A Machine Learning Approach for Detection of Phished Websites Using Neural Networks

K. Selvan, M. Vanitha

Abstract: Phishing is a means of obtaining confidential information through fraudulent website that appear to be legitimate On detection of all the criteria ambiguities and certain considerations involve hence neural network techniques are used to build an effective tool in identifying phished websites There are many phishing detection techniques available, but a central problem is that web browsers rely on a black list of known phishing website, but some phishing website has a lifespan as short as a few hours. These website with a shorter lifespan are known as zero day phishing website. Thus, a faster recognition system needs to be developed for the web browser to identify zero day phishing website .To develop a faster recognition system, a neural network technique is used which reduces the error and increases the performance. This paper describes a framework to better classify and predict the phishing sites.

Keywords: Detection, Machine Learning, Neural Network, Phishing, Security.

I. INTRODUCTION

Internet banking (e-banking) is defined as the automated delivery of new and traditional banking products and services directly to customers through interactive electronic communication channels. E-Banking includes the systems that enable customers, individuals or businesses, to access accounts, transact business, or obtain information on products and services through a public or private network, including the Internet. Commercial banking is undergoing rapid changes, as the international economy expands and advances towards institutional and market completeness. A major force behind these developments is technology, which is breaching geographical, industrial and regulatory barriers, creating new products, services and market opportunities, and developing more information and systems-oriented business and management processes. Phishing is a relatively new internet crime in comparison with other forms, e.g., virus and hacking. More and more phishing web pages have been found in recent years in an accelerative way. Its impact is the breach of information security through the compromise of confidential data and the victims may finally suffer losses of money or other kinds. A phishing website is a broadly launched social engineering attack that attempts to defraud people of their personal information including credit card number, bank account information, social security number, and their personal credentials in order to use these details fraudulently against them. Phishing has a huge negative impact on organizations revenues, customer relationships, marketing efforts, and overall corporate image.

Revised Version Manuscript Received on December 12, 2015.

K. Selvan, Research Scholar, Department of Computer Science, JJ College of Arts and Science (Autonomous), Pudukkottai, Tamilnadu, India.

Dr. M. Vanitha, Research Guide, Head, Department of Information Technology, JJ College of Arts and Science (Autonomous), Pudukkottai, Tamilnadu, India.

Phishing attacks can cost companies tens to hundreds of thousands of dollars per attack in fraud-related losses and personnel time. Even worse, costs associated with the damage to brand image and consumer confidence can run into the millions of dollars. In replication, the replicas for each data structure are identical to the given data structure. In fusion, the backup copies are not identical to the given data structures and hence, it make a distinction between the given data structures, referred to as primaries and the backup data structures, referred to as backups. There are many definitions of phishing website; we want to be very careful how we define the term, since it is constantly evolving. One of these definitions comes according to the Anti-Phishing Working Group (APWG)'s definition, "Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials". Typically a phishing attack is a combination of fraudulent emails, spoofed websites, and identity theft. Internet users or customers of many banks and financial institutions are the targets of phishing attacks.

II. RELATED WORK

In[1], Phishing is a means of obtaining confidential information through fraudulent website that appear to be legitimate .On detection of all the criteria ambiguities and certain considerations involve hence neural network techniques are used to build an effective tool in identifying phished websites There are many phishing detection techniques available, but a central problem is that web browsers rely on a black list of known phishing website, but some phishing website has a lifespan as short as a few hours. These website with a shorter lifespan are known as zero day phishing website. Thus, a faster recognition system needs to be developed for the web browser to identify zero day phishing website. The prediction of phishing websites is essential and this can be done using neural networks. For the prediction of phishing websites, earlier works were done using various data mining classification algorithms were used but the error rate of those algorithms were very high. When an element of the neural networks fails, it can continue without any problem because of its parallel nature. Thus performance can be made better by considering neural networks as it reduces the error and gives better classification. In[2], Machine-learning technique for modelling the prediction task and supervised learning algorithms namely Multi layer perceptron, Decision tree induction and Naïve bayes classification are used for exploring the results. It has been observed that the decision tree classifier predicts the phishing website more accurately when comparing to other learning algorithms. the phishing website prediction as a classification task and demonstrates the machine learning approach for predicting whether the given website

