A SOFT COMPUTING APPROACH TO DETECTING E-BANKING PHISHING WEBSITES USING ARTIFICIAL NEURAL NETWORK

By

SHAFI'I MUHAMMAD ABDULHAMID * MUBARAQ OLAMIDE USMAN ** OLUWASEUN A. OJERINDE ***
VICTOR NDAKO ADAMA **** JOHN K ALHASSAN *****

** Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria.*
*** Department of Computer Science, Federal University of Technology, Minna, Nigeria.*

Date Received: *Date Revised:* *Date Accepted:*

ABSTRACT

Phishing is a cybercrime that is described as an art of cloning a web page of a legitimate company with the aim of obtaining confidential data of unsuspecting internet users. Recent researches indicates that a number of phishing detection algorithms have been introduced into the cyber space, however, most of them depend on an existing blacklist or whitelist for classification. Therefore, when a new phishing web page is introduced, the detection algorithms find it difficult to correctly classifies it as phishy. In this paper, we put forward a soft computing approach called Artificial Neural Network (ANN) algorithm with confusion matrix analysis for the detection of e-banking phishing websites. The proposed ANN algorithm produces a remarkable percentage accuracy and reduced false positive rate during detection. This shows that, the ANN algorithm with confusion matrix analysis can produce a competitive results that is suitable for detecting phishing in e-banking websites.

Keywords: Artificial Neural Network; E-banking; Phishing; Websites; Intelligent Algorithm; Soft Computing.

INTRODUCTION

Phishing is a type of cybercrime that is characterized as the way toward copying a site of a reliable company intending to acquire or pick up a secret data, for example, usernames credentials and Bank Verification Number (BVN) (Mohammad, Thabtah, & McCluskey, 2014). Phishing websites are made by questionable people to imitate the websites of legitimate sites. These sites have high graphical resemblances to the true legitimate ones trying to swindle the genuine web clients. Social engineering and specialized deceits are regularly consolidated together so as to begin this cyber-attack. Phishing websites have turned into a significant problem not just as a result of the expanded number of these sites but in addition the smart approaches used to design such sites, hence even clients having great involvement in the cyber security and web may be misled. Normally, phishers initiate attacks by sending email that is by all accounts from a credible or legitimate organization to targets by encouraging them to refresh or authorize their data by clicking a hyperlink that is contain in an email (Babagoli, Aghababa, & Solouk, 2018; Idris & Abdulhamid, 2014; Madni, Latiff, Coulibaly, & Abdulhamid, 2017). Phishing detection techniques uses user verified URL blacklist or whitelist. In any case, the blacklist or whitelist is frail as far as recently showing up phishing websites and cannot distinguish phishing website in the case of spear-phishing, when the attacker purposefully tries to make hurt specific victims. Figure 1 shows a typical life cycle of banking phishing websites.

Artificial Neural Network (ANN) can be characterized as an information handling method that is inspired by the way natural sensory systems process data. One of the most important component of this soft computing algorithm is

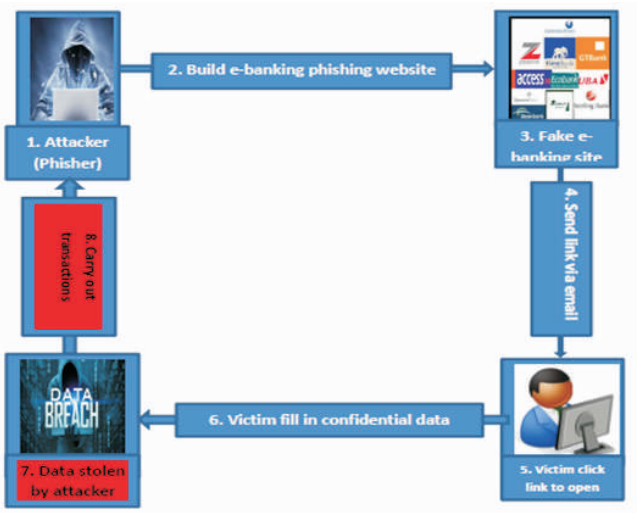

Figure 1. E-banking Phishing Life Cycle

the unmistakable structure of the data preparing scheme. ANN comprises of a huge number of exceedingly interconnected preparing components called "neurons", working in concordance to take care of complex problem. ANNs, similar to human, learn by illustration (Mohammad, McCluskey & Thabtah, 2013). The utilization of ANN is successful to settle countless basic processing neuron, huge number of weighted connections among the components, circulated representation of information over the connections knowledge is gained by organization through a learning process.

