Chapter

Intelligent Decision Support System

Moruf Akin Adebowale

Abstract

A phishing attack is one of the most common forms of cybercrime worldwide. In recent years, phishing attacks have continued to escalate in severity, frequency and impact. Globally, the attacks cause billions of dollars of losses each year. Cybercriminals use phishing for various illicit activities such as personal identity theft and fraud, and to perpetrate sophisticated corporate-level attacks against financial institutions, healthcare providers, government agencies and businesses. Several solutions using various methodologies have been proposed in the literature to counter web-phishing threats. This research work adopts a novel strategy to the detection and prevention of website phishing attacks, with a practical implementation through development towards a browser toolbar add-in. The IPDS is shown to be highly effective both in the detection of phishing attacks and in the identification of fake websites. Experimental results show that approach using the CNN + LSTM has a 93.28% accuracy with an average detection time of 25 seconds, whilst the approach has a slightly lower accuracy. These times are within typical times for loading a web page which makes toolbar integration into a browser a practical option for website phishing detection in real time. The results of this development are compared with previous work and demonstrate both better or similar detection performance. This is the first work that considers how best to integrate images, text and frames in a hybrid feature-based solution for a phishing detection scheme.

Keywords: cybercrime, deep learning, convolutional neural network (CNN), long short-term memory (LSTM), big data

1. Introduction

The use of technology for fraudulent activities has flourished in recent years. The technical resources required to carry out phishing attacks are readily available through private and public sources. Hence, some of these technical resources have been automated and streamlined, thereby allowing their use by non-technical criminals. This automation has made it easier for a larger population of less-sophisticated criminals to commit crimes online, as it has made phishing more viable and economical.

In the recent times, there has been a considerable increase in the assortment, technology and complexity of phishing attacks in response to the increase in countermeasures and user awareness in order to sustain profitability from the illegal activities by the phisher [1]. Providing the ability to detect website phishing attacks may help individual users or organisations in identifying legitimate websites. The effectiveness in recognising an attack may significantly contribute to the making

of an effective decision between a fake and legitimate site [2]. Phishing is a form of social engineering attack in which an attacker, also known as a phisher, attempts to fraudulently retrieve sensitive user information by sending an email claiming to be a legitimately established organisation. They scam the user into giving confidential information that will be used for identity theft [2]. A phisher uses various methods, including email, web pages, and malicious software, to steal personal information and account credentials [3]. The aim of the phishing website is to use users' private information without their permission, and they do this by developing a new website that mimics a reliable website [4].

Hence, phishing website detection has become the object of a great deal of consideration among many academics who are attempting to find ways to incorporate malicious detection devices into web servers as a safety precaution [5]. Despite there being several ways to carry out phishing attacks, current phishing detection techniques unfortunately only cover some attack vectors such as fake website and emails [6]. Moreover, phishing has become more sophisticated, and such attacks can now bypass the filters that have been put in place by anti-phishing techniques [7]. Some detection techniques have been proposed, but most of them only deal with spoof web pages [8]. However, it is quite challenging in detection due to the evading techniques that the phisher uses.

Currently, machine learning is continuously demonstrating its effectiveness in an extensive range of applications. This technology has come to the fore in recent times, owing to the advent of big data [9]. Big data has enabled machine learning algorithms to discover more fine-grained patterns and to make more accurate and timely predictions than ever before [10]. Machine learning techniques are used for object identification in images, the transcription of voice into text, matching news items and products with user interests and presenting relevant search results [11]. The most common form of machine learning, whether deep or not, is supervised learning [12]. Previous methods have failed to combine the usage of frames, images, and text to develop an effective phishing detection method. Because using only text which is the common trend to a detection phishing website, this will not be effective as some changes can be made to the frame and the image. Doing so is, therefore, the focus of this work and therein lies its originality as well using the deep learning of Convolutional Neural Network (CNN) and Long short-term memory (LSTM) as classification algorithm in this solution.

Given the above, the objective is to develop a solution that includes the decision support system for detection of phishing attacks as well as providing insights and improving awareness as to how active Internet users can protect themselves against phishing attacks. It is hoped that this will help to formulate an upward trend in the practice of preventive measures against cyber-security issues. Despite various approaches having been utilised to develop anti-phishing tools to combat phishing attacks, these methods suffer from limited accuracy [1].

