TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 11972 - 11979

A Review of Phishing Email Detection Approaches with Deep Learning Algorithm Implementation

Nursyafiqah Hazira Mohamad Nazir, Faculty of Computing and Informatics, Universiti Malaysia Sabah, Kota Kinabalu, Malaysia.
Nordaliela Mohd Rusli, Faculty of Computing and Informatics, Universiti Malaysia Sabah, Kota Kinabalu, Malaysia.
Tan Soo Fun, Faculty of Computing and Informatics, Universiti Malaysia Sabah, Kota Kinabalu, Malaysia.
Chin Kim On, Faculty of Computing and Informatics, Universiti Malaysia Sabah, Kota Kinabalu, Malaysia.

Article Info
Volume 82
Page Number: 11972 - 11979
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 21 February 2020*

Abstract
Phishing email is designed to mimics the legitimate emails to fool the victim into revealing their confidential information for the phisher's benefit. There have been many approaches in detecting phishing emails but the whole solution is still needed as the weaknesses of the previous and current approaches are being manipulated by phishers to make phishing attack works. This paper provides an organized guide to present the wide state of phishing attack generally and phishing email specifically. This paper also categorizes machine learning into shallow learning and deep learning, followed by related works in each category with their contributions and drawbacks. The main objective of this review is to uncover the utility of machine learning in general, and deep learning in particular, in order to detect phishing email by studying the literature. This will provide an insight of the phishing issue, the alternatives prior to the phishing email detection and the contrast of machine learning and deep learning approaches in detecting phishing emails.

Keywords: *deep learning, detection, machine learning, phishing email.*

I. INTRODUCTION

Phishing attack is one today's most prevalent and severe threats to cyberspace. Phishing in general is a technique of deception that employs social engineering and technology to convey socially engineered messages as a trustworthy institution or entity. Phishing uses electronic communication channels such as emails, Hypertext Transfer Protocol (HTTP), Short Message Service (SMS), Voice over Internet Protocol (VoIP), and other more to deliver the socially engineered messages to persuade victims to perform certain actions, for the attacker's benefit. The attacks are designed to steal victim's confidential information by mimicking the legitimate entities [8]-[9], [18].

In 2017, according to [23], phishing attempts have grown 65% while report by [33] stated that 76% of business became a victim of phishing attack. Subsequently, according to [7], the number of phish detected in the first quarter of 2018 was up by 46% over the last quarter of 2017 from 180,557 to 263,538 total number of phish detected.

According to [29], the main motives of the phishing attacks or the attacker's intention behind the phishing attacks are:

a. Financial gain: Attackers gain financial benefits from the stolen banking credentials.
b. Identity hiding: Attackers will offer victims' identities to those who may be criminal who tries to hide their identities and activities.
c. Fame and notoriety: Sometimes the attackers attack victims mainly for peer recognition process.

There are two types of phishing attacks and it can be classified based on the mechanism that allows attackers to acquire victim's confidential information. The mechanisms are either an attacker

January - February 2020
ISSN: 0193 - 4120 Page No. 11972 - 11979

uses deceptive phishing in which the attacker frauds the victims, or a malware-based phishing where the attacker use any malicious code to access the victim's privacy. The first type of phishing attack is associated to social engineering schemes that rely on fake emails that seems to be from a trusted businesses and agencies to fraudulently obtain the victim's financial data and personal information by way of an embedded link in the email that redirects users to fake websites. The second type of phishing attack includes technical subterfuges schemes that use malicious code or malware that require user to click on the email link or using security holes on the user's computer to acquire victim's online account information directly [3], [22].

Phishing attacks are the most accessible form of attack in terms of investment and level of technical skills needed, given the prevalence of other types of cybercrime. Phishing is also a semantic attack aimed at exploiting the way people perceive computers instead of manipulating the technical system's weaknesses [2], [5], [16]. Phishing mainly affects the information technology by jeopardizing user information that hurt victims in terms of financial losses and valuables. Moreover, people lose their confidence in Internet transaction for fear of becoming a victim and eventually can hurt Internet business [2], [16].

In this paper, the type of phishing attack that is focuses on is phishing attack by social engineering as it is one of the common methods for phisher to steal information from the victim. Phishing email is designed to mimics legitimate emails to fool the victim and steal their confidential information through clicking on the link embedded in the email. To trick user into thinking that the email is from credible and trusted source, phishing emails normally contains graphic, text or design elements [21].