To summarize the key contributions of our paper, we chronicle them as follows:

- We present an architectural framework for the proposed model.
- We develop an e-banking phishing website detection algorithm using ANN with confusion matrix analysis.
- We then demonstrated the practical experimentation of the proposed model using MatLab.

The aim of this research work is to develop an intelligent detection algorithm for e-banking phishing websites using Artificial Neural Network (ANN) with confusion matrix in order to achieve more consistent accuracy in classification. The remaining sections of the manuscript are organized as follows: Section II details some related works, while Section III presented the architecture of the proposed framework. Section IV explains the method of dataset collection and presentation. Section V chronicles the ANN algorithm with confusion matrix, Section VI enumerates the performance metrics used, Section VII presents the experimental setup and Section VIII discusses the results. The conclusion was presented in Section IX.

1. Related Works

In this section, we present some related literatures that attempt to address the problem of phishing in e-banking websites. All the more light has been shed on experimental contextual analyses for examining e-banking phishing systems and attack approaches on telephone phishing and phishing website attack where viable preventions and investigating the effectiveness of performing security mindfulness of phishing dangers. The test in the paper audit demonstrates the noteworthiness of directing phishing preparing mindfulness for innovation clients and enhancing the endeavors in creating phishing counteractive action procedures. In the analysis completed in this paper, it demonstrates that conventional phishing countermeasures are not generally successful for identifying phishing websites, and option shrewd phishing discovery approach are expected to battle phishing attacks (Aburrous, Hossain, Dahal, & Thabtah, 2010).

In detecting phishing websites hyper-heuristic and machine learning procedures were considered to investigate short life time of phishing websites, decrease of computational volume and probability examining and controlling a scope of sites are at the same time. In accomplishing this consistently, the decrease of elements in assessed includes through discovery of phishing websites are characterized by hyper heuristic gravitational pursuit calculations. At that point, order of the sites into two phishing website and legitimate sites is performed through the help of vector machine calculation, which is a procedure in machine learning. The examination of results utilizing best discovery calculation as demonstrate that want goals of precision rate is accomplished at 87%, mistake rate at 7.8 and run time at 8190ms (Khonji, Iraqi, & Jones, 2013). A powerful web based banking extortion recognition system which incorporates pertinent assets and coordinate a few

propelled information mining procedures was introduced. Another algorithm called Contrast Miner was also applied with productively mine difference designs and recognize fake from genuine conduct, trailed by a compelling example determination and hazard scoring that consolidates forecasts from various models. Results in the paper demonstrate that a higher exactness and lower ready volume can be accomplished (Wei, Li, Cao, Ou, & Chen, 2013).

Particle Swarm Optimization (PSO) technique utilizing association and characterization data mining algorithms optimizing is an approach utilized as a part of the distinguishing phishing websites. These algorithms were utilized to describe and distinguish every one of the elements and standards keeping in mind the end goal to characterize the phishing website and the relationship that correspond them with each other. It likewise utilized Missing Completely at Random (MCAR) classification algorithm to remove the phishing preparing informational indexes criteria to group their authenticity. The work has impediments like sequences of arbitrary choices (not free) and time to meeting indeterminate in the phishing characterization. So, to beat this impediment we improve PSO which finds an answer for an advancement issue in a pursuit space, or show and foresee social conduct within the sight of phishing websites. This will enhance the effectively arranged phishing websites (Damodaram & Valarmathi, 2011).

A Naive Bayes Classifier is utilized as a part of identifying phishing websites. The proposed framework removes the source code highlights, URL highlights and picture highlights from the phishing website. The highlights that are separated are given to the ant colony optimization algorithm to gain the lessened highlights. The decreased highlights are again given to the Naïve Bayes classifier so as to order the site page as real or phished (Priya, 2016). In a related work, the proposed model has been outlined with the multidirectional include investigation alongside the Back Propagation Probabilistic neural network (BP-PNN) order. The anticipated soft computing algorithm has accomplished better performance in terms of the exactness in the greater part of the spaces in view of the assault recognition and arrangement (Goyal & Bansal, 2017).

