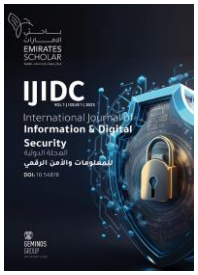

International Journal of Information & Digital Security
Vol 1 Issue 1 (2023)
Pages (1 –14)

Available at www.emiratesscholar.com

A NEW INTELLIGENT MODEL FOR PHISHING WEB SITES DETECTION

Saad M. Almalki[a], Nabih T. Abdelmajeed[b]

[a] *Naif Arab University for Security Sciences, Riyadh, Saudi Arabia*

[b] *Higher Colleges of Technologies, Dubai,, United Arab Emirates*

Abstract

In this paper, we propose a new version of neural network algorithm to enhance the accuracy of detecting website phishing attacks. The proposed algorithm is presented to update weights on multi layers network. The updated algorithm initially started by collecting and storing data in phishing website dataset. We compare the performance of neural network with several machine learning algorithms. The feature selection method applied by the improved neural network algorithms is effective for characteristic capturing with reasonable results. The neural network techniques involve innovative phishing detection model to extract the significant phishing features and patterns. The evaluation of the proposed method accuracy. Accuracy measures the phishing websites correctly detected as trusted websites among all instances. The main conclusion gained from this research is the effectiveness of neural network in detecting website phishing attacks. In addition, the incremental method used for combination of different datasets provided a good insight. We can conclude that the accuracy rate is dependent to the feature counts and dataset size. In addition, the proposed model helps to avoid loss of cumulative knowledge over time and even with the change of characteristics of phishing websites with respect to the designers and developers of these websites.

Keywords: Neural Network, Classification, Incremental Learning, Website Features

Email addresses: saadfame@gmail.com (Saad M. Almalki), nabdelmajid@hct.ac.ae (Nabih T. Abdelmajeed)

1. Introduction

Phishing attack is a type of social engineering attacks that users received spoofed emails to be permitted to share sensitive data or to bother and harm the victim. Victims may receive these emails as trusted websites, but they are not [1]. Phishing aims to trace the private information of users with no permission through a design of a new website imitate the trusted one [2] Phishing attacks are increasingly becoming sophisticated and pervasive utilizing SMS, VOIP, multi-player games, social networking sites, and instant messaging. Phishing also have shifted from the distribution of information to trick someone to spear phishing attacks that are more selective based on contextual information [1]. With the increasing threat of web phishing at great extent, the detection methods to detect phishing are still inadequate and limited. Furthermore, the phishing attackers might avoid detection by changing their strategies with lower costs [3].

Phishing has extremely gained the attention of research community of the modern technologies development for worldwide computer networks [4]. Commercial and academic research in phishing is an active area to merge the components of economics, public policy, machine learning, social psychology, and distributed systems [1]. As stated by [1] that has examined the mechanisms of phishing attacks and discussed how people fall in phishing attacks. In addition, the work involved an explanation of the actual damage caused by phishing. Subsequently, the survey has been closed with a set of countermeasures against phishing.

Some attackers utilize the security measures such as firewalls, certificates, two-step authentication methods, and encryption. Further, some phishing attacks seem like spams. Conversely, phishing attack can cause loss of identity and sensitive intellectual property, as well as loss of national security secrets [1].

There are many used techniques that face several challenges such as the performance that is degraded with the change of phishing websites characteristics with the increasing of database and the progress of time. Therefore, the construction of such that techniques lets the engineers to review the already built designs continuously, as well as the tools used to extract the best characteristics that assist to get a satisfied accuracy for phishing website detection. This will be investigated in more details in the next paragraph as we used Neural Network technique.

Neural network techniques have been widely utilized to build an effective tool to identify the phished website. Many phishing detection techniques are developed. However, they are dependent to URL only and the blacklist is not sufficient to detect unknown phishing websites. Further, the lifespan of the phishing website might be a few hours like zero phishing website. Neural network techniques allow developing faster recognition performance and reduced error, as well as increased performance [5]. In this paper, we introduced a new module that resolve the problem of pattern changes in the website characteristics over time without the loss of previous knowledge obtained from the groups of data in addition to the search of the most important characteristics that allow us to categorize these sites in accurate way and to reduce the opportunities for the designers of these websites to know the way of detecting phishing websites.

The rest of the paper is organized as follows. Section 2 presents a background about the phishing website and highlights on the related works in this area. The proposed module will be provided in section 4 after presenting the motivations in previous section. Finally, an implementation of the proposed module and the result discussion are shown along with a conclusion in last section.

2. Literature Review

2.1. The Features Of Phishing Websites

Many characteristics are available for discriminating phishing website from trusted ones. Phishing detection can be done through checking website and searching the characteristics of the source code. In this research, we present an improved neural network algorithm for phishing detection by checking some characteristics of website to detect the phishing websites instead of just checking blacklist. These characteristics are classified as follows:

1. Using the IP Address
2. Using URL

A. Long URLs
B. Using URL Shortening Services (Tiny URL
C. URL with @ Symbol
D. .htaccess Redirecting
E. Adding Prefix or Suffix Separated by (-) to the Domain
F. Sub-Domain and Multi Sub-Domains
G. HTTPS
H. Using Free Hosting Domains
I. Favicon
J. Using Non-Standard Port
K. The Existence of (HTTPS) Token in the Domain

3. Abnormal based Features

A. Request URL

B. URL of Anchor

C. Links in <Meta>, <Script> and <Link> Tags

D. Suspicious Action Upon Submitted Information

E. Submitting Information to Email

F. Website's Owner

4. HTML and JavaScript based Features

A. Redirect Page

B. Status Bar Customization

C. Disabling Right Click

D. Using Pop-up Window

E. IFrame

5. Domain based Features

A. Age of Domain

B. DNS Record

C. Website Traffic

D. PageRank

E. Google Index

F. Number of Links Pointing to the Webpage

G. Statistical Reports based Feature

These previous characteristics are extracted from the website to check their parameters in the source code. If there is a phishing character, the initial secure weight will be decreased. After that, the final weight is calculated as security rating; the highest rated website indicates the website is most likely to be a phishing website. Multilayer neural network is applied against phishing websites and the evaluation of its effectiveness based on feature set, using phishing dataset and implementing neural network systems. A cross-validation mechanism is used to evaluate the performance of the improved neural network algorithm implementing multiple activation functions and hidden units. The next section will describe each characteristic.