The main aim of this research is to develop an intelligent phishing detection and protection scheme for identification of website-based phishing attacks. This goal involves improving on previous work by building a robust classifier for intelligent phishing detection in online transactions. In order to achieve this aim the intelligent phishing detection support system should possess the following characteristics:

1. **Robustness**: It should have a hybrid algorithm that can support efficient classification for website phishing detection in real-time.

2. **Accuracy**: It should improve accuracy by reducing the false positive (FP) rate and increasing the true positive (TP) rate with absolute precision.

3. **Optimisation:** It should be able to optimise performance by employing a hybrid method that uses the features of website images, frames, and text for the user's objectives.

4. **Real-time functionality:** It should notify the user about the about the legitimacy of the website before the user web browser loads the intended page.

These requirements will be met by achieving the following five specific objectives:

I. Examine the Adaptive Neuro-fuzzy Inference System (ANFIS) algorithm as a baseline and the use of more advanced methods to improve accuracy.

II. Develop an algorithm that improves phishing-detection accuracy by comparing the text, images and frames of a given website with a knowledge model.

III. Train, test, and validate the developed system (machine learning) for real-time phishing detection.

IV. Automate the detection mechanism in real-time and test it offline.

V. Develop a plug-in and implement on a cross-platform operating system.

This section introduces the issue of interest and the significance of this research study. It provides details of the research problem and the research questions to be resolved together with the precise research objectives. It also summarises the existing literature and clarifies the main contributions of this research.

2. Online user decision support system protection against phishing attack using deep learning algorithm

This section contains a review of the literature on the topic under study, namely phishing detection schemes. It also discusses the focus of the research by critiquing the relevant existing research methods and summarising their findings as well as their strengths and weaknesses. It then discusses appropriate provision for the phishing detection problems and how to resolve them.

Big data has enabled machine learning algorithms to discover more fine-grained patterns and to make more accurate and timely predictions than ever before [10]. Deep learning techniques are used for object identification in images, the transcription of voice into text, matching news items and products with user interests and presenting relevant search results [11]. Deep learning architectures are composed of non-linear operations in multiple levels, such as neural networks (NNs) with hidden layers, or of complicated relational methods in reusable approaches [13]. The deep learning concept started with the study of artificial NNs [14], and it has become an active research area in recent years. In a standard neural network (NN), neurons are used to produce real-value activations, and with the adjustment of weights, the scheme behaves as required. Moreover, training the ANN with backpropagation makes it useful with gradient descent algorithms which have played a vital role in the model in the past decades. Although training accuracy is high with back-propagation, when it is applied to testing data, its performance might not be satisfactory [15].

Yi et al. (2018) designed two sets of features for web-phishing interaction features and original content. They also developed a scheme based on a deep belief network (DBN). The test, which included using real IP flows from an Internet service provider (ISP), indicated that the proposed DBN-based model was able to achieve an approximately 90% true positive rate. Also, in the area automotive proposed in [16] in which a deep NN was used to assist the driver in the aspect of traffic light classification, the techniques were used to develop a system to assist in driving. Currently, machine learning is continuously demonstrating its effectiveness in an extensive range of applications. The most common form of machine learning, whether deep or not, is supervised learning [12]. Also, Le et al. (2018) proposed a solution called URLNet, which is an end-to-end deep-learning framework for learning non-linear malicious URLs by detecting it from the URL. They applied a CNN to both the words and characters of the URL features to learn the URL embedding in a jointly optimised framework. This approach allowed their model to capture several types of semantic data, which would not have been possible using existing schemes. They also presented advanced word-embeddings to solve the problem of too many rare words being observed in a classification task [17]. They conducted their experiments on a large-scale dataset and demonstrated that their proposed method gave a strong performance that was better than that of an existing method. The approach has two branches; the first branch has a character-level CNN where character-level embedding is used to represent the URL. The second branch contains a word-level CNN where word-level embedding is used to represent the URL. Thus, word-embedding itself is a mixture of character-level embedding and individual word-embedding. Their approach works in such a manner that it does not require any expertise.

Below are some of the advantages of deep learning algorithms [15]:

Unsupervised Learning: It has robustness by getting most of its connecting structure in other to observe data, which is crucial in other to limit an enormous number of tasks and if the upcoming tasks are not known on time.

1. **Unlabelled Data**: It can learn from mostly from unlabelled data. This means that it can work in a semi-supervised situation, where not all the dataset has comprehensive and correct semantic tags.