In spite of the fact that an extensive variety of countermeasures to phishing attacks in e-banking websites have been proposed, most of them are not fit to settle on a choice impeccably in this manner the false positive choices raised intensely, therefore reducing the accuracy.

2. Architecture of Proposed Framework

The research work is based on the proposed detection framework of e-banking phishing websites using ANN with confusion matrix. The proposed architecture of the conceptual framework is diagrammatically shown in Figure 2.

3. Dataset Collection and Presentation

The ANN experimentation is achieve by obtaining dataset that consist of different website which will be used to extract the features. The dataset comprises of both legit and phishy sites which are collected from (Yahoo Directory 2017; Starting point directory, 2018; Phishtank, 2018; Millersmiles archives, 2018). The dataset collected holds definite input i.e. "Legit", and "Phishy". Theinputs were converted to mathematical standards so that the neural network can execute its calculations thus we replaced the input 1, and 0 instead of "Legit", and "Phishy" respectively. From the dataset collected, legitimate websites hold 256 and phishy websites hold 134.

In artificial neural network this study is concerned in attaining a model with a good generalization performance. However, the error rate on the training

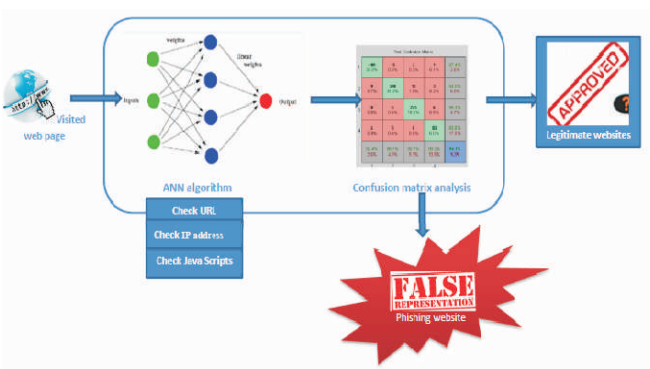

Figure 2. Architecture of Proposed ANN Detection Framework

dataset drops in the course of the training phase, the error rate on the unseen dataset (testing dataset) rises at certain point. To defeat this issue, we utilized the "HOLD OUT" approval method, by isolating our dataset into preparing, approval and testing datasets. In this undertaking each dataset is precisely picked arbitrarily. We separated the dataset to 15% for approval, 15% for testing and 7o% for preparing. Preparing dataset is utilized to prepare the system and to modify the weights of the system, while the testing dataset stays concealed and it is utilized to survey the prescient execution of the model. In the wake of preparing, we ran the system on the testing dataset. The mistake an incentive on the testing dataset offers a fair- minded estimate of the generalization error.

4. ANN Algorithm with Confusion Matrix

The algorithm begins by stacking the training dataset, at that point we make the underlying ANN structure by methods for number of layers, amount of neurons in each layer and the learning parameters i.e. learning rate, force esteem and amount of ages. Once the ANN structure is resolved, the weights are introduced to little non-zero esteems. The model is then prepared until the point that the most extreme number of ages or the expected mistake rate is accomplished. The model is then tried on the testing dataset which is never being seen once. On the off chance that the prescient execution is worthy then the ANN is created and the weights are delivered. Something else, the ANN structure is enhanced by changing the quantity of neurons in the concealed layer or by refreshing the system parameters i.e. learning rate and energy esteem. In our model we received the pruning way to deal with indicate the quantity of neurons in the concealed layer, since we began with countless, and the logically at least one neurons expelled amid preparing until the point when the coveted execution is met. Figure 3 shows the phishing detection model algorithm used in artificial neural network with confusion matrix analysis. Figure 4 presents the ANN models phases, starting with data collection, preprocessing of data, building the ANN network, training the network and then testing it.