2.2 Neural Network

The original goal of the ANN approach was to solve problems in the same way that a human brain would. However, over time, attention focused on matching specific tasks, leading to deviations from biology. ANNs have been used on a variety of tasks, including computer vision, speech recognition, machine translation, social network filtering, playing board and video games and medical [6]. In neural networks we have back-propagation and forward-propagation. Multilayer neural network is applied against phishing websites and the evaluation of its effectiveness based on feature set, using phishing dataset and implementing neural network systems. A cross-validation mechanism is used to evaluate the performance of the improved neural network algorithm implementing multiple activation functions and hidden units.

A challenging problem when designing a classification model for dynamic domains (as in phishing websites classification problem) is how to make the model learns continuously from evolving data sets. Resolving this issue demands a technique that can trace any changes that might affect the classification model overall accuracy; hence, revising the decision boundaries accordingly. Such a situation requires a learning schema that offers balance between stability and plasticity.

2.3 Related Work

A proposed by [4] model to predict phishing attacks based on artificial neural network trained by propagation algorithm for website phishing classification. A high acceptance ability of the proposed model for high prediction accuracy and fault tolerance for noisy data in terms of false negative and false positive rates. The neural network model has connection weights that are altered frequently in training to reach accepted solution. The proposed model is applied in the field of information to determine how neural networks can achieve acceptable predictive performance and identify the neural network architecture to predict phishing websites. The number of hidden layers, momentum value, and number of hidden neurons to provide optimal predictive accuracy. The results showed crucial suitable number of hidden neurons in neu- ral network construction for improved performance. The overall performance confirmed the impact of neural net- works as a good technique for prediction phishing web- sites. However, the automation of neural network requires reduction in training run time.

The paper of [7] has provided an integration between fuzzy systems and neural networks to combine the advan- tages of both techniques. A new neuro-fuzzy approach was proposed base on rules to detect phishing attacks by calculating the heuristic value of membership func- tion. Neural network generates the weights. The system model established a mechanism for phishing sites detec- tion via deploying neuro-fuzzy network and considering page rank, primary domain, alexa rank, path domain, sub- domain, and alexa reputation. The training dataset has been used for the experiment in addition to two testing dataset. The evaluation of the approach revealed 99% detection ratio from 10,000 legitimate sites and 11,660 phishing sites. The comparison between the proposed technique and the other techniques has been also carried out to confirm the efficiency of the proposed technique. However, it could be improved and enhanced for better de- tection ratio and evolving larger dataset with more heuris- tic parameters.

[8] presented a detection and prediction mechanism or framework of phishing mails based on neural fuzzy approach. The proposed framework, namely Phishing Evolving Neural Fuzzy Framework (PENFF), can detect phishing mails considering the level similarity between features of URL email and body email. The common vector of features is managed by the rules followed to predict the phishing email. It was designed to deal with zero day attack. The results proved the ability of the proposed framework in detecting phishing mails and the improved performance of detection ratio, as well as the decreased value of error rate during the process of classification. It was a highly compacted framework according to the small values of non-dimensional error index and root mean square error as performance indicators. In addition, the framework has learning capacity. However, it has consuming footprint memory and needs to include dynamic system on real implementation.

The goal of the project presented by [9] was to implement a multilayer neural network with feedforward on phishing email detection. They also have evaluated the effectiveness of the proposed approach. Feature set was designed and phishing dataset was used to implement neural network system with the application of cross-validation technique to assess its performance testing multiple numbers of hidden layers and activated units. The evaluation also included a comparison against main machine learning approaches. The results revealed that the neural network achieved a satisfied level of accuracy with a suitable number of hidden layers and with scarce training instances. Feature selection method that has been used is effective to capture phishing mails. Two activation functions have been used to compare the performance of neural network namely sigmoid function and hyperbolic tangent function. The results also showed a noticeable improved performance of the sigmoid function better than hyperbolic function. A small training dataset size was examined to demonstrate the dataset overfitting. In conclusion, the precision was over than 95% and the high recall in detecting phishing mails with small portion of mails.

[10] has discussed how to predict the phishing websites based on neural network that works on multiple layers to reduce the errors and increase the performance. It also described a better framework of classification in prediction phishing sites with lower error rates.

[11] used neural network to rapidly detect suspected email with pruning strategy in order to determine if the email is legitimate or suspected. The version of neural network is based on multilayer feedforward neural network to extract features to identify the phishing email. The key features were specified and extracted using pruning approach to identify the features that play a major role in determining the phishing mail from legitimate one. The experimental design has verified that the proposed approach can be implemented using dataset containing phishing mails. Using weight elimination pruning technique, the number of features was reduced to minimal number, 18 features, taken to perform the experimental implementation of the proposed approach. The effectiveness of the proposed approach was determined by testing it on a dataset containing 4000 emails to decide ham and phish instances. Moreover, the results showed satisfactory performance with respect to false negative and false positive. The experiment conducted indicated enhanced detection rate in short time. However, new features may evolve and need to be classified accurately incorporated with the new input features of the training domain.

In the article of [12] , an intelligent model to predict phishing attacks has been proposed considering an artificial neural network called self-structuring neural network. The main goal was to improve the structure of network and coping with the constant changes. The work also included several experiments conducted with more than one epoch. The model solved the problem by creating an automated procedure to structure network and show high accepted level of outlier data, as well as high prediction accuracy with fault tolerance. The training model used in the experiment improved the network performance that also adjusted learning by adding new neuron to the hidden layers.

[13] analyzed and combined the phishing web forms and phishing emails into one framework to extract features and constructing feature model. The framework can classify phishing emails from legitimate ones, as well as suspicious emails to detect phishing attacks in accu- rate manner. They used adaptive neuro fuzzy inference system combined with different sources of extracted fea- tures. Two-fold cross-validation approach was performed to evaluate the proposed system. The results showed higher accuracy of the intelligent phishing security ap- proach. The web forms have been also examined to deter- mine and extract the most effective features required for classification of phishing websites. 56 features have been utilized to apply the algorithm and specify the features based on sensitive information. The promising results presented and demonstrated effective phishing detection by applying feature model.

