ISSN-2347-2227
Subscribers copy
Not for sale

i-manager's

Journal on Computer Science

Disseminating new ideas in Information and Computation

i-manager® Publications

ISSN-2347-2227
Volume 6. No. 3
September - November 2018

i-manager's
Journal on Computer Science

About the Journal

i-manager's Journal on Computer Science deals with all aspects of computer science and contributes theoretical results and offers a compilation of high quality articles to encompass a wide spectrum of advancements in the actively developed domain. i-manager's Journal on Computer Science covers a great deal of what has been done in the field recently and intends to bring together the most recent advances and applications in all branches of the academic computer science community with new knowledge and technology for the benefit of students, professionals and industrial practitioners.

i-manager's Journal on Computer Science is presently in its 6th Year. The first issue was launched in 2013.

i-manager's Journal on Computer Science is published by i-manager Publications, one of India's leading Academic Journal Publisher, publishing 28 Academic Journals in diverse fields of Engineering, Education, Management and Science.

Why Publish with us

i-manager Publications currently publishes academic Journals in Education, Engineering, Scientific and Management streams. All of i-manager's Journals are supported by highly qualified Editorial Board members who help in presenting high quality content issue after issue. We follow stringent Double Blind Peer Review process to maintain the high quality of our Journals. Our Journals target both Indian as well as International researchers and serve as a medium for knowledge transfer between the developed and developing countries. The Journals have a good mix of International and Indian academic contributions, with the peer-review committee set up with International Educators.

Submission Procedure

Researchers and practitioners are invited to submit an abstract of maximum 200 words on or before the stipulated deadline, along with a one page proposal, including Title of the paper, author name, job title, organization/institution and biographical note.

Authors of accepted proposals will be notified about the status of their proposals before the stipulated deadline. All submitted articles in full text are expected to be submitted before the stipulated deadline, along with an acknowledgement stating that it is an original contribution.

Review Procedure

All submissions will undergo an abstract review and a double blind review on the full papers. The abstracts would be reviewed initially and the acceptance and rejection of the abstracts would be notified to the corresponding authors. Once the authors submit the full papers in accordance to the suggestions in the abstract review report, the papers would be forwarded for final review. The final selection of the papers would be based on the report of the review panel members.

Format for Citing Papers

Author surname, initials (s.) (2018). Title of paper, i-manager's Journal on Computer Science, 6(3), xx-xx.

Copyright

Contact e-mails

editor_jcom@imanagerpublications.com
submissions@imanagerpublications.com

ISSN-2347-2227
Volume 6. No. 3
September - November 2018

i-manager's
Journal on Computer Science

ISSN-2347-2227
Volume 6. No. 3
September - November 2018

i-manager's
Journal on Computer Science

OUR OFFICES

Registered Office

3/343,Hill view,
Town Railway Nager,
Nagercoil, Kanyakumari District - 629001
Ph : 91-4652- 277675
E-mail : info@imanagerpublications.com

Editorial Office

13-B, Popular Building,
Mead Street, College Road,
Nagercoil, Kanyakumari District - 629001
Ph : (91-4652) 231675, 232675, 276675
E-mail : editor_jcom@imanagerpublications.com

Abstracting / Indexing

ProQuest · ULRICHSWEB GLOBAL SERIALS DIRECTORY · Google Scholar · OCLC WorldCat

Join with us

https://www.facebook.com/Journal-on-Computer-Science-2168468313379110/

https://www.facebook.com/imanagerPublishing/

https://twitter.com/imanagerpub

CONTENTS

RESEARCH PAPERS

EDITORIAL

The current issue of i-manager's Journal on Computer Science mainly focuses on Authentication System, Artificial Neural Network used to detect e-banking Phishing Websites, Password Management, Adaptive Personnel Selection Expert System to Support Organization's Personnel Recruitment Decision Process, Evaluation of Classification Algorithms for Phishing URL Detection and detection of Captcha Smuggling Attacks using Supervised Deep Learning Based Approach.

Omorogiuwa and his co-author Aziken have proposed a study about Computer-Based Local Area Authentication System. The system was developed using XAMPP integrated net-base application and JAVA object-oriented programming language. This security system is controlled through the network via the server and controls all clients that choose to use the resources like e-exam platform, e-library, etc. The performance of the system has been monitored and the result is found to be satisfactory, as all unauthorized users are blocked and appropriate warning messages are sent to the client's system by the server when the user attempts to login which eliminates external users from gaining access to the examination platform.