Confusion matrix is a table that is regularly used to show

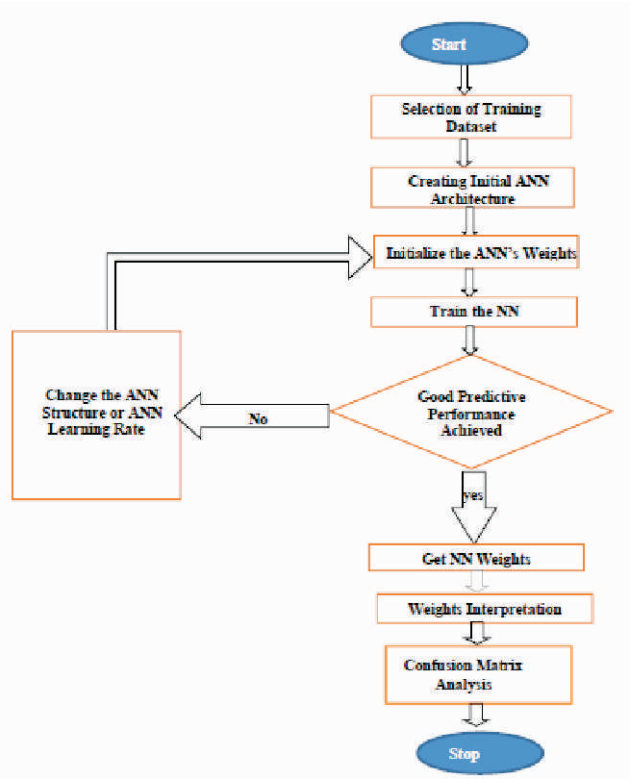

Figure 3. ANN Detection Algorithm with Confusion Matrix Analysis

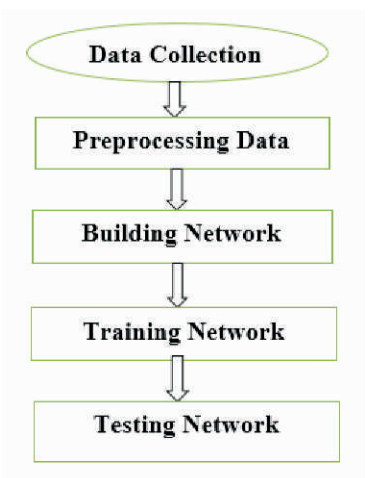

Figure 4. An ANN Models Phases

the execution of an order display on an organization of test data for which the authentic values are known. On the confusion matrix, the lines relate to the anticipated class (output class), and the segments demonstrate the genuine class (target class). The corner to corner cells appear for what number of and what level of the dataset the prepared system accurately evaluates the classes of perceptions. That is, it indicates what level of the genuine

and anticipated classes coordinate. The off corner to corner cells demonstrate where the classifier has committed errors. The section on the most distant right of the plot demonstrates the precision for each anticipated class, while the line at the base of the plot demonstrates the exactness for each evident class. The cell in the base right of the plot demonstrates the general precision or accuracy.

5. Performance Metrics

To assess the accuracy of the forecast of e-banking phishing websites, certain performance assessment measurements will be utilized as a part of the reason for this examination. The accompanying parameters are considered in (Abdulhamid et al., 2017; Madni, Latiff, Abdullahi, Abdulhamid, Usman, 2017; Latiff, Madni, Abdullahi, 2018).

- True positive rate (TPR): - This is the number of websites that are accurately classified.
- False positive rate (FPT): - This is the number of websites that are wrongly rejected from the class.

From the parametric definition above, the following metrics were deduced: accuracy and precision. The deduced metrics is defined as follows:

- Percentage Accuracy (PA) decides the percentage of websites that are classified accordingly.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \; x\,100 \qquad (1)$$

- Precision is the comprehensive version of accuracy. It is defined as a simple metric that calculates the fraction of cases for which the accurate result is returned.

$$Precision = \frac{Tp}{TP + FP} \qquad (2)$$

6. Experimental Setup

MATLAB ANN toolbox was utilized for this experiment. The NN Toolbox is utilized for configuration, execution, graphics and to recreate our ANN. MATLAB gives far reaching support for a few ANN standards, and GUIs upheld by MATLAB enables the client to plan NN in an exceptionally straightforward manner. We created Multi-Layer Perceptron (MLP) show and figured the subsequent NN demonstrate execution by methods for Mean Square Error (MSE). Figure 4 which shows the phases necessary to build an ANN model. The MLP program begins by perusing the preparation, validation and testing datasets. Each dataset is stored in an Excel record. To read the datasets we utilized "xlsread" worked in function. Next, the information factors site highlights (Using_IP address, Long URL, URL having @ symbol and so forth.) and output variable (site class) are expressed for both preparing and validation dataset.