is legitimate website or phishing. Naïve Bayes classifier, Decision tree classifier, Multilayer perceptron have been applied for training the prediction model. Features have been extracted from a set of 200 url and the corresponding HTML source code of phishing and legitimate websites and the training dataset has been prepared in order to facilitate training and implementation. The performance of the models has been evaluated using 10-fold cross validation and two performance criteria, predictive accuracy and ease of learning. In [3], proposed a new neuro-fuzzy model without using rule sets for phishing detection. Specifically, the proposed technique calculates the value of heuristics from membership functions. Then, the weights are generated by a neural network. The proposed technique is evaluated with the datasets of 11,660 phishing sites and 10,000 legitimate sites. The results show that the proposed technique can detect over 99% phishing sites. We have proposed a new technique to detect phishing sites effectively. In the proposed technique, the system model is built to detect phishing sites by using neurofuzzy network and six heuristics (primarydomain, subdomain, pathdomain, pagerank, alexarank, alexareputation). The technique is experimented with the training dataset containing 11, 660 sites and 2 testing datasets that each dataset contains 5,000 phishing sites or 5,000 legitimate sites. The best results show that 99.10% phishing websites are detected by using the proposed technique. The proposed technique is compared to the technique and found that it is more efficient. [3]. In [4], we propose a hybrid model to classify phishing emails using machine learning algorithms with the aspiration of developing an ensemble model for email classification with improved accuracy. We have used the content of emails and extracted 47 features from it. The processed emails are provided as input to various machine learning classifiers. Going through experiments, it is observed and inferred that Bayesian net classification model when ensemble with CART gives highest test accuracy of 99.32%. With the emergence of phishing as a global security issue, detection and filtration of phishing emails from legitimate ones has become one of the challenging aspects. In this paper, we have extended previous model for some classification techniques like CART, CHAID and QUEST model and ensemble each model to the Bayesian net classification model. We concluded that ensemble of the Bayesian net classification model with these three models individually, gives noticeable increase in classification accuracy for each case.

III. PROPOSED WORK

Anti Phishing is a means of to protect confidential information through fraudulent websites that appear to be legitimate. On detection of phishing attacks, neural network techniques are used to build on effective tool to identifying phishing websites. There are several phishing detection techniques available, neural network for faster recognition system for web browser to identify phishing websites. Also neural network reduce error and increase the performance

IV. METHODOLOGY USED

4.1 Features

After referring to available literature, we have selected and defined a set of features that capture the characteristics of phishing emails.

4.1.1 Structural Features

Total number of body parts According to MIME standard, "Content-Type" attribute of one email could be multipart, meaning that this email has multiple body parts. Phishers are likely to utilize this fact to construct phishing emails with sophisticated structures. By counting the number of boundary variables, we obtain the number of body parts in a multipart email. If the "Content-Type" of the email is not multipart, this feature is set to0, for the purpose of differentiating from multipart emails with only one body part. If one part can be further divided into multiple parts, the number of sub-parts is added to the number of parts of the entire email. For example, if an email has 2 body parts, one of which has 2 sub-parts, the number of body parts is set to 4. However, only 3 parts of the content are scanned in the feature extraction process.

4.1.2 Link Features

Total number of links Phishing emails usually contain multiple links to fake web-sites for readers to sign in. Number of IP-based links A legitimate website usually has a domain name for identi-fication while phishers typically use multiple zombie sys-tems to host phishing sites. Besides, the use of IP address makes it difficult for readers to know exactly which site they are being directed to when they click on the link. Therefore, the presence of IP-based links can be a good indicator of phishing emails. Number of deceptive links Deceptive links are the ones with visible URLs different from the URLs to which they are pointing. Some phishers use this technique to fool email readers into clicking on the links.