Shafi'i Muhammad Abdulhamid et al., have proposed a study about a soft computing approach to detect e-banking phishing websites using Artificial Neural Network (ANN). Confusion matrix analysis was used in this study to detect e-banking phishing websites. Datasets from various websites comprises of both legitimate and phishing websites collected from directory and analysed by ANN Algorithm with Confusion Matrix. The study results showed that the proposed ANN algorithm produces a remarkable percentage of accuracy and reduced false positive rate during detection and can produce competitive results that is suitable for detecting phishing in e-banking websites.

Victor N. Adama et al., have presented a study to analyse about password knowledge and password management. This research was conducted via a case study aimed at establishing the theoretical password knowledge in comparison to actual password management practice of staff and students from Information Technology (IT) inclined departments of the Federal University of Technology, Minna. The data collection was carried out primarily based on a survey. The study results concluded that, there is a significant difference between what respondents know compared to their actual practice. The authors recommend that, more extensive research into enhancing graphical password entropies are to be conducted in future as they possess the potential to replace text passwords.

Muhammad Ahmad Shehu et al., have proposed a study to analyze the personnel recruitment operation which is an essential human resource operation of an organization. An adaptive personnel selection model was developed to minimize the complexity and to carry out the personnel selection by considering some of the operational behaviors. The adaptive personnel selection model was developed using a C4.5 decision tree and frequent and non-frequent pattern analysis of data mining. The study results showed that, the proposed expert system enables the personnel selection strategy changes to be fed in by the organization, when it occurs.

Oluyomi Ayanfeoluwa et al., have conducted a study to evaluate the capacity of different algorithms to detect phishing URLs. Dataset was obtained from UCI Machine Learning Repository, and the algorithms were assessed in terms of Accuracy, Precision, Recall, F-Measure, Receiver Operating Characteristic (ROC) area and Root Mean Squared Error (RMSE). In terms of accuracy, precision, recall, F-measure, and RMSE, the Random Forest algorithm was found to perform better than the other algorithms analyzed and a number of others from existing literature. The authors recommend that, further studies are to be conducted, to ascertain if performances are dataset-specific.

Moses O. Omoyele et al., have proposed a study to analyze a predictive model for the detection of captcha smuggling attacks. In order to achieve the aim, framework based on hyper parameter specification was developed in this study. The model was evaluated on the available CAPTCHA smuggling dataset. The outcome of this research will benefit web developers, web users, web hosting companies and internet service providers. The study results showed that, the accuracy of prediction achieved in this work is 77.89% at consistency of 0.1543. The sensitivity and specificity of the model are 78.11% and 78.2%, respectively.

All papers of this issue, papers 1 to 6 were submitted from the 2nd International Conference on Information and

EDITORIAL

Communication Technology and Its Applications (ICTA 2018), conducted on 5 -6th September 2018 at Federal University of Technology, Minna, Nigeria. We express our gratitude to the Conveners Dr. Shafii Abdulhamid & Dr. Oluwafemi Osho for their support in ensuring the papers were submitted on time.

We extend our sincere thanks to the authors for their contributions towards this issue and we are grateful to the reviewers for spending their quality time in reviewing these papers. Our special thanks to the Editor-in-Chief, Dr. Kamal kumar Mehta for his continuous support and efforts in improving further the quality of the Journal.

Enjoy reading!

Warm regards,

Ramani R
Junior Associate Editor
i-manager Publications

A SOFT COMPUTING APPROACH TO DETECT 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: 11/01/2019 Date Revised: 28/01/2019 Date Accepted: 22/03/2019

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 indicate 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 classification. Therefore, when a new phishing web page is introduced, the detection algorithms find it difficult to correctly classify it as phishing. This paper puts 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 of accuracy and reduced false positive rate during detection. This shows that, the ANN algorithm with confusion matrix analysis can produce 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 the website 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 legitimate websites. These sites have high graphical resemblances to the true legitimate ones trying to swindle the genuine web clients. Social engineering and specialized deceits regularly consolidat together such information 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 websites, but also in addition the smart approaches used to design such websites, even clients having great involvement in cybersecurity and web may be misled. Normally, phishers initiate the attack by sending email that imitates a credible or legitimate organization to the targets users by encouraging them to refresh or authorize their data by clicking a hyperlink contained in the 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 as in case of spear-phishing, when the attacker purposefully tries to hurt specific victims. Figure 1 shows a typical life cycle of e-banking phishing websites.