The stages in predicting phishing websites using Artificial Neural Network with supervised learning which are: training, testing and validation. The stages were achieved by designing a neural network architecture that will give us "5" hidden neurons, "8" input, and "1" output, as shown in Figure 5.

We demonstrate how the neural system is prepared utilizing scale conjugate gradient (transcg), and utilizing the mean square error to gauge the training performance. From the training, these are a piece of the algorithm thought about in reason for training the network. Additionally, in training the neural network, we consider the advance of the network itself, whereby the neural system repeats at 12 epochs which demonstrates the iteration at which the approval execution achieved a base, as at the time of 1 second. From the result it shows that neural network validation checks as at 6 also with the gradient of 0.0051633 at 12 epochs.

7. Results and Discussion

Figure 6 demonstrates that the training is indicated with a

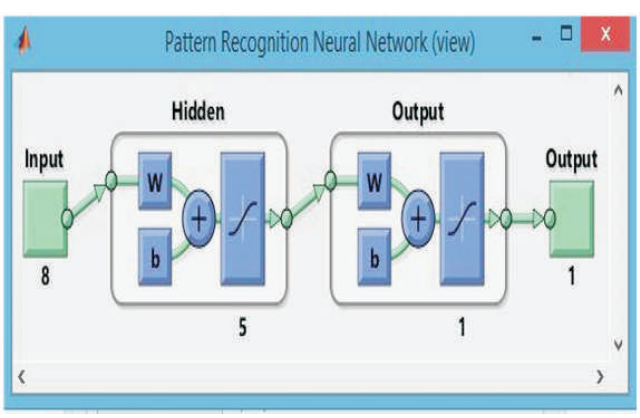

Figure 5. ANN MATLab Architecture

thick blue line, testing with a thick red line, approval with a thick green line, and the best execution is meant with a dash line. This figure does not demonstrate any significant issues with the training. The approval and test fittings are fundamentally the same as. On the off chance that the test fitting had expanded fundamentally before the approval fitting expanded, at that point it is conceivable that some finished fitting may have happened. In this figure the best approval execution landed at 0.030232 at epoch 5.

The Figure 7 shows variety in slope coefficient as for number of epochs. The last estimation of angle coefficient at epoch number 12 is 0.0051633. This also shows that the validation checks were arrived at 6 at epoch number 12.