4.1.3 Element Features

A Boolean indicator of whether it is in HTML format Phishing emails are mostly in HTML format as plain text does not provide the opportunity to play the tricks of phish-ing. A Boolean indicator of whether it contains JavaScript JavaScript enables phishers to perform many actions behind the scene, such as creating popup windows and changing the status bar of a web browser . If the email contains strings, "javascript" or "onclick", this feature is set to one.3. A Boolean indicator of whether it contains <Form> tagHTML forms are one of the techniques used to gather information from readers.

4.2 Neural Networks

An artificial neural network, or neural network, is a mathe-matical model inspired by biological neural networks. In most cases it is an adaptive system that changes its struc-ture during learning . There are many different typesof NNs. For the purpose of phishing detection, which is basically a classification problem, we choose multilayer feed forward NN. In a feed forward NN, the connections between neurons do not form a directed cycle. Contrasted with recurrent NNs, which are often used for pattern recog-nition, feed forward NNs are better at modeling relation-ships between inputs and outputs. In our experiments, we use the most common structure of multilayer feed forward NN, which consists of one input layer,

one hidden layer and one output layer. The number of computational units in the input and output layers corresponds to the number of inputs and outputs. Different numbers of units in the hidden layer are attempted in the following experiments. To fit our dataset, hyperbolic tangent and sigmoid are used as activation functions. A comparison of the two is also conducted. With regard to the training method, we choose resilient propagation training (RPROP), as it is usually the most efficient training algorithm for supervised feed for-ward NNs.

4.3 Other Machine Learning Techniques

To further evaluate the performance of NNs in phishing detection, we compare its performance against that of other major machine learning classifiers – decision tree (DT),K-nearest neighbors, naive Bayes (NB), support vector ma-chine (SVM) and unsupervised K-means clustering. The same dataset and feature set are used in the comparison.

4.4 Cross Validation

Given a training dataset and a proposed classifer, we as- sess the performance of the classifier by using hold-outcross validation, also known as simple cross validation. The dataset is randomly divided into Strain and Scv. The proposed classifier is trained on Strain to get parameter esti-mates and tested on Scv. We then obtain the output which indicates whether each email in Scv is ham or phishing. This procedure is repeated 20 times for different sizes of Strain and Scv. The proportions of the dataset used as Strainare as follows: 0.1%, 1%, 10%, 20%, 30%, 40%, 50%, 60%,70%, 80% and 90%.

4.5 Evaluation Metrics

By comparing the classification predictions with the actual categories of the emails, we are able to compute the numbers of true negatives (TN, correctly classified ham email),false negatives (FN, phishing email mistakenly classified asham), true positives (TP, correctly classified phishing email)and false positives (FP, ham email mistakenly classified as phishing). To evaluate the classifier performance, we compute the accuracy(Accu) and the weighted accuracy(Wacc) by the following formula:

$$Accu = \frac{TN + TP}{TN + FP + TP + FN} \quad (1)$$

$$w_{acc}(\lambda) = \frac{\lambda . TN + TP}{\lambda . (TN + FP) + TP + FN} \quad (2)$$

In phishing email filtering errors are not of equal importance. A false positive is much more costly than a false negative in the real world. It is thus desirable to have a classfier with a low false positive rate. The "weighted accuracy" measure is proposed by Androutsopoulos et al.[2] to address this issue. Different values of l can be ap-plied to the formula (1). Notice that when l is one, the FPand FN are weighed equally. In our simulations, we pickl = 9 so that FP are penalized nine times more than FN.In addition, we compute the precision, recall and F1-scoreof each classifer as follows:

$$Precision = \frac{TP}{TN + FP} \quad Recall = \frac{TP}{TN + FN} \quad (3)$$

$$F_1 = \frac{2.precision.recall}{precision + recall} \quad (4)$$

V. EXPERIMENTAL RESULT

The dataset is using from UCI Machine Learning Repository PHISHING WESITES. This dataset mainly collected the data from PhishTank archive, MillerSmiles archive, Googleâ€™s searching operators. There are 30 attributes are there to implemented and consisting nearly 2456 instances are gathered and manipulate the results.

