, X., Liu, Z., Shi, L., Chen, G., Development. A behavior-based SMS antispam system, 2010; *54*(6): 1-3: 16.
43. Warade, S. J., Tijare, P. A., & Sawalkar, S. N. J. I. J. o. R. i. A. T. An approach for SMS spam detection, 2014; *2*(12): 8-11.
44. Weider, D. Y., Nargundkar, S., & Tiruthani, N. *A phishing vulnerability analysis of web based systems.* Paper presented at the 2008 IEEE Symposium on Computers and Communications, 2008.

45. Xu, Q., Xiang, E. W., Yang, Q., Du, J., & Zhong, J. J. I. I. S. Sms spam detection using noncontent features, 2012; *27*(6): 44-51.
46. Yamakami, T. *Impact from mobile spam mail on mobile internet services.* Paper presented at the International Symposium on Parallel and Distributed Processing and Applications, 2003.
47. Yan, X., Guo, J., Lan, Y., & Cheng, X. *A biterm topic model for short texts.* Paper presented at the Proceedings of the 22nd international conference on World Wide Web, 2013/
48. Yeboah-Boateng, E. O., Amanor, P. M. J. J. o. E. T. i. C., & Sciences, I. Phishing, SMiShing & Vishing: an assessment of threats against mobile devices, 2014; *5*(4): 297-307.
49. Zainal, K., Sulaiman, N., Jali, M. J. I. J. o. C. S., & Security, I. An analysis of various algorithms for text spam classification and clustering using RapidMiner and Weka, 2015; *13*(3): 66.
50. Zheng, K., Wu, T., Wang, X., Wu, B., & Wu, C. J. I. A. A session and dialogue-based social engineering framework, 2019; *7*: 67781-67794.
51. Zhou, Y., & Jiang, X. *Dissecting android malware: Characterization and evolution.* Paper presented at the IEEE symposium on security and privacy, 2012.