In Figure 8, it demonstrates to visualize errors between

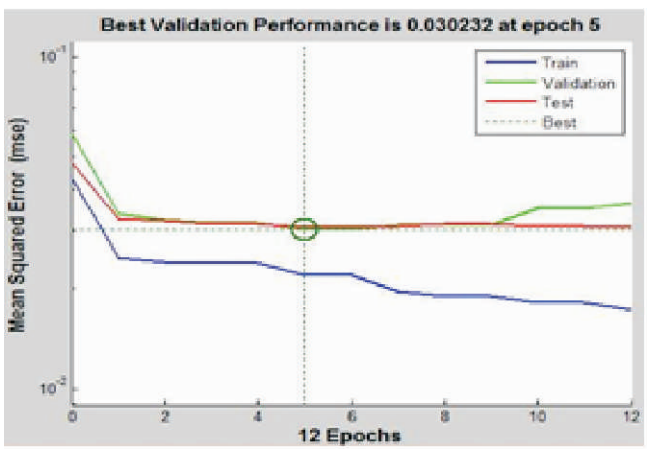

Figure 6. Training Performance

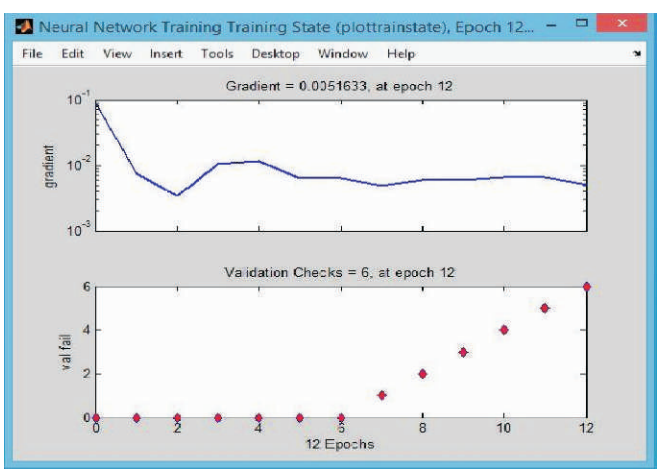

Figure 7. Training State (Plot Train State)

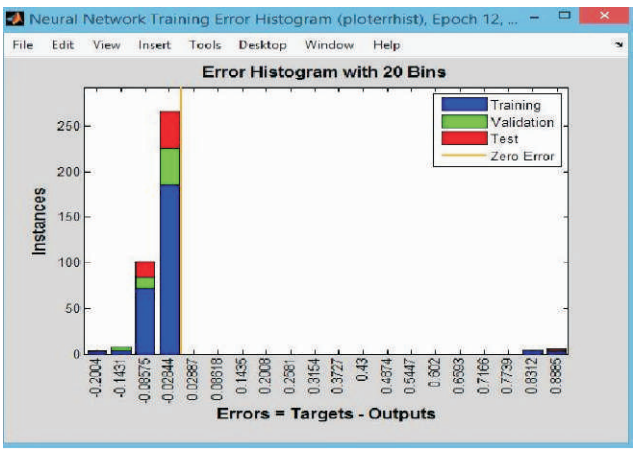

Figure 8. Error Histogram

target values and anticipated values in the wake of training a network utilizing a feedforward neural system. The blue bars direct to training data, the green bars direct to the validation data, and the red bars direct to testing data. The histogram can give you an indication of special cases, which are data centers where the fit is generally more repulsive that the bigger piece of data.

From Figure 9 below it shows that a linear regression amongst the network outputs and the resultant targets is carried out. The output tracks the target very well for training, testing, validation, which hold the value of 0.3771, 0.6349, and 0.52917 respectively and the R-value for training, testing, and validation which is over 0.46773 for the total response.

From the Figure 10, the first two diagonal cells show the

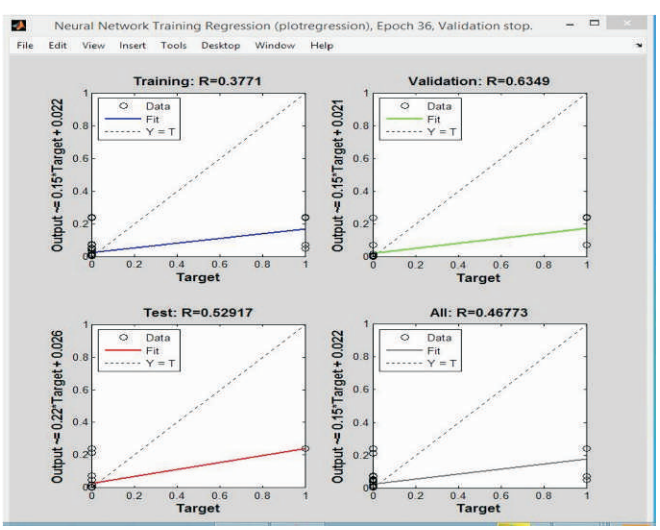

Figure 9. Training Regression

Figure 10. Confusion Matrix for Training, Testing, Validation and all Confusion Matrix