Artificial Neural Network (ANN) can be characterized as information handling method that is inspired by the way natural sensory systems process data. One of the most important components of this soft computing algorithm is the unmistakable structure of the data preparing scheme. ANN comprises of a huge number of exceedingly

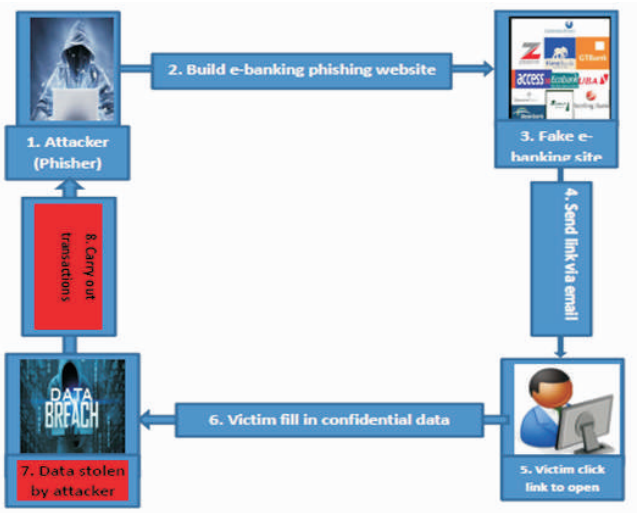

Figure 1. E-banking Phishing Life Cycle

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 neurons, huge number of weighted connections among the components, circulated representation of information over the connections and knowledge is gained through an organized learning process.

To summarize the key contributions of this paper, the authors chronicle them as follows:

- an architectural framework for the proposed model is presented.
- an e-banking phishing website detection algorithm using ANN with confusion matrix analysis is developed.
- the practical experimentation of the proposed model using MatLab is demonstrated.

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.

1. Related Works

In this section, some related literatures that attempt to address the problem of phishing in e-banking websites are presented. All the more, light has been shed on experimental contextual analyses for examining e-banking phishing systems and attack approaches based 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. The analysis in this paper, 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 the short life time of phishing websites, decreasing computational volume, examining probability and controlling the scope of sites are done at the same time. In accomplishing this, the decrease of elements are consistently assessed through discovery of phishing websites characterized by hyper heuristic gravitational pursuit calculations. At that point, order of the sites two website phishing and legitimate sites are performed with the help of vector machine calculation, which is a procedure in machine learning. The examination of results utilizing best discovery calculation demonstrates that goals of precision rate is accomplished at 87%, mistake rate at 7.8 and run time at 8190 ms (Khonji, Iraqi, & Jones, 2013). A powerful web based banking extortion recognition system was incorporated pertinent to assets and coordinated a few propelled information mining procedures. Another algorithm called Contrast-Miner was applied with productively mine difference designs that recognize fake from genuine conduct, trailed by a compelling example determination and hazard scoring which 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 is utilized in association with characterization to optimize data mining algorithms is an approach used to distinguish phishing websites. These algorithms were utilized to describe and distinguish the elements and standards keeping in mind the end goal to characterize the phishing website and to establish the relationship that correspond between them. Likewise Missing Completely at Random (MCAR) classification algorithm is utilized 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 phishing characterization. So, to resolve this impediment the use of improved PSO finds an answer for advancement issue in pursuit space, or show and foresee social conduct within the sight of phishing websites. This will enhance the effectiveness in 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 removed highlights are given to the Ant Colony Optimization (ACO) algorithm to gain the lessened highlights. The decreased highlights are again given to the Naïve Bayes classifier so as to classify the website page as real or phished (Priya, 2016). In another 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, thereby 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 achieved by obtaining dataset that consisted of different websites which were used to extract the features. The dataset comprises of both legitimate and phishing websites which are collected from (Yahoo Directory, 2017; Starting point directory, 2018; Phishtank, 2018; Millersmiles archives, 2018). The dataset collected holds definite input i.e. "Legitimate", and "Phishing". The inputs were converted to mathematical standards so that the neural network can execute its calculations and therefore replaced the 1, and 0 instead of "Legitimate", and "Phishing" respectively. From the collected dataset, 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 training the 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, the "HOLD OUT" approval method was utilized, by isolating the dataset into preparing, approval and testing datasets. In this method, each dataset is precisely picked arbitrarily. The dataset were grouped as 15% for approval, 15% for numeral testing and 70% for preparing. The prepared dataset are utilized by the system and to modify the weights, while the testing dataset stays concealed and it is utilized to survey