The Attributes are,

1. having_IP_Address { -1,1 }
2. URL_Length {1, 0,-1 }
3. Shortining_Service { 1,-1 }
4. having_At_Symbol { 1,-1 }
5. double_slash_redirecting { -1,1 }
6. Prefix_Suffix { -1,1 }
7. having_Sub_Domain { -1,0,1 }
8. SSLfinal_State { -1,1,0 }
9. Domain_registeration_length { -1,1 }
10. Favicon { 1,-1 }
11. port { 1,-1 }
12. HTTPS_token { -1,1 }
13. Request_URL { 1,-1 }
14. URL_of_Anchor { -1,0,1 }
15. Links_in_tags { 1,-1,0 }
16. SFH { -1,1,0 }
17. Submitting_to_email { -1,1 }
18. Abnormal_URL { -1,1 }
19. Redirect { 0,1 }
20. on_mouseover { 1,-1 }
21. RightClick { 1,-1 }
22. popUpWidnow { 1,-1 }
23. Iframe { 1,-1 }
24. age_of_domain { -1,1 }
25. DNSRecord { -1,1 }
26. web_traffic { -1,0,1 }
27. Page_Rank { -1,1 }
28. Google_Index { 1,-1 }
29. Links_pointing_to_page { 1,0,-1 }
30. Statistical_report { -1,1 }
31. Result { -1,1 }

VI. RESULTS

The collected dataset holds categorical values i.e. “Legitimate”,”Suspicious” and “Phishy”. These values should be transformed to numerical values so that the neural network can perform its calculations thus we replaced the values 1,0 and -1 instead of “Legitimate”, “Suspicious” and “Phishing” respectively. We are interested in obtaining a model with a good generalisation performance. However, most models are susceptible to overfitting, which means, while the error rate on the training dataset decreases during the training phase, the error rate on the unseen dataset (testing dataset) increases at some point. To overcome this problem, we used the “Hold-Out” validation technique, by dividing our dataset into training, validation and testing datasets. The

examples in each dataset were selected randomly. We using Neural network validity measures like LTN (Low Treshold Neuron), RMSE (Root Mean Square Error), real log canonical threshold (RLCT) values,

VII. ALGORITHM

Initialize the weights vector
S = the training set fed to the network
Repeat
For each "input-output" pair denoted by P in S
In = input pattern in P
Out = desired output
Compute network output (netout)
network error = Out – netout
end For
Find weight change for weights connecting hidden to output
Find weight change for weights connecting input to hidden
Update weights
Until reaching (a satisfactory network error value OR maximum iteration)