Expose neural network based on deep learning approach have been developed by [14] to analyze input such as malicious URLs, registry keys, file paths, named mutexes, and named pipes. The learning algorithm was also trained to extract features and classify inputs using neural network and character level embeddings. Feature design and feature extraction approaches have been fully automated to outperform manual feature extraction and other intrusion detection issues. The proposed approach enables implicit extraction of features which immediately affect the optimization of classification better than natural language processing. The percentage of detection rate enhancement was between 5% and 10% with 0.1% false positive rate in comparison with other approaches. However, the experiment was costly in terms of computations of training dataset taking long strings which prohibited implementing more complicated scenarios.

The author [2] have proposed a supervised feature extraction mechanism to solve the problem of phishing samples that have similar features with trusted ones. The proposed mechanism called weighted feature line embedding can virtually generate training samples through the utilization of feature line metric. The approach can solve small sample size problem and corrects unwanted the quality of abnormal samples by assigning proper weights for each pair of feature points. These extracted features can improve the performance of phishing detection even withsmall training data set. The improved method embeds fea- ture line in discriminant analysis to provide virtual sam- ples that deal with small size of sample training set. The considered training sample was divided into two groups: normal samples and abnormal samples. Normal samples are appropriate for classification because the similar sam- ples belong to the same class or a different class, while abnormal samples cause classification error because the non-similar samples belong to the same or another class. It degrades the negative effort of abnormal training sam- ples and decreases the classification error because of neg- ative effect to abnormal training set. However, the perfor- mance becomes slow when the number of training sam- ples is limited.

The paper of [15] presented a client side software for protection from phishing attacks as an extension to Firefox browser integrated into the toolbar to check whether the recipient website is trusted or not. It can block the suspicious website based on the evaluation of the URL to the corresponding features including heuristics characteristics such as primary domain, sub-domain, and path. In addition, Naïve Bayes classifier was implemented using four lexical features integrated with page ranking to classify the URL. It does not require any server change to be made on to prevent fraudulent websites for phish- ing utilizing URL deceptive. The proposed approach used URL structure with page ranking and four lexical features for capturing phishing attacks depending on the deceptive links and URLs through a third party service and search engines. It also serves as an architecture for anti-phishing. The phished website will warns the user by changing the color and providing the user with the ability to unblock the website through adding a trusted list. Additionally, a report would be viewed to the user in the case of phishing site. The approach minimized the false positive. The experimental result showed the improved accuracy of the approach.

[16] introduced feature selection to determine the effective feature set helping in classifying websites into phishing websites. Two common features selection methods have been explored and compared to define the least features of phishing detection. Data mining techniques have been utilized to conduct experimental tests to the huge number of features in the dataset. The main concerning question of the paper is “can small features sets be identified and used to generate high predictive classifiers?”. It also tried to search for small set of websites features not hinder the accuracy of classifier against phishing. The training of data mining algorithms have been trained on several sets of selected features to show and identify new knowledge in the forms of rules among significant features. The labels of phishy and legitimate are used to classify the websites according to the training data containing many features and attributes of websites with the class attributes which is the label. The promising direction of phishing is to reduce the dimensionality of search space by eliminating irrelevant features and grouping relevant features together for automatics

classification of websites, as well as to minimize computing resources. Two algo- rithms have been applied namely decision tree and rule in- duction. The feature selection methods that have been chosen are broadly used in multiple domains with proven quality of filtering features. The results revealed that the redun- dant classifiers can degrade the phishy prediction rate.

[17] have introduced better methods for phishing prediction and detection based on URL exploration to be analyzed using machine learning models such as feature engineering approach and random forest, compared to the proposed novel method developed from recurrent neural networks. The main focus was on using machine learning techniques to classify websites according to their URLs. The features have been manually created for classification using LSTM model. The proposed model was based on character sequence and prediction of URL. The results confirmed that the proposed approach provided high accuracy rate with no need to manually perform feature selection. It is also a scalable and proactive detection methods based on fast acting and does not need complete content analysis. The evaluation validated the proposed approach in corpus phishing URLs with achieved accuracy in terms of evaluation run time and coverage to data. However, the inner working cannot be easily interpreted. Moreover, it requires far more training data and time to expertise satisfied result.

The use of random forest machine learning approach was investigated and reported by [18] to classify the phishing attacks looking forward a major goal in getting better prediction and classification accuracy of development and improvement of phishing email classifiers. The number of prominent features was also was concerning in the paper noticed in the dataset containing 2000 phishing mails. Training and testing datasets have been specified on the classifier and considering 10-fold cross-validation that divides dataset into 10 segments. In the first round, 9 of the parts are used as training dataset and the remaining part is used as testing dataset. In the second round, the 9 parts change to include other parts, and so on till 10 times. The training results obtained from the earlier rounds used to validate next rounds. Content-based phishing approach was presented to bridge the gap identified by literature. It proved its high classification accuracy. The classification accuracy was 99.7%, whereas false positive and false negative was low, which was 0.06%.

A novel dynamic phishing detection framework was proposed by [19] to adapt the evolving connectionist system with neural fuzzy framework. The proposed approach is hybrid combining supervised an unsupervised learning approaches. the detection is done in both states offline and online learning for dynamic detection of the phishing email involved as zero day phishing mails. The proposed framework was designed to work in high speed life long and with low memory footprint that can reduce the complexity of the implemented rules. Moreover, the number of rules was also minimized based on the configuration for email classification to achieve high performance and high detection rate in terms of precision, accuracy, sensitivity, F-measure, true negative, and true positive.

3. Motivations

Phishing websites aims to convert the way of how legitimate users receiving unwanted signals from the websites they are browsing [20] . To detect phishing, many detection methods have been introduced to prevent like attacks, but the current approaches are suffering from the following issues:

3.1 First Motivation

Most of these samples suffer from classification errors and Slow to implement in real time applications and cannot be easily manipulated [2] .