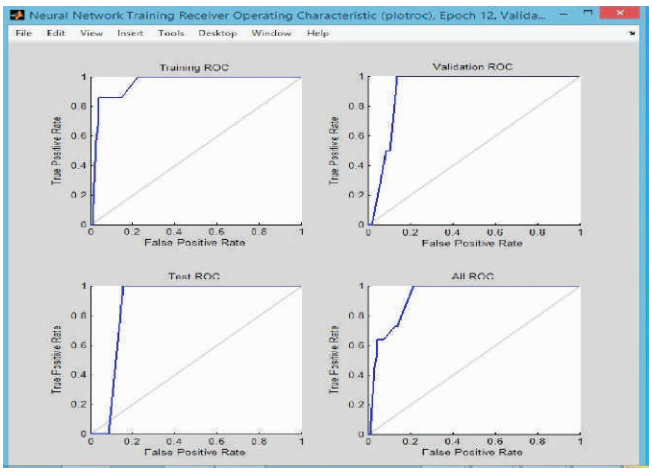

Figure 11. TPR by FPR for Training, Testing and Validation ROC

number and percentage of correct classifications by the trained network under the training confusion matrix. For 265 websites that classify correctly to be legitimate. This correspond to 97.4% of all 379 websites. Similarly, o websites are correctly classifying as phishy.

This corresponds to 0.0% of all legitimate websites. Seven of the websites are incorrectly classified as legitimate and this corresponds to 2.6% of all 379 websites in the data. Similarly, 0 of the websites are incorrectly classified as phishy and this correspond to 0.0% of all websites in the training section. Out of 272 of the websites predictions, 97.4% are correct and 2.6% are wrong. Out of 0 predictions, 0% are correct and 0% are wrong. Out of 265 legitimate websites dataset, 100% are correctly predicted as legitimate and 0.0 are phishy. Overall, 97.4% of the predictions are correct and 2.6% are wrong classifications. This are carried out at training, testing, validation, and over all confusion matrix.

In Figure 11, the hued lines in each pivot signify to the ROC curves. It is a graph of the TPF against FPR as the edge is fluctuated. An immaculate test would indicate point in the upper-left angle, with 100% sensitivity and 100% specificity. This shows that the system performs extremely well.

Conclusion

Artificial neural network (ANN) is thought to be an alternative algorithm that can be utilized to anticipate or predict e-banking phishing websites among different algorithms. ANN with a regulated learning calculation consolidated with an encouraged confusion matrix, whereby various hidden layers and number concealed neurons was taken to give a decent prescient execution. Over all, the principle objective of this undertaking is to build up an ANN algorithm shows that will detect and classify sites either as "phishy" and "legitimate" and furthermore to demonstrate that ANN with confusion matrix is a decent strategy for detecting e-banking phishing websites with the best accuracy.

References

[1]. Abdulhamid, S. M., Latiff, M. S. A., Chiroma, H., Osho, O., Abdul-Salaam, G., Abubakar, A. I., & Herawan, T. (2017). A Review on mobile SMS spam filtering techniques. *IEEE Access,* 5(1), 15650-66.

[2]. Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Experimental case studies for investigating e-banking phishing techniques and attack strategies. *Cognitive Computation,* 2(3), 242-253.

[3]. Babagoli, M., Aghababa, M. P., & Solouk, V. (2018). Heuristic nonlinear regression strategy for detecting phishing websites. *Soft Computing,* 19(1), 1-13.

[4]. Damodaram, R., & Valarmathi, M. L. (2011). Phishing website detection and optimization using particle swarm optimization technique. *International Journal of Computer Science and Security (IJCSS),* 5(5), 477-490.

[5]. Goyal, B., & Bansal, M. (2017). Competent approach for type of phishing attack detection using multi-layer

neural network. *International Journal of Advanced Engineering Research and Science,* 4(1), 210-215. https://dx.doi.org/10.22161/ijaers.4.1.34.

[6]. Idris, I., & Abdulhamid, S. M. (2014). An improved AIS based e-mail classification technique for spam detection. arXiv preprint arXiv:1402.1242.

[7]. Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys & Tutorials,* 15(4), 2091-2121.

[8]. Latiff, M. S. A., Madni, S. H. H., & Abdullahi, M. (2018). Fault tolerance aware scheduling technique for cloud computing environment using dynamic clustering algorithm. *Neural Computing and Applications,* 29(1), 279-293.

[9]. Madni, S. H. H., Latiff, M. S. A., Abdullahi, M., Abdulhamid, S. M., & Usman, M. J. (2017). Performance comparison of heuristic algorithms for task scheduling in IaaS cloud computing environment. *PloS One,* 12(5), e0176321.