A lot of studies have been done in the field of phishing email detection to counter the growing problem of phishing emails. The purpose of this paper is to have structured guide to portray the extensive literature of phishing email detection. The main contribution of this paper is to uncover the utility of deep neural network or deep learning in detecting phishing email. Other than that, this review will provide an overview in the field of phishing detection which can assist academia, industries and researchers to find the most ideal approach for phishing email detection as well as overcoming the limitations of previous phishing email detection approaches. The remainder of the paper is organized as follows: related works are discussed in Section II. Section III discuss the literature survey on existing phishing email detection approaches using deep learning or deep neural network and Section IV concludes the paper.

II. RELATED WORKS

Since phishing causes serious abuse of user confidential information and hurt Internet business, there have been many approaches proposed to detect phishing attack. "Phishing attack approaches are identified by five different phases of the attack flow, such as network level protection, authentication, client-side tool, user education and server-side filter and classifiers [4]". The categories and their matching subcategories will be reviewed and summed up in Table 1. Subsequently, part A in this section reviews phishing email detection using machine learning.

Table 1. Classification of approaches against phishing attack

	Description	Discussion and Summaries
Network level protection	Set of domains and IP addresses are barred from entering the network. The messages from system that send spam or phishing email will be blocked by administrator. Examples of network level protection tools are domain name system blacklist [30] and Snort [24].	For this network level protection, time to time update is needed and it can only be changed as it is reactive in nature once the trend of abuse has been witnessed for some time.
Authentication	"Designed to confirm whether email was sent by valid path and domain name not being imitated by attacker" [4]. This authentication level work at two levels	This technology is not pervasive as it does not have enough of agreement between mail service providers.

January - February 2020
ISSN: 0193 - 4120 Page No. 11972 - 11979

	which are, user level and domain level.	
Client-side tools	"Include user profile filters and browser-based toolbars such as SpoofGuard [12], NetCraft [31], CloudMark [32] and etc." [4]	User will eventually become a victim of phishing attacks when they do not pay attention to the dialog boxes of warning.
User education	Refers to increasing the exposure and guidance on phishing attack in overall and phishing email in specific, to the Internet users. There are two approaches, first approach is education-based approach which offer online information about phishing and the avoidance technique, and another approach is online training and testing.	It is helpful but not sufficient as phishers can generate phishing email with enough detail that make users unable to recognize whether it is legitimate or fake.
Server-side filter and classifier	Differs with an extracted set of phishing email features trained in machine learning algorithms by incorporating statistical classifier to distinguish legitimate and phishing email.	As the usage of feature sets unable to adjust to technological changes, it shows many weak points. From the results, too many misclassifications and classifiers do not deliberately classify words misspelled, merged and disjointed. Clever changes can be made by phishers attempts to use different words.

A. Phishing Email Detection Using Machine Learning

Machine learning (ML) is the new approach to artificial intelligent (AI) that mainly used in supervised learning to build predictive models, in which algorithm or a classifier maps the inputs to the desired outputs using a particular function. Machine learning approach is applicable to solve phishing email detection problem as the problem can be converted into a standard task of classification. Classifier will attempt to study several features in classification problem to determine the output or response. With regard to the classification of phishing emails, the classifier classifies emails into legitimate emails or phishing emails by studying the features of the emails [1], [25]. A review of few research studies that apply machine learning algorithms in phishing email detection is summarized in the following.

An experimental study to compare five machine learning algorithms namely as Classification and Regression Trees (CART), Logistic Regression (LR), Random Forest (RF), Bayesian Additive Regression Trees (BART), Support Vector Machine (SVM) and Neural Network (NN) was conducted to classify emails as legitimate or phishing. The training datasets have been used with 43 email features and 2889 emails. The test method used was tenfold cross validation to produce the results and using the evaluation measures of accuracy, recall and harmonic mean. RF obtained a lower error rate from the results while highest error rate among the classifiers is produced by NN. It also produced the least false positive rate among all algorithms, despite RF generating the highest predictive classifier. The authors argue that features more carefully selected can improve phishing email detection performance [1].

Structural features in which the implementation of the prototype takes place between user's mail transfer agent (MTA) and mail user agent (MUA) was proposed and the simulated annealing is applied as an algorithm for the selection of features. There are three categories used in phishing email classification:

a. Amount of features style maker derived from emails

b. The structural attributes

c. Frequency distribution of selected words

The features then evaluated by using Support

January - February 2020
ISSN: 0193 - 4120 Page No. 11972 - 11979

Vector Machine (SVM) classifier with accuracy of 95%. On the contrary, the result was based on small dataset [11].