3.2 Second Motivation

Till now, the specialists in information security have not been agreed on a single definition of the characteristics and features that discriminate phishing websites. For this reason, many reliable training samples for detection phishing issues are not adequate and need more investigate

3.3 Third Motivation

The ability of phishers and the designers of phishing websites to detect the architectures of models and systems work as well as the used features that let them change the design an use different features to mitigate detection. This leads to attain ineffective models for phishing websites detection and the increasing of the neediness to update databases and the design of websites.

4. Proposed Module

With high increase of the number of phishing websites and its presence on the web, as well as the effects on the users, businesses, limited tools, and systems for phish- ing websites detection the demand of developing a new model to detect phishing

website becomes a curious need- iness. This refers to the knowledge of the attackers about the design of the websites and the architecture of these systems as well as the changes in the types and patters of the websites over time.
Our study creates a designated model to adopt these changes by specifying all the important features and choosing a subset of them through an algorithm to produce high accuracy of results for phishing websites detection and based on previously collected and up to date databases, and then use them to train the proposed model and keep providing newly updated changes over time. Moreover, this model saves the secret of the architecture and mechanism of system processing. In addition, protecting how the system choose the features to get high accuracy in detecting phishing websites without degrading the performance by making a balance between the number of features and the accuracy obtained. . But the proposed module faces some challenges which were presented in the next section.

5. Challenges and Contributions

One of the main challenges that addressed by the paper is dealing phishing websites and their features. Therefore, we will use different datasets documented and integrated to be used for training and development of the proposed model with the ability to keep these datasets up to date. Another challenge, there are many features used for phishing websites, but the selection of the best and im- portant features that describe the phishing websites in a proper accuracy. To enable these features to describe the phishing websites, we will use an algorithm for most im- portant features selection to allow classify the websites. The last challenge was how we keep the design of model to detect phishing websites in accurate way and with the use of a specific number of features of the web- sites in a way that hide the architecture and the mecha- nism of detection and the features used for categorization of these websites as well as the use of a maximum num- ber of datasets in building the model and keeping the data updated.

6. Proposed Solution

The proposed algorithm was presented to update weights on multi layers network. The updated algorithm initially started by collecting and storing data in phishing website dataset. We are going to compare the performance of neural network with several machine learning algorithms. The feature selection method applied by the improved neural network algorithms is effective for characteristic capturing with reasonable results. The neural network techniques involve innovative phishing detection model to extract the significant phishing features and patterns.

In our methodology, we prepare dataset that contains various types of phishing threats including their signatures and other attributes. The dataset will be trained using Neural Network. We will divide the huge dataset into smaller segments and then add them one by one in the training of the algorithm. The repeated instances will be ignored and eliminated. Only the new instances of signatures will be added and considered for later trainings. Different training times will enhance the ability of the algorithm to predict the phishing attacks from usual mails. These repeated trainings would be compared and then augmented in one integrated dataset that enlarges once we add new kinds of attacks from the upcoming datasets. During the addition of new dataset, the accuracy of detection could improve the final accuracy of testing and then enhance the performance of neural network.

The proposed algorithm was presented to update weights on multi layers network. The updated algorithm initially started by collecting and storing data in phishing website dataset. We are going to compare the performance of neural network with several machine learning algorithms. The feature selection method applied by the improved neural network algorithms is effective for characteristic capturing with reasonable results. The neural network techniques involve innovative phishing detection model to extract the significant phishing features and patterns.

The enhanced performance of the proposed neural network as a mathematical model for the structural and functional properties. It is a computation approach and adaptive system to structure the orientation of flows of information in the learning phase. The features of neural networks enable learning and training input values with weighted factors manipulated to bring out the output. The units of neural network achieves simple computation of input to generate new activation level of each output link. The values of the activation level are based on the neighbor nodes and input link weights.

6.1 Feature Selection

Data clustering, optimization, classifica- tion, and pattern matching have large number of dramat- ically interconnected processing components working in parallel to structure regular architecture for classification process. Two combination methods are the units of neural network as input functions and activation functions.

The most common and important attributes are determined by applying feature selection method. The features also can be selected manually. PCA will be used for feature extraction.

Feature selection is performed in the classification process to identify phishing websites containing huge number of features for detecting attack. The approach utilized neural network to make use of similar values to create processing systems. Data clustering, optimization, classification, and pattern matching have large number of dramatically interconnected processing components working in parallel to structure regular architecture for classification process. Two combination methods are applied in the proposed model to include the units of neural network as input functions and activation functions.

6.2 Neural Network

One reason why phishers keep changing the features combination when creating phishing websites might be that they have the ability to interpret the anti-phishing tool and thus they pick a new set of features that can circumvent it. However, besides the generalization capability, fault tolerance, and strong ability to learn, a Neural Network (NN) classification model is considered as a black box. Hence, if someone has the skills to hack into the NN based classification model, he might face difficulties to interpret and understand how the NN processes the input data in order to produce the final decision. Other reasons include the easy of construction of NN, the ability of NN to deep learning an knowledge, and the capacity of NN to deal with big data.

The type of neural network called feedforward back propagation frequently repeat the training of data to update weights of layers. Three pieces bounded by neu- ral network are structural design, activation function, and learning paradigm [22]. Further, it establishes additional hidden layers to import new features and then transforms training data into output. It is also called multi-layer perceptron that contains multiple layers of neurons that are activated as processing units. It is a kind of supervised machine learning techniques that is the dataset is trained and class label is known. It works on mapping a group of input layers and input data that are considered features in this case into a group of outputs that represent the class value [21].

The main reason that motivated us to choose neural network as a main approach of implementation is its nature of nonlinear data modelling and the ability to model inputs into outputs to discover data patterns. It also has a wide range of applications such as phishing detection, intrusion detection, financial forecasting, etc. In this study, phishing detection forms a classification issue that works around forecast phishing based on owned learning and generalization feature. The nature and learning feature of neural network made it a proper approach to classify and recognize such that problem of phishing detection [22].