2. **Develop Interactions**: It can exploit interaction that are existing across a vast number of tasks. These interactions exist because all that the algorithm task offer is a diverse view of the same underlying reality.

3. **Multifaceted Learning**: It can learn from complex with highly varying function with several disparities much higher than the number of training instances.

4. **Huge Dataset**: It can learn from a massive dataset of features and can compute the training data in a short period with several linear examples.

However, there are some challenges associated with deep learning algorithms regarding the issue of the data used [18], as follows:

1. **Unbalanced data**: This is an issue that occurs in learning and mostly happens during classification if there are more features of some class than others. This issue can be resolved by using some techniques that focus on the data level or the classifier level.

2. **Inadequate data for learning**: This is an issue that occurs when a limited amount of data is available for cross-validation methods which are mostly applied by dividing the available data into two sets, one for learning and the other for validation, in order to check the behaviour of the network. However, to gain a better knowledge of the network, the size and features may be modified for training and evaluating the various aspects of the network.

3. **Overflow of data**: This problem occurs in big data because the generation of data is growing exponentially, and it is forecast that the information contained big data will continue to increase daily.

4. **Partial data**: Sometimes, a collection of data is used for solving a particular task, but the data becomes partial when some of it is lost or because some of its variables or features are unidentified. To resolve this issue, it is necessary to approximate missing values and then discover the relationship between the identified and unidentified data. There some methods based on NNs [15] and some other approaches that can be used to solve the problem.

5. **High measurement:** Information in the real-world application is often over-flowing from the determination of a specific problem point of view which can be handled by the algorithm.

Due to the growth in cyberspace technology, computer users have a significant role to play in making the Internet a safer place for everyone because cyber-attacks are targeted at achieving either financial or social gain [19] to the detriment of the user. On the other hand, some people undertake phishing activities for fun and a sense of accomplishment rather than for financial or social gain, but can also have adverse consequences for the user [1].

Phishing awareness has been improved through the development and use of online game training and email-based training to combat phishing attacks [20]. The use of legislation is a direct measure to reduce phishing by tracking and arresting those who are involved in this criminal activity. The US was the first nation to use laws to combat illegal cyber activities, and many cyber attackers have been arrested and arraigned. The main issue with this approach is the effectiveness of the laws as it is challenging to trace phishing attacks. Fraudulent websites naturally migrate quickly from one server to another. Also, an average phishing website is online for less than 48 hours [21]. Hence phishing attacks are committed very quickly and, subsequently, the criminals who commit these attacks also quickly disappear into cyberspace. The other issue is that many laws are applied only when the damage has been done, and the online user has already been defrauded as a result of phishing attacks. A great deal of background knowledge and experience of phishing and an enormous amount of related information was gained during this development. The use of high-quality datasets in phishing detection classification plays a significant role in building phishing model classifiers [22].

2.1 Long short-term memory (LSTM)

The LSTM algorithm Long short-term memory is based on the recurrent neural network (RNN), which is used to recognise the occurrence of patterns in time series and which also uses error flow in its analysis. However, the LSTM architecture was developed to overcome the shortfalls in RNN, which is a highly non-linear recurrent network with multiple gates and propagative feedback [23]. An LSTM layer contains

a set of recurrently connected blocks, known as memory blocks. These blocks can be a look-alike version of memory chips in a digital system. Hence, each of the blocks includes one or more repeatedly connected memory cells and contains three multiplicative units, namely, the input, forget gate and the output, which provide non-stop analogues of the read, write and reset functions for the block cells [24]. The LSTM network has achieved excellent results in character recognition applications [23]. It has also been used extensively in the analysis of handwriting recognition, speech recognition and polyphonic music modelling, where the results have shown that its usage leads to an improvement in standard detection analysis with variance in the parameter [25]. It has also been used in language modelling to analyse speech in a speech recognition system, where it was found to show an improvement in confusion over the RNN [24].

2.2 Convolutional neural network (CNN)

In recent years, the convolutional neural network (CNN) has seen massive adoption in computer vision applications [26]. In the area of object recognition, CNN has also been used for feature extraction [27]. The CNN belongs to the family of multilayer NNs that are developed for use with two-dimensional data, such as videos and images [28]. CNN is one of the most prominent deep-learning methods where numerous layers are trained using a rigorous methodology.

As mentioned above, CNN has also been shown to be highly effective in computer vision applications [18] and is, therefore, commonly used for that purpose. The CNN contains an input layer, convolution layer, pooling layer, fully connected layer, and output layer. The