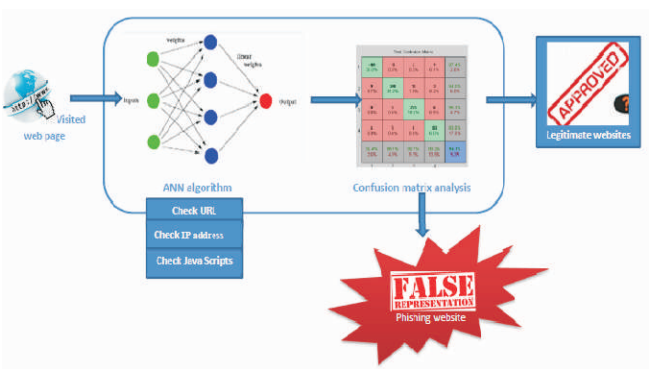

Figure 2. Architecture of Proposed ANN Detection Framework

the prescient execution of the model. In the wake of preparing, the system ran on the testing dataset. The error 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 the underlying ANN structure is made into 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 small non-zero esteems. The model is then prepared until the point that the most extreme number of ages or the expected error 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. Then, 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. This model received the pruning way to deal with the indicate quantity of neurons in the concealed layer, countless, or the logically at least one neuron was expelled, amid preparing, until the point when the coveted execution is met. Figure 3 shows the phishing detection model algorithm used in ANN 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 execute, an order display in 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 with the number level of the dataset the prepared, for which the system accurately evaluates the classes of perceptions. They indicate the level of the genuine and anticipated classes coordinate. The off corner to corner cells demonstrate where the classifier has committed errors. The position on the distant right most cell of the plot demonstrates the precision for each

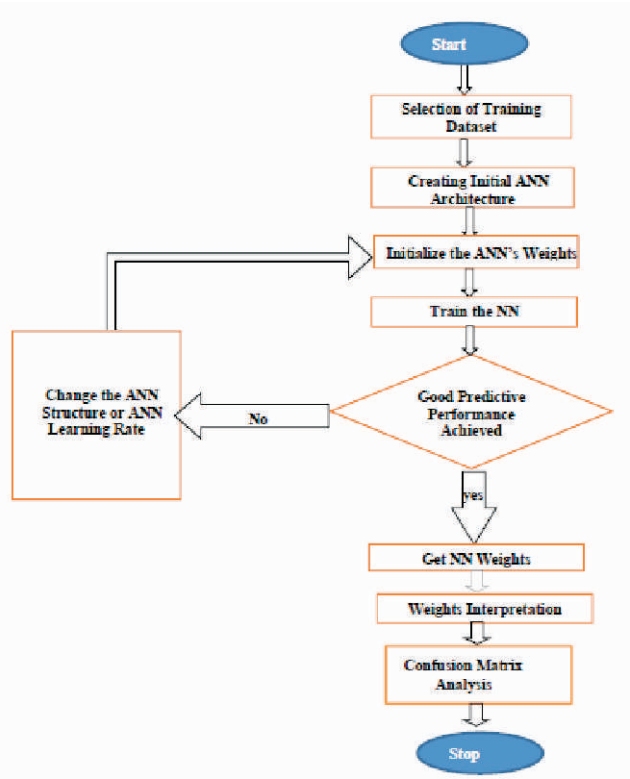

Figure 3. ANN Detection Algorithm with Confusion Matrix Analysis

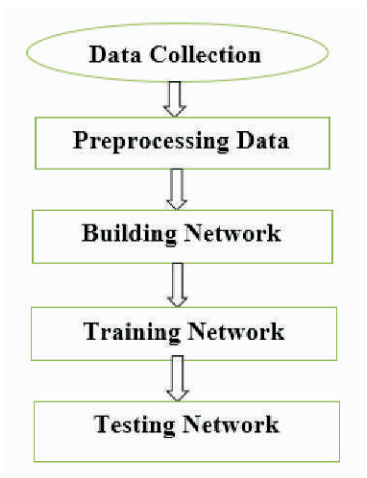

Figure 4. An ANN Model's Phases

anticipated class, while the line at the bottom of the plot demonstrates the exactness for each evident class. The cell in the bottom 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 would be utilized as a part of 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 as defined in equations (1) and (2).