The neural networks will be discussed as the key works and contributions to be addressed when creating any phishing detection model. In this chapter, we discuss the details of the proposed method based on the realiza- tion of up to data developments in phishing techniques as shown in the previous chapter. The building of NN is not so difficult, but the attacker who wants to outbreak the website can do it in different ways. However, we might find a common method that the phishing attackers use to make phishing mails seem genuinely as a well-known enterprise including their identifiers and logo. The attackers take the information from the official authentic website of the company. The main issue faced in this part is how to know which the website is under attacking. In fact, the full prevention of phishing attacks might not possible that lead enterprises to take several counter measures against phishing attacks.

The first step in our proposed approach is to build the neural network algorithm. We selected BPNN version. As known, neural network depends on the number of layers. Moreover, the more layers and cells used, the longer training times. However, it only consumes the time of training dataset not testing. Once the NN is built, it will be easy task to determine the attacking attempt. We purpose to use Java development to build NN. After that, we can change the algorithm such as changing some function or parameter lists. Our contribution will be advanced.

Each layer of NN algorithm has its own activation function, and we will allow to change it via set function. In practice, we will add several functions for feature extraction. Further, we will add a feature of changing the learn-

ing rate or the number of neurons in each layer, as well as the size of the layer. NN is a supervised machine learning algorithm that enforce to be trained in advance and then building the model.

The enhanced performance of the proposed neural network as a mathematical model for the structural and functional properties. It is a computation approach and adaptive system to structure the orientation of flows of information in the learning phase. The features of neural networks enable learning and training input values with weighted factors manipulated to bring out the output. The units of neural network achieves simple computation of input to generate new activation level of each output link. The values of the activation level are based on the neighbor nodes and input link weights.

7. Implementation and Results Discussion

A major concerning issue faced by the designers and developers of classification models for domain-specific applications such as phishing detection is the problem of model learning and training to allow continuous evolving of dataset. To resolve this issue, we have designed an efficient technique that can adapt and accommodate the changes in phishing classification and detection models in terms of the accuracy. In this case, we need a learning model to make a balance between flexibility and stability. The proposed algorithm was presented to update weights on multi layers network. The updated algorithm initially started by collecting and storing data in phishing website dataset. We are going to compare the perfor- mance of neural network in different scenarios of features selected. The feature selection method applied by the improved neural network algorithms is effective for char- acteristic capturing with reasonable results. The neural network techniques involve innovative phishing detection model to extract the significant phishing features and
patterns.

In our methodology, we prepared dataset that contains various types of phishing threats including their attributes. The dataset was trained using Neural Network. We divided the huge dataset into smaller segments and then add them one by one in the training of the algorithm. The repeated instances were ignored and eliminated. Only the new instances of signatures have been added and considered for later trainings. Different training times can enhance the ability of the algorithm to predict the phishing attacks from usual mails. These repeated trainings are realized, compared and then augmented in one integrated dataset that enlarges once we add a new kind of attacks from the upcoming datasets. During the addition of new dataset, the accuracy of detection could improve the final accuracy of testing and then enhance the performance of neural network.

7.1 Data set

The dataset we used was collected via a special automated tool by [23]. It includes 30 features (integer values) that have been extracted based on suggested extractioning rules. The dataset was collected from google search operators, PhishTank archive, and MillerSmiles archive. Number of instances is 2456. The main associated task for this dataset is classification.

The lack of a reliable training dataset is one of the main challenges faced by researchers. Conversely, many studies have developed prediction mechanism for phishing attacks but they have used not reliable training dataset that are public available. Moreover, there is no agreement on the definitive features that help to forecast phishing sites according to the literature. Thus, we are facing a difficult task in choosing a reliable dataset that includes most types of features and selecting the most important features at the same time [24].

The data input is received by the algorithm to decide what is the similarities among different datasets to avoid duplicates. After importing the dataset, the output and the final result of NN appears immediately. The result ranges from -1 to 1. Normal takes -1, while phishing takes 1. 0 is cannot be defined. The output then is corrected and verified and if the result is as expected and accepted, then it will be considered. Otherwise, the dataset should be trained from beginning. In each repetition, it's better to add this data to dataset for the network performance. In addition, the accuracy depends on epsilon.

First, we import the dataset for training and build the NN that includes the setting of network parameters. In this situation, we define the parameters as follows: hidden layer size, layer neurons, activation function, and number of layers. Furthermore, we have to set learning rate, maximum epoch, and epsilon. The second step is to train the algorithm on the dataset and then check if the output error is lower than the defined epsilon or not. The weight of NN should be enough to the output result for the provided dataset. The performance of the algorithm will be verified through testing

7.2 Installed Programs

7.2.1 JDK 1.8 update 152
7.2.2 IDE: Eclipse Oxygen 2017.9.

7.3 Implementation and Testing

In this subsection, we explain the main steps we carried out to achieve our intended objectives. At first stage, data preparation takes place to set data input and transform it to compatible format and type. Data set is divided into multiple data input turns; this means that at each run or turn, we add a new data set and compare between the old and new dataset looking for new instances that have not been investigated before.

This procedure helps to cover the most types of phishing attacks and then getting higher accuracy of detection. As known, the greater number of instances, the greater value of detection ratio. It refers to the training and learning of model on dataset that become more and more smart. We add several segments of the whole dataset in order way and show how the accuracy is affected after each addition.

The approach starts with setting the model and selecting the dataset. Followed by building and training the model. After that, testing and verifying the model on a different dataset as follows..

7.4 Results Discussion

At this time, we should verify the results by performing an experiment of Neural Network but with different verification dataset. Figure shows the specification of verify option. The result her is 94% with 7 features selected.

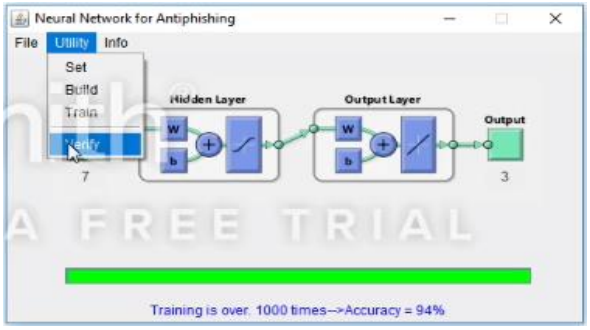

Figure1: verification model

Now, verify.txt file is chosen to verify the results obtained.