The development of new RF method called "Phishing Identification by Learning on Features of Email Received" (PILFER) was resulted from the deployment of C4.5 decision tree classifier. The experiment was done using 860 phishing emails and 695 legitimate emails. Several features to differentiate the phishing email are identified as follows: IP URLs, time of space, HTML messages, number of connections inside email and Javascript. The authors believed that PILFER could be advanced by adding all the classifier's features except for "Spam filter output" to group messages [14].

A technique was presented that work based on 16 features. This technique also able to detect phishing email even with finite prior knowledge. Many machine learning algorithms such as SVM, Biased SVM, Leave One Model Out, Neural Network (NN) and Self Organizing Maps (SOMs) which mostly were supervised learning based, adapted in this technique to do phishing email classification. Some authors used unsupervised learning performed by SOMs which depends on analysis produced through U-matrix and the accuracy was 90.8% using 4000 samples which consists of 50% legitimate and another 50% phishing emails. The best algorithm from the result was Biased SVM. Biased SVM and NN have similar 97.99% accuracy and NN shows trouble with valuable information for the future [9].

A comparison that compare approaches to binary and ternary classification was presented in which spam and not spam are the examples of binary classification, while ham, spam and phishing are the ternary classification. 30 features used by some of the authors, 15 features were taken from other researchers and 15 features for "online and offline" features to filter phishing email. From the result, the accuracy of the classification of the new features increased by using the ternary classification, and reached up to 97% by adapting SVM. However, this technique is highly expensive as the access to online features depends on the internet connection status. Other than that, this method requires large servers of mail and can affect the efficiency and usability of the email filtering system by extracting too many online features [15].

Another approach based on machine learning is Neural Network (NN). Trial and error are one of the most prevalent ways of training a NN [20]. The time spent adjusting the parameters and the necessity of the domain expert has made this method criticized. Anti-phishing model of the NN based on self-structuring classification was proposed instead of the use of trial and error [26]. Before adding a new neuron to the hidden layer, the algorithm proposed by the authors dynamically updated a few parameters, such as learning rate. During the construction of the classification model, the updating process for these neural network features is carried out according to network environment, the actions of the required error rate and the calculated error rate at that point.

In order to detect phishing on large UCI dataset with more than 11,000 websites, the dynamic neural network model was applied and experiment were conducted using different epoch sizes (100, 200, 500, 100) and the result showed better predictive systems compared to Bayesian Network and Decision Trees.

III. PHISHING EMAIL DETECTION USING DEEP LEARNING

As machine learning expands, several established methods are being polished with the capacity to understand and adapt to real problems. The environment is greatly valued and this results in the adaption of machine learning in variety fields, such as computer vision, medical analysis, gaming and social media marketing [17]. Machine learning is better for certain cases than traditional algorithms based on rules or even human operators [19]. This pattern has an impact on cyber security where certain detection systems have been updated to ML components [10]. Machine learning is classified into two categories as shown in Figure 1. The first one is referred as Shallow Learning (SL) which demands domain expert to conduct crucial tasks to identify the relevant data qualities before

January - February 2020
ISSN: 0193 - 4120 Page No. 11972 - 11979

practicing SL algorithm, and the second is Deep Learning (DL) which depended on a multi-layered input data representation and picks features independently through a representation learning process [6]. To be further characterized, SL and DL can be differentiated by either supervised or unsupervised algorithms.

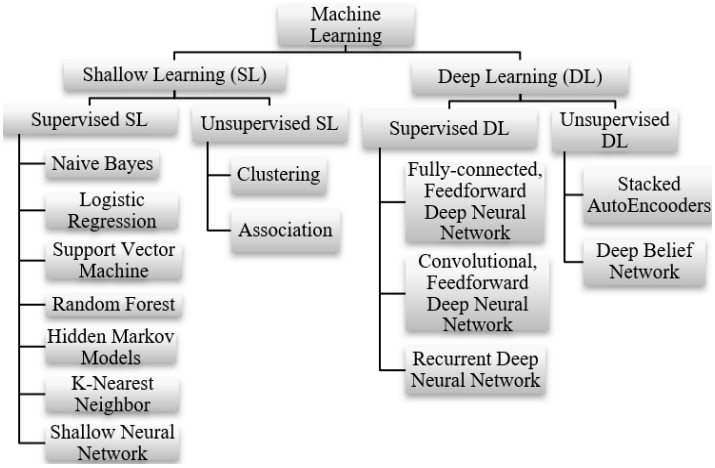

Fig 1. Classification of Machine Learning (Source: On the Effectiveness of Machine and Deep Learning for Cyber Security, 371–390)

A. Background

Deep learning is a specific subset of machine learning and is defined as mathematical framework that focus on learning the successive layers of increasingly significant representations. In deep learning, these layered representations are learned based on Deep Neural Network (DNN) which structured in many layers capable of autonomous representation learning. Tens or hundreds of successive representation layers often involve in modern deep learning and they are learned automatically from the exposure of training data. Meanwhile, learning only one or two layers of representation of the data is the focus in shallow learning [6], [13].