- 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 the proposed 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. After creation of Multi- Layer Perceptron (MLP), it shows the subsequent NN demonstrate execution by methods for Mean Square Error (MSE). Figure 4 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 sheet. To read the datasets "xlsread" worked in function in MATLAB was utilized. Next, the information factors of website highlights (Using_IP address, Long URL, URL having @ symbol, etc.) and output variable (site class) are expressed for both preparing and validating the 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.

The following demonstrate how the neural system is prepared utilizing scale conjugate gradient (transcg), and utilizing the Mean Square Error (MSE) to gauge the training performance. From the training, a piece of the algorithm is used for training the network. Additionally, in training the neural network, the model considers 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, with in a time of 1 second. The result shows that neural network validation checks at epoch 6 and epoch 12 with the gradient of 0.0051633.

7. Results and Discussion

In Figure 6, training is indicated with a thick blue line, testing with a thick red line, approval with a thick green line, and the best execution is represented with a dashed line. This figure does not demonstrate any significant issues with the training. The approval and test fittings are fundamentally the same. On the off chance, the test fitting had expanded before the approval fitting expanded, at that point it is conceived that some finished fitting may have happened. In this figure, the best approval execution landed at 0.030232 at epoch 5.

Figure 7 shows variety in slope coefficient for different of epochs. The last estimation of angle coefficient at epoch