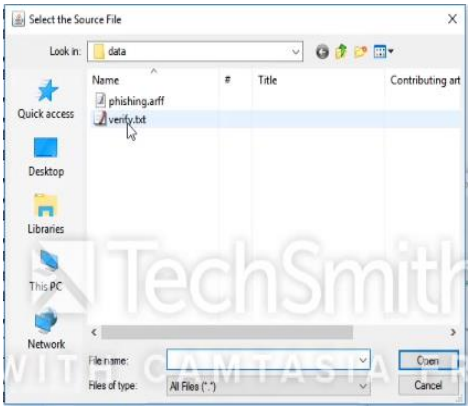

Figure shows the class value predicted by the algorithm based on the features selected in the experiment. The final class value is either -1 or 1 in this case.

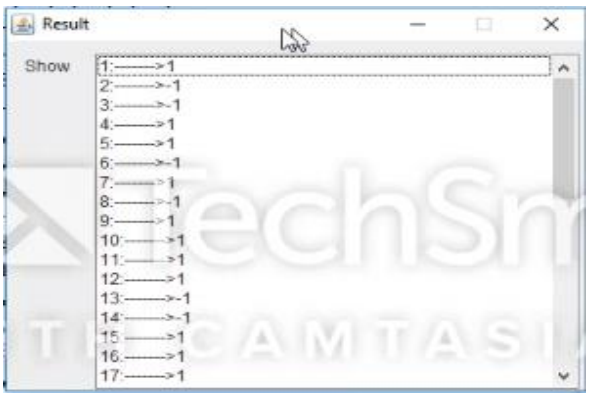

Figure 3: prediction results

This scenario shows the verification process. We also have to build the model again as shown in Figure.

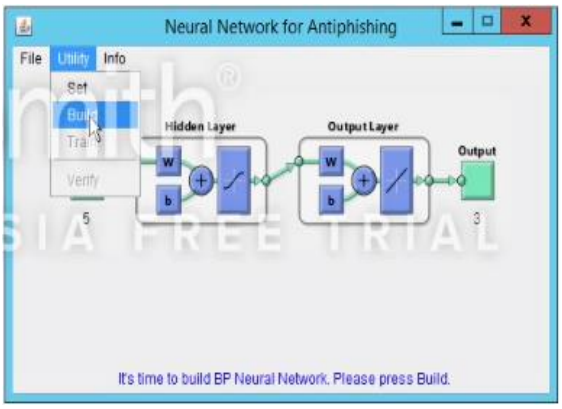

Figure 4: building model with parameter setting

Figure shows that we have added 4 datasets to the training and verification model. In addition, 7 features are selected and three values in the output layer.

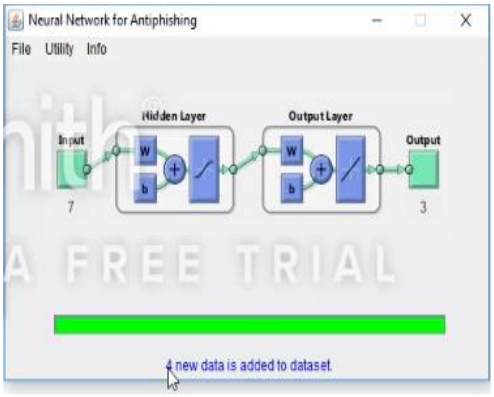

Figure 5: number of datasets used.

Five features show 92% accuracy as shown in figure.

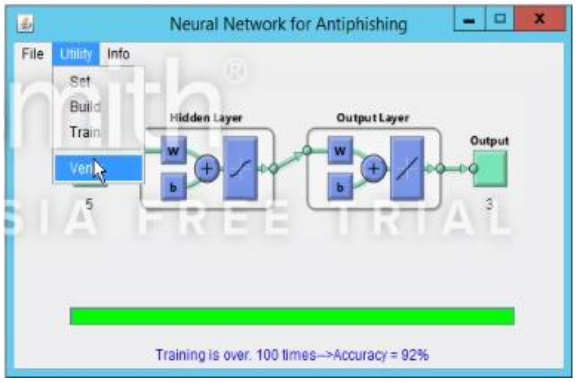

Figure 6: Accuracy
The five features are shown in Figure.

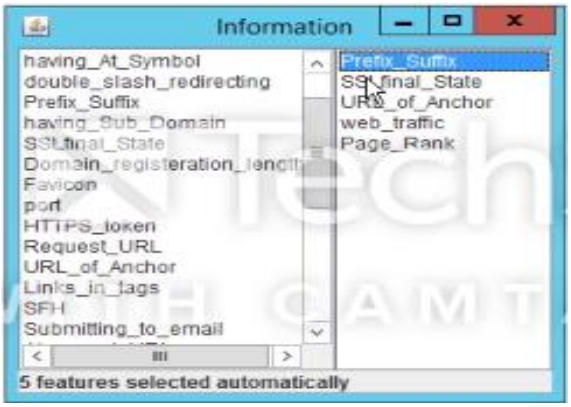

Figure 7: selected features
Now we are attempting to set 12 features and the number of iterations is 100 as shown in Figure.

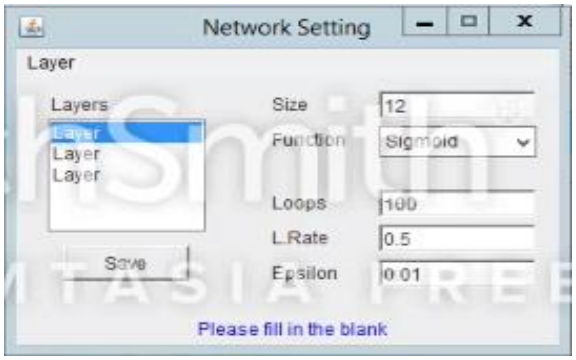

Figure 8 : parameter changes

If we set feature counts as 12, then we used 12 features for neural training. At this stage, the overall accuracy is improved and hence become 97%.