[10]. Madni, S. H. H., Latiff, M. S. A., Coulibaly, Y., & Abdulhamid, S. (2017). Recent advancements in resource allocation techniques for cloud computing environment: A systematic review. *Cluster Computing,* 20(3), 2489-2533.

[11]. Millersmiles Archives (2018). Retrieved from http://www.millersmiles.co.uk/

[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]. Mohammad, R., McCluskey, T. L., & Thabtah, F. A. (2013, July). Predicting phishing websites using neural network trained with back-propagation. In *Proceedings on the International Conference on Artificial Intelligence (ICAI), The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).*

[14]. Phishtank (2018). Retrieved from http://www.phishtank.com/,

[15]. Priya, R. (2016). An ideal approach for detection of phishing attacks using naïve bayes classifier. *International Journal of Computer Trends and Technology (IJCTT),* 40(2), 84-87.

[16]. Starting Point Directory (2018). Starting Point Web Directory. Retrieved from http://www.stpt.com/directory/

[17]. Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J. (2013). Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web,* 16(4), 449-475.

[18]. Yahoo Directory (2017). (http://dir.yahoo.com/), Access date: 15/10/2017.

ABOUT THE AUTHORS

Shafi'i Muhammad Abdulhamid is a Senior Lecturer and Head of Department (HOD) of Cyber Security Science, Federal University of Technology Minna, Nigeria. He is also supervising both Masters and Ph.D students (in both Nigeria and Malaysia). He received his Ph.D in Computer Science from University of Technology Malaysia (UTM), M.Sc in Computer Science from Bayero University Kano (BUK), Nigeria and a Bachelor of Technology in Mathematics with Computer Science from the Federal University of Technology (FUT) Minna, Nigeria. He has been appointed as an Editorial board member for Big Data and Cloud Innovation (BDCI) and Journal of Computer Science and Information Technology (JCSIT). He has also been appointed as a Reviewer of several ISI and Scopus indexed International Journals. He has also served as Program Committee (PC) member in many National and International Conferences. He is one of the pioneer instructors at the Huawei Academy of FUT Minna and a holder of Huawei Certified Network Associate (HCNA). He is as well a member of IEEE Computer Society, International Association of Computer Science and Information Technology (IACSIT), Computer Professionals Registration Council of Nigeria (CPN), International Association of Engineers (IAENG), The Internet Society (ISOC), Cyber Security Experts Association of Nigeria (CSEAN) and Nigerian Computer Society (NCS). His current research interests are in Cyber Security, Cloud Computing, Soft Computing, Internet of Things Security, Malware Detection and Big Data. He has published many academic papers in reputable International journals, conference proceedings and book chapters.

Mubaraq Olamide Usman is a Graduate of Computer Science (Cyber Security Science option) from the Federal University of Technology (FUT) Minna, Nigeria. His current research interests are in Cyber Security, Cloud Computing, Soft Computing and Big Data.

Oluwaseun A. Ojerinde is a Lecturer in the Department of Computer Science in the School of Information and Computer Technology in Federal University of Technology, Minna. He bagged his B.Sc in Computer Technology at Babcock University in 2006. He received his M.Sc in Mobile Communication System from Loughborough University in 2008. He also obtained his Ph.D in Mobile Communication System from Loughborough University in 2014. His research area is in Antenna, On-body Systems, Multiple Input Multiple Output (MIMO) Systems, Spanning, Telecommunications, Networking and Radiation. He has worked on the effects of Metallic Objects on Radiation for Mobile Devices. He is a member of IEEE and IET.

Victor Ndako Adama is a Lecturer at the Computer Science Department of the Federal University of Technology Minna, Niger State. He holds B.Tech Degree in Mathematics with Computer Science and M.Tech Degree in Computer Science from Federal University of Technology Minna. His Research area interests are in the following HCI and Security Systems. His areas of interest are Software Engineering and Artificial Intelligence.

John K. Alhassan is a Lecturer and current head of the Department of Cyber Security Science, Federal University of Technology Minna, Niger State, Nigeria. He holds Ph.D in Computer Science. His area of research includes Artificial Intelligence, Data Mining, Internet Technology, Database Management System, Software Architecture, Machine Learning, Human Computer Interaction, Computer Security and Big Data Analytics