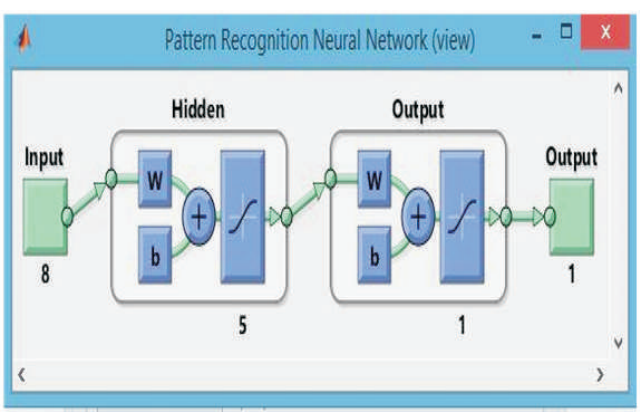

Figure 5. ANN Matlab Architecture

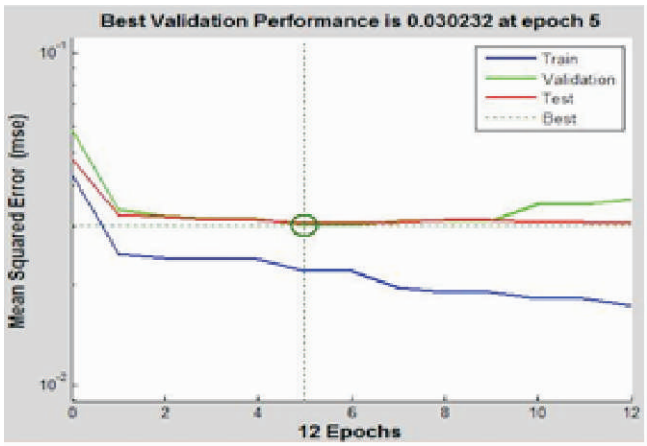

Figure 6. Training Performance

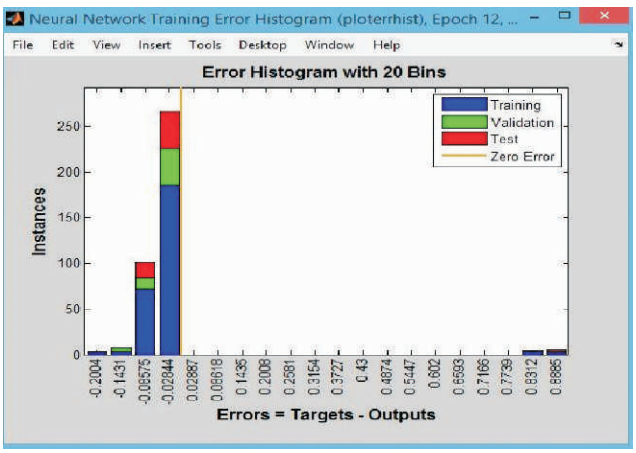

Figure 8. Error Histogram

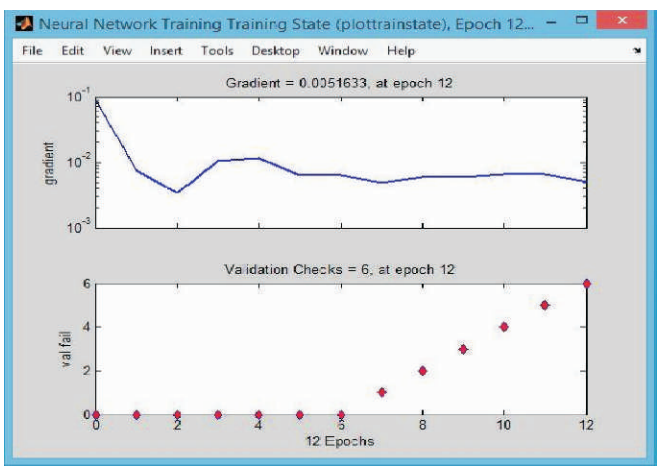

Figure 7. Training State (Plot Train State)

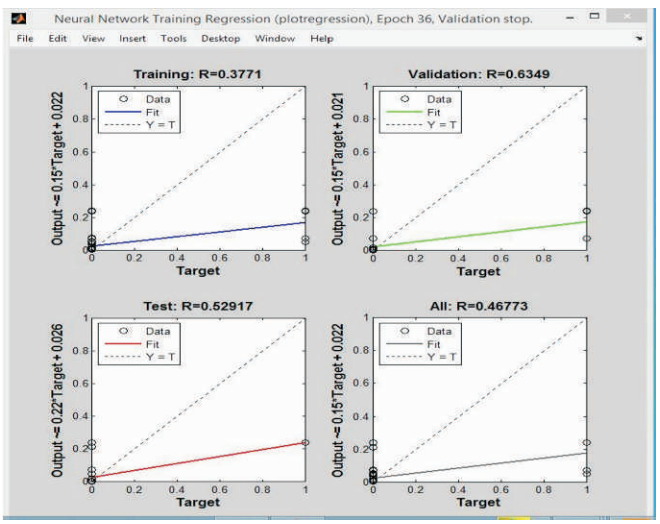

Figure 9. Training Regression

12 is 0.0051633. This also shows that the validation checks were arrived at epoch 6 and at epoch 12.

Figure 8 visualizes the errors between target values and anticipated values in the wake of training the 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 an indication of special cases, which are data centers where the fit is generally more repulsive than the bigger piece of data.

Figure 9 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 Figure 10, the first two diagonal cells show the number and percentage of correct classifications by the trained network under the training confusion matrix. 265 websites are classified correctly to be legitimate, and correspond to 97.4% of all 379 websites. Similarly, 0 websites are correctly classifying as phishing.

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 phishing and this correspond to 0.0% of all websites in the training section. Out of 272 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

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

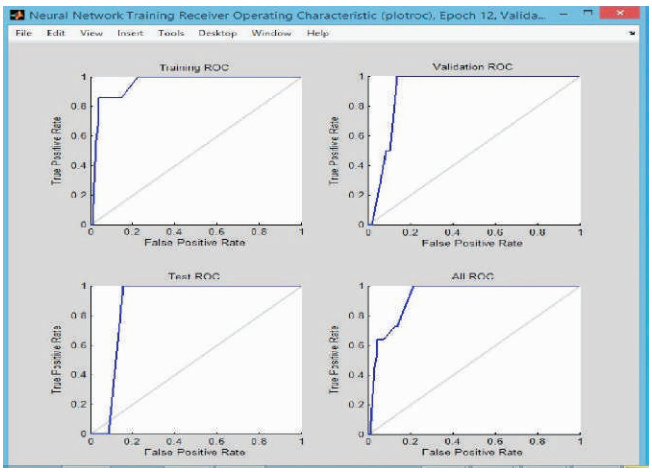

Figure 11. TPR by FPR for Training, Testing and Validation ROC

websites dataset, 100% are correctly predicted as legitimate and 0.0 are phishing. 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 an ANN algorithm to show that it will detect and classify sites either as "phishing" 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 of the 2013 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). website: http://dir.yahoo.com/, Access date: 15/10/2017.

ABOUT THE AUTHORS

Dr. 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.

Dr. 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 are 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 HCI and Security Systems. His areas of interest are Software Engineering and Artificial Intelligence.

Dr. 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.

i-manager® Publications

3/343, Hill view, Town Railway Nager, Nagercoil
Kanyakumari Dist. Pin-629 001.
Tel: +91-4652-276675, 277675

e-mail: info@imanagerpublications.com
contact@imanagerpublications.com
www.imanagerpublications.com

i-manager Printing Press