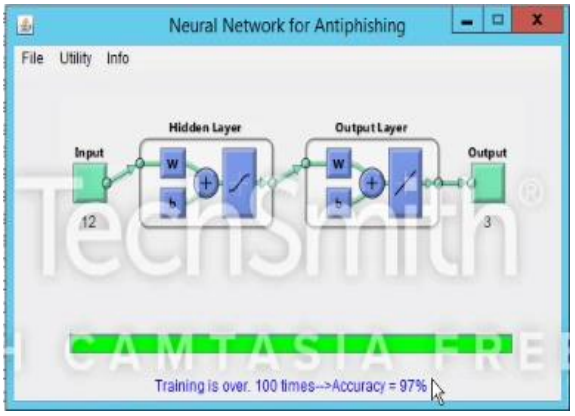

Figure 9: improved accuracy

7.4.1 Evaluation And Validation

In this section, we show the evaluation metrics of our proposed neural network approach. We will com- pute accuracy, false positive, and false negative. First, we will also show the effect of the selected features on the result by experimenting different scenarios with dif- ferent number and type of features. For 30 features, we got 98.37% in 100 iterations. For 18 features, we got 97.5% in 100 iterations. Figure shows these fea- tures. The accuracy rate is about 97% for Prefix Suffix, URL of Anchor, web traffic, having_Sub_Domain ,SSLfinal_State,Request URL,URL_of_Anchor, Links_in_tags, DNS Record, and PageRank.

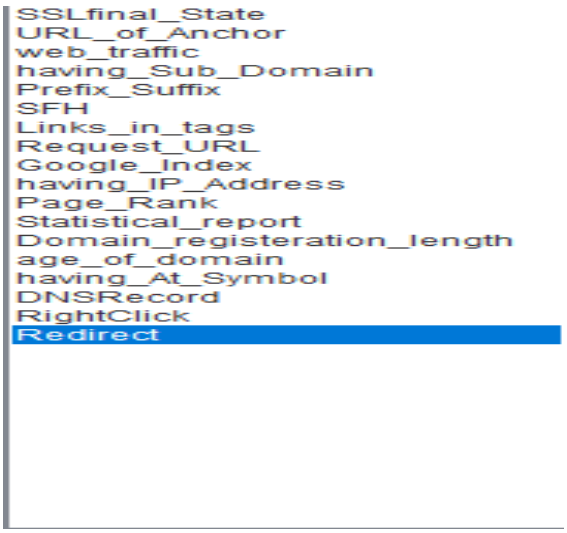

Figure 10: first scenario

For 15 features, we got 97.3% in 100 iterations as shown in Figure.

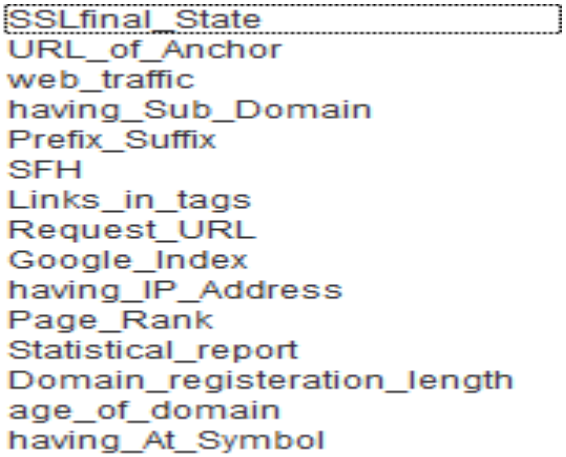

Figure 11: second scenario

For 9 features, we got 94% as shown in Figure.

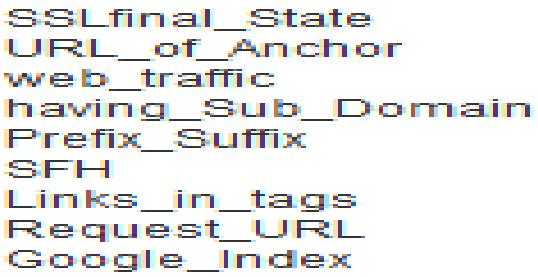

Figure 12: third scenario

For 5 default features, we got 92%. Prefix_Suffix SSL-final_State URL_of_Anchor web_traffic Page_Rank and for these 5 features, accuracy rate is about 92%

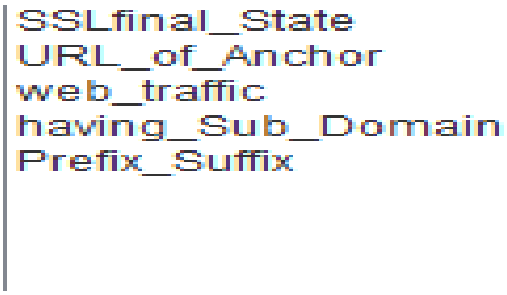

Figure 13: fourth scenario

We can conclude that the accuracy rate is dependent to the feature counts and dataset size.

7.4.2 Proposal Model Vs Other Modules

In this section, presented a comparative evolution of accuracy measure by implemented three different classifiers which they are Naïve Bayes, Neural Network and Random forest. The experimental results showed that the Neural Network achieved the high accuracy on 98.27% among others. Followed by Random Forest which achieved 97.38% and the worst given by Naïve Bayes 90.70%. The evaluation results in table 1 and print screen show for each classifier.

Table 1

Classifier	Accuracy Rate
Naïve Bayes	90.70%
Neural Network	98.37%
Random Forest	97.38%

This result is from program.

```
<--------- Random Forest Classifier -------->

Results
======

Correctly Classified Instances       10766               97.3858 %
Incorrectly Classified Instances       289                2.6142 %
Kappa statistic                          0.947
K&B Relative Info Score            1014104.2557 %
K&B Information Score                10045.8559 bits      0.9087 bits/instance
Class complexity | order 0          10951.3482 bits      0.9906 bits/instance
Class complexity | scheme           22487.9008 bits      2.0342 bits/instance
Complexity improvement     (Sf)    -11536.5526 bits     -1.0436 bits/instance
Mean absolute error                      0.0446
Root mean squared error                  0.1401
Relative absolute error                  9.0375 %
Root relative squared error             28.2074 %
Total Number of Instances            11055

Accuracy Rate: 97.38579828132067 %
```

```
<--------- Naive Bayes Classifier -------->

Results
======

Correctly Classified Instances       10027               90.701  %
Incorrectly Classified Instances      1028                9.299  %
Kappa statistic                          0.8111
K&B Relative Info Score             849020.4312 %
K&B Information Score                 8410.5129 bits      0.7608 bits/instance
Class complexity | order 0          10951.3482 bits      0.9906 bits/instance
Class complexity | scheme            4267.2181 bits      0.386  bits/instance
Complexity improvement     (Sf)      6684.1301 bits      0.6046 bits/instance
Mean absolute error                      0.1197
Root mean squared error                  0.274
Relative absolute error                 24.2585 %
Root relative squared error             55.1609 %
Total Number of Instances            11055

Accuracy Rate: 90.70104025327906 %
```