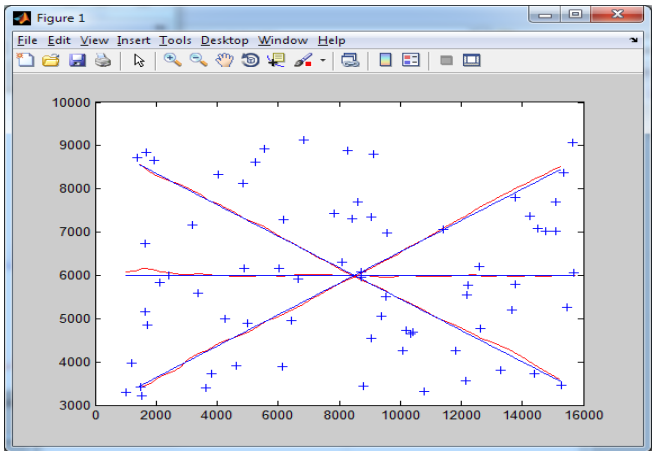

Figure1. Accuracy for Different Gamma And C Pairs

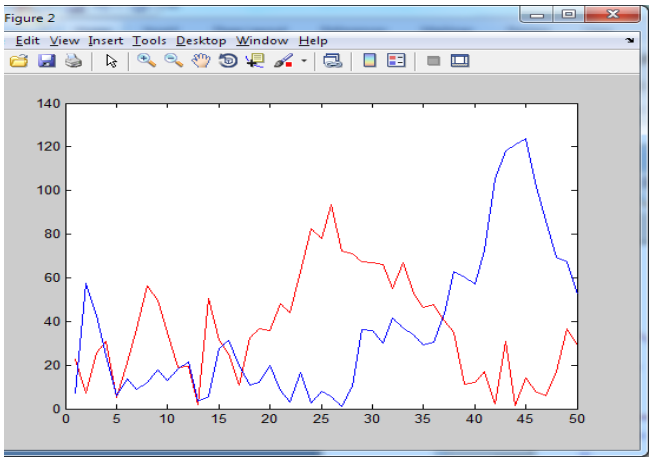

Figure2. Neural Network Results Using Different Features

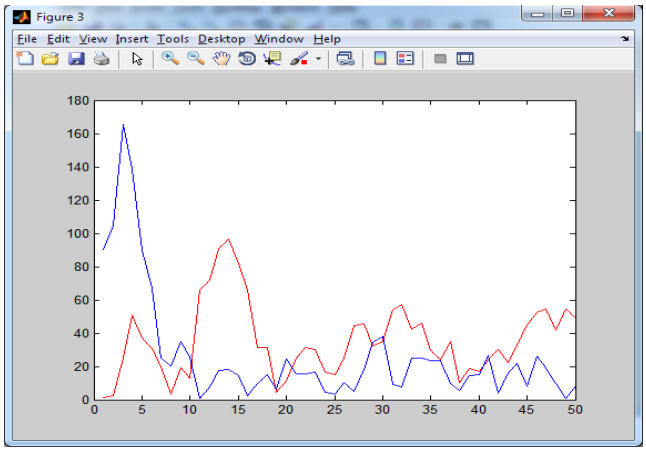

Figure3. Accuracy of NN With Activation Function

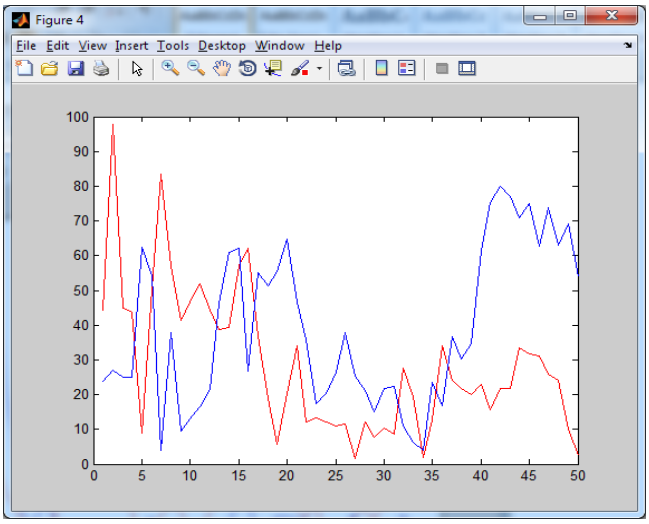

Figure4. Accuracy of NN With Machine Learning

VIII. CONCLUSION AND FUTURE WORK

The prediction of phishing websites is essential and this can be done using neural networks. For the prediction of phishing websites, earlier works were done using various data mining classification algorithms were used but the error rate of those algorithms were very high. When an element of the neural networks fails, it can continue without any problem because of its parallel nature. Thus performance can be made better by considering neural networks as it reduces the error and gives better classification. We believe that this framework works better and gives a lower error rate. In this work proposed a phishing detection approach that classifies the webpage security by checking the webpage source code, we extract some phishing characteristics to evaluate the security of the websites, and check the webpage source code, if we find a phishing character, and we will decrease from the initial secure weight. Finally we calculated the security percentage based on the final weight, the high percentage indicates secure website and others indicates the website is most likely to be a phishing website. Overall, the propose system to show that NN is a good technique in predicting phishing websites. In near future the system is automating the process of building a NN in order to reduce the training time. As a future work we plan to use more machine learning algorithms to compare accuracy rates.