From Figure 1, we can see that deep learning is differentiate into supervised or unsupervised algorithms. There are three deep learning algorithms and two unsupervised deep learning algorithms. The supervised deep learning algorithm includes:

a. Fully-connected Feedforward Deep Neural Networks (FNN): A form of DNN in which each neuron in the previous layer is connected to other neurons. Flexible and general-purpose classification solution is obtained at the expense of high computational costs and the input data is not assumed.

b. Convolutional Feedforward Deep Neural Networks (CNN): The trait where each neuron receives only input from the previous layer neuron subset makes CNN practical for spatial data analysis. But the performance will decrease when adapted to non-spatial data. CNN's computational costs are lower compared to FNN.

c. Recurrent Deep Neural Network (RNN): A form of DNN which hard to train compared to FNN because of the design in which neurons can send output to the previous layers. As sequence generators, it is particularly good for long short-term memory.

While, the unsupervised deep learning algorithm includes:

a. Deep Belief Network (DBN): A group of non-output layered neural networks modeled on the formation of Restricted Boltzmann Machines (RBM) that can be used for pre-training task as they are excellent in the feature extraction function. It needs unlabeled training phase datasets.

b. Stacked Autoencoders (SAE): A group of neural networks in which autoencoders from the same number of input and output neurons. Small datasets give better results and good at pre-training similar to DBN.

B. Related Works

Evaluating which category of algorithms that can achieve essential results is very crucial as machine learning and deep learning approaches are gradually used for different applications to detect phishing emails. Now that deep learning is still at an initial stage, to the best of our knowledge, there are not many papers proposed on phishing email detection using deep learning algorithm. Therefore, we will review two case studies that apply deep learning algorithms in the detection of phishing email.

A work that use word embedding and Neural Bag-of-ngrams with deep learning methods such as Convolutional Neural Network (CNN), Recurrent

January - February 2020
ISSN: 0193 - 4120 Page No. 11972 - 11979

Neural Network (RNN), long short-term memory (LSTM) and multi-layer perceptron (MLP) was proposed to detect phishing email. The function of word embedding and Neural Bag-of-ngrams is to extract syntactic and semantic similarity of emails. Meanwhile the deep learning algorithms is to extract the abstract and optimal feature representation and fully connected layer with non-linear activation function for classification. All of the experiments are done on anti-phishing shared task corpus at IWSPA-AP 2018 and run on GPU enabled TensorFlow in conjunction to Keras. From the experimental results, word embedding with deep learning especially LSTM claimed to be appropriate for the phishing email detection. The author claimed that one significant direction towards the future work is to enhance the phishing email detection rate by adding additional extra publicly available or private data sources. Deep learning architectures can be trained by using advanced hardware but the author also claimed that they were not able to train complex deep learning architecture because of the computational cost and other constraints [28].

Other research studies that apply deep learning algorithm in phishing email detection proposed a model that use Keras Word Embedding and Convolutional Neural Network (CNN) to classify the emails into legitimate and phishing emails. The combination of Keras word embedding and CNN provides a dense vector representation for words which then used to classify emails given in the datasets. The dataset consists of two sets of datasets. The first task, namely as Task 1 with header files and for Task 2, without the header files. As for the training dataset, Task 1 consists of 4583 emails in which 4082 were legitimate and another 501 were phishing emails. For Task 2, total of 5700 emails were given and 5088 were legitimate and another 612 were phishing emails. A total of 4195 email given to Task 1 and 4300 to Task 2 for the test dataset. The authors claimed that, for both subtasks, the model performed well with the accuracy rate of 0.968 for task without header and 0.942 for task with header. The authors were able to get good detection rate for phishing email in both subtasks without using any external datasets and consider adding some additional data source can increase the phishing email detection rate [27].

IV. CONCLUSION

There have been tremendous efforts in detecting phishing emails but the whole complete solution is still needed as the weaknesses of the approaches are being manipulated by the phishers to make phishing attack works. Machine and deep learning approaches are also growingly utilized for the detection of phishing emails. As a consequence, it is important to determine which category of algorithm can offer better result. From the review, we can see that there are several limitations and challenges in using deep learning approaches which can affects and reduce the effectiveness of phishing email detection such as, computational cost, the impact of dataset size, and others. According to [19], it is true that deep learning can outdo shallow learning, but only in some application such as computer vision and there is no final conclusion that can be taken since deep learning is still at an initial phase. As a matter of a fact, we are still finding the great extent of what deep learning can do in phishing email detection and the scope of the future review might be expanded. The results from the review of phishing email detection approaches using deep learning can be further improved by enhancing training or by adding additional data sources, as the direction towards the future work.

ACKNOWLEDGMENT

This work is supported by Skim Geran Penyelidikan Universiti Malaysia Sabah (SGPUMS) under grant SBK0366-2017.

REFERENCES

[1] Abu-Nimeh, S., Nappa, D., Wang, X., & Nair, S.:A comparison of machine learning techniques for phishing detection. PROCEEDINGS OF THE ANTI-PHISHING WORKING GROUPS 2ND ANNUAL E-CRIME RESEARCHERS SUMMITON - ECRIME '07, 60–69 (2007). https://doi.org/10.1145/1299015.1299021

[2] Akanbi, O. A.: A Machine Learning Approach to Phishing Detection and Defense (2015). https://doi.org/10.1016/B978-0-12-802927-5/00008-3

January - February 2020
ISSN: 0193 - 4120 Page No. 11972 - 11979

[3] Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E.: A Survey of Phishing Email Filtering Techniques, *15*(4), 2070–2090 (2013).

[4] ALmomani, A., Gupta, B. B., Wan, T.-C., Altaher, A., & Manickam, S.: Dynamic Evolving Neural Fuzzy Framework for Phishing E-Mail Detection, (March), 3960–3964 (2013).

[5] Alnajim, A., & Munro, M.: An approach to the implementation of the anti-phishing tool for phishing websites detection. INTERNATIONAL CONFERENCE ON INTELLIGENT NETWORKING AND COLLABORATIVE SYSTEMS, INCOS 2009, 105–112 (2019). https://doi.org/10.1109/INCOS.2009.3

[6] Apruzzese, G.: On the Effectiveness of Machine and Deep Learning for Cyber Security, 371–390 (2018).

[7] AWPG: Phishing Activity Trends Report 1 Quarter. *Most*, *1*(March), 1–12 (2018).

[8] Bahnsen, A. C., Bohorquez, E. C., Villegas, S., Vargas, J., & Gonzalez, F. A.: Classifying phishing URLs using recurrent neural networks. ECrime Researchers Summit, ECrime, 1–8 (2017). https://doi.org/10.1109/ECRIME.2017.7945048

[9] Basnet, R., Mukkamala, S., & Sung, A. H.: Detection of phishing attacks: A machine learning approach, *226*, 373–383 (2008). https://doi.org/10.1007/978-3-540-77465-5_19

[10] Buczak, A. L., & Guven, E.: A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176 (2016). https://doi.org/10.1109/COMST.2015.2494502

[11] Chandrasekaran, M., Narayanan, K., & Upadhyaya, S.: Phishing E-mail Detection Based on Structural Properties. NYS CYBER SECURITY CONFERENCE, 1–7 (2006). https://doi.org/10.1109/SPW.2014.26

[12] Chou, N., Ledesma, R., Teraguchi, Y., Mitchell, J. C., & Ca, S.: Client-side defense against web-based identity theft (2004).

[13] François C.: Deep Learning with Python. Manning Publications Company (2017)

[14] Fette, I., Sadeh, N., & Tomasic, A.: Learning to detect phishing emails. Proceedings of the 16th International Conference on World Wide Web - WWW '07, 649 (2007). https://doi.org/10.1145/1242572.1242660

[15] Gansterer, W. N., & Pölz, D.: E-Mail Classification for Phishing Defense. In M. Boughanem, C. Berrut, J. Mothe, & C. Soule-Dupuy (Eds.), Advances in Information Retrieval (pp. 449–460). Berlin, Heidelberg: Springer Berlin Heidelberg (2009).

[16] Jameel, N. G. M.: Detection of Phishing Emails using Feed Forward Neural Network, *77*(7), 10–15 (2013). https://doi.org/10.5120/13405-1057

[17] Jordan, M. I., & Mitchell, T. M.: Machine learning: Trends, perspectives, and prospects. Science, *349*(6245), 255–260 (2015). https://doi.org/10.1126/science.aaa8415

[18] Khonji, M., Iraqi, Y., & Jones, A.: Phishing detection: A literature survey. IEEE Communications Surveys and Tutorials, 15(4), 2091–2121 (2013). https://doi.org/10.1109/SURV.2013.032213.00009

[19] Lecun, Y., Bengio, Y., & Hinton, G.: Deep learning. *Nature*, *521*(7553), 436–444 (2015). https://doi.org/10.1038/nature14539

[20] Mohammad, R. M., Thabtah, F., & McCluskey, L.: Predicting phishing websites based on self-structuring neural network. Neural Computing and Applications, *25*(2), 443–458 (2014). https://doi.org/10.1007/s00521-013-1490-z

[21] Moradpoor, N., Clavie, B., & Buchanan, B.: Employing Machine Learning Techniques for Detection and Classification of Phishing Emails, (July), 149–156 (2017).

[22] Nalin, B. B. G., & Kostas, A. G. A.: Defending against phishing attacks : taxonomy of methods, current issues and future directions, 247–267 (2018). https://doi.org/10.1007/s11235-017-0334-z

[23] PhishMe.: Human Phishing Defense Enterprise Phishing Resiliency And Defense Report 2017 Analysis Of Susceptibility, Resiliency And Defense Against Simulated And Real Phishing Attacks (2017). Retrieved from https://cofense.com/wp-content/uploads/2017/11/

January - February 2020
ISSN: 0193 - 4120 Page No. 11972 - 11979

Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf

[24] Ramanathan, V., & Wechsler, H.: phishGILLNET — Phishing Detection Methodology Using Probabilistic Latent Semantic Analysis, AdaBoost, and co-training, 1–22 (2012).

[25] Tan, C. L., Chiew, K. L., & Sze, S. N.: Phishing Webpage Detection Using Weighted URL Tokens for Identity Keywords Retrieval. In H. Ibrahim, S. Iqbal, S. S. Teoh, & M. T. Mustaffa (Eds.), 9TH INTERNATIONAL CONFERENCE ON ROBOTIC, VISION, SIGNAL PROCESSING AND POWER APPLICATIONS (pp. 133–139). Singapore: Springer Singapore (2017).

[26] Thabtah, F., Qabajeh, I., & Chiclana, F.: Constrained dynamic rule induction learning. Expert Systems with Applications, *63*, 74–85 (2016). https://doi.org/10.1016/j.eswa.2016.06.041

[27] Unnithan, N. A., & Vidyapeetham, A. V.: Deep Learning Based Phishing E-mail Detection, (IWSPA) (2018).

[28] Vinayakumar, R., Barathi Ganesh, H. B., Anand Kumar, M., Soman, K. P., & Poornachandran, P.: DeepAnti-PhishNet: Applying deep neural networks for phishing email detection CEN-AISecurity@IWSPA-2018. CEUR Workshop Proceedings, 2124, 39–49 (2018).

[29] Yu, W. D.: A Phishing Vulnerability Analysis of Web Based Systems, 326–331 (2008).

[30] DNSBL Homepage, https://www.dnsbl.info/, last accessed 2019/04/26

[31] Netcraft Homepage, https://toolbar.netcraft.com/, last accessed 2019/04/26

[32] CloudMark Homepage, https://www.cloudmark.com/en/s/desktopone, last accessed 2019/04/26

[33] 2018 State of Phish, https://www.wombatsecurity.com/state-of-the-phish-2018, last accessed 2019/04/26

AUTHORS PROFILE

Nursyafiqah Hazira Mohamad Nazir (Pursuing MSc. Computer Science) is currently pursuing her Master from Universiti Malaysia Sabah. Her area of interest is Machine Learning.

Nordaliela Mohd Rusli is currently working as lecturer in Universiti Malaysia Sabah. Her research area includes System and Network Management and Quantitative Science.

Dr. Tan Soo Fun is currently working as senior lecturer in Universiti Malaysia Sabah. Her research area and interests includes Cryptography, Data Security, Information Security, Network Security, Secure Big Data Analytics and Internet of Things.

Dr. Chin Kim On is currently working as senior lecturer in Universiti Malaysia Sabah. His research area and interests includes Gaming AI, Neural Networks, Artificial Intelligence, Evolutionary Computing, Image and Video Processing, and Biometric Security System.