8. Recommendations and Future Works

In future, we plan to improve this research and enhance the proposed approach by applying different techniques for feature selection and extraction. In addition, we aim to improve the accuracy obtained in this work through im- plementing other types of neural network algorithm. An- other line of future direction for research is to investigate other features important to detect phishing attacks in dif- ferent domains.

9. Conclusion

During the paper, the main conclusion gained from this research is the effectiveness of neural network in detecting phishing mail attacks. In addition, the incremental method used for combination of different datasets provided a good insight. We can conclude that the accuracy rate is depen- dent to the feature counts and dataset size.

References

[1] J. Hong, The state of phishing attacks, Communications of the ACM 55 (1) (2012) 74–81.

[2] M. Imani, G. A. Montazer, Phishing website detection us- ing weighted feature line embedding, The ISC Interna- tional Journal of Information Security 9 (2) (2017) 49–61.

[3] Z. Futai, G. Yuxiang, P. Bei, P. Li, L. Linsen, Web Phish- ing detection based on graph mining, 2nd IEEE Interna- tional Conference on (2016) 1061–1066.

[4] R. M. Mohammad, F. Thabtah, L. Mccluskey, Predicting phishing websites using neural network trained with back- propagation, Proceedings on the International Conference on Artificial Intelligence (ICAI) (p. 1) (2013).

[5] C. J. Chandan, H. P. Chheda, D. M. Gosar, H. R. Shah, U. Bhave, A Machine Learning Approach for Detection of Phished Websites Using Neural Networks, International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC) (2) (2014) 12–12.

[6] Z. Zhang, Artificial neural network, in: Multivariate Time Series Analysis in Climate and Environmental Research, Springer, 2018, pp. 1–35.

[7] L. A. T. Nguyen, B. L. To, H. K. Nguyen, An Ef- ficient Approach for Phishing Detection Using Neuro-Fuzzy Model, Journal of Automation and Control Engi- neering 3 (6) (2015).

[8] A. Almomani, T. C. Wan, A. Altaher, A. Manasrah, E. Al- momani, M. Anbar, . . Ramadass, S, Evolving fuzzy neural network for phishing emails detection, Journal of Computer Science 8 (7) (2012) 1099–1099.

[9] Zhang, N., & Yuan, Y. (2013). Phishing detection using neural network. Department of Computer Science, Department of Statistics, Stanford University, CA, available at: http://cs229. stanford.edu/proj2012/ZhangYuanPhishingDetection UsingNeuralNetwork.pdf (accessed April 23, 2016).[Google Scholar].

[10] Martin, A., Anutthamaa, N., Sathyavathy, M., Francois, M. M. S., & Venkatesan, D. V. P. (2011). A framework for predicting phishing websites using neural networks. arXiv preprint arXiv:1109.1074.

[11] Kathirvalavakumar, T., Kavitha, K., & Palaniappan, R. (2015). Efficient Harmful Email Identification Using Neural Network. British Journal of Mathematics & Computer Science, 7(1), 58.

[12] Mohammad, R. M., Thabtah, F., & McCluskey, L. (2014). Predicting phishing websites based on self-structuring neural network. Neural Computing and Applications, 25(2), 443-458.

[13] Fehringer, G., & Barraclough, P. A. (2017). Intelligent Security for Phishing Online using Adaptive Neuro Fuzzy Systems. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 8(6), 1-10.

[14] Saxe, J., & Berlin, K. (2017). eXpose: A Character-Level Convolutional Neural Network with Embeddings For Detecting Malicious URLs, File Paths and Registry Keys. arXiv preprint arXiv:1702.08568.

[15] Kausar, F., Al-Otaibi, B., Al-Qadi, A., & Al-Dossari, N. (2014). Hybrid client side phishing websites detection approach. International Journal of Advanced Computer Science and Applications (IJACSA), 5(7), 132-140.

[16] Al-diabat, M. (2016). Detection and Prediction of Phishing Websites using Classification Mining Techniques. International Journal of Computer Applications, 147(5).

[17] Bahnsen, A. C., Bohorquez, E. C., Villegas, S., Vargas, J., & González, F. A. (2017). Classifying Phishing URLs Using Recurrent Neural Networks.\

[18] Akinyelu, A. A., & Adewumi, A. O. (2014). Classification of phishing email using random forest machine learning technique. Journal of Applied Mathematics, 2014.

[19] Almomani, A., Gupta, B. B., Wan, T. C., Altaher, A., & Manickam, S. (2013). Phishing dynamic evolving neural fuzzy framework for online detection zero-day phishing email. arXiv preprint arXiv:1302.0629.

[20] Asudeh, O., & Wright, M. (2016, October). POSTER: Phishing Website Detection with a Multiphase Framework to Find Visual Similarity. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 1790-1792). ACM.

[21] Yasin, A., & Abuhasan, A. (2016). An intelligent classification model for phishing email detection. arXiv preprint arXiv:1608.02196.

[22] Sharma, A., Singh, P., & Kaur, A. (2015). Phishing Websites Detection Using Back Propagation Algorithm: A Review.

[23] Mohammad, R. M., Thabtah, F., & McCluskey, L. (2012, December). An assessment of features related to phishing websites using an automated technique. In Internet Technology And Secured Transactions, 2012 International Conference for (pp. 492-497). IEEE.

[24] Mohammad, R.M., Thabtah, F. & McCluskey, L., 2015-C. Phishing Websites Dataset. [Online] Available at: http://eprints.hud.ac.uk/24330/ [Accessed 14 October 2017].