We also plan to do a thorough feature ranking and selection on the same data set to come up with the set of features that produces the best accuracy consistently by all the classifiers. More functionally can be added for protecting user against key-loggers and screen-grabbers and client side scripting attacks. The uses Google search to validate a URL which can be refined by using more external repositories such as Yahoo search etc. Artificial neural network approach an achieves 97% accuracy. This can be improved by adding more rules and using other machine learning approaches.

REFERENCES

1. A Machine Learning Approach for Detection of Phished Websites Using Neural Networks by Charmi J. Chandan, Hiral P. Chheda, Disha M. Gosar, Hetal R. Shah.
2. Efficient prediction of phishing websites using supervised learning algorithms by Santhana Lakshmi V, Vijaya MS.
3. An Efficient Approach for Phishing Detection Using Neuro-Fuzzy Model by Luong Anh Tuan Nguyen, Ba Lam To, and Huu Khuong Nguyen.
4. Development of Anti-Phishing Model for Classification of Phishing E-mail by Niharika Vaishnaw , S R Tandan.
5. Evolving Fuzzy Neural Network for Phishing Emails Detection-Ammar ALmomani, Tat-Chee Wan
6. Phishing Detection Using Neural Network-Ningxia Zhang, YongqingYuanFreedman
7. Detection of Phishing Attacks: A Machine Learning Approach-Ram Basnet, Srinivas Mukkamala, and Andrew H. Sung
8. A Framework for Predicting Phishing Websites Using Neural Networks-A.Martin1, a.Ba.Anutthamaa, M.Sathyavathy, Marie Manjari Saint Francois, Dr.PrasannaVenkatesan
9. Phishing Activity Trends Report- 2nd Quarter 2012-APWG
10. Techniques for detecting zero day phishing websites by Michael Blasi
11. www.phishtank.com
12. Saeed Abu-Nimeh, Dario Nappa, Xinlei Wang, and Suku Nair. A comparison of machine learning techniques for phishing detection. In Proceedings of the Anti-Phishing Working Group eCrime Researchers Summit, pages 649–656, 2007.
13. Ion Androutsopoulos, John Koutsias, Konstantinos V.Chandrinos, George Paliouras, and Constantine D.Spyropoulos. An evaluation of naive bayesian anti-spam filtering. In Proceedings of the Workshop on Machine Learning in the New Information Age, 11th European Conference on Machine Learning, Barcelona,Spain, 2002.
14. Ram Basnet, Srinivas Mukkamala, and Andrew H.Sung. Detection of phishing attacks: A machine learning approach. Studies in Fuzziness and Soft Computing,226:373–383, 2008.
15. Madhusudhanan Chandrasekaran, Krishnan Narayanan, and Shambhu Upadhyaya. Phishing e-mail detection based on structural properties. In Proceedings of the NYS Cyber Security Conference, 2006.
16. James Clark, Irena Koprinsk, and Josiah Poon. A neural network based approach to automated e-mail classification. In Proc. IEEE/WIC International Conference on Web Intelligence (WI), pages 702–705, 2003.
17. Ian Fette, Norman Sadeh, and Anthony Tomasic. Learning to detect phishing emails. In Proceedings of the International World Wide Web Conference(WWW), 2007.
18. Network Working Group. Multipurpose internet mail extensions (MIME) part two:media types. http://tools.ietf.org/html/rfc2046#section-5.1.4,1996.
19. Andrew Ng. CS229 lecture notes. http://cs229. stanford.edu/notes/cs229-notes5.pdf, 2012
20. Martin Riedmiller and Heinrich Braun. A direct adaptive method for fast back propagation learning: The rprop algorithm. In Proceedings of the IEEE International Conference on Neural Networks, volume 5, pages 586–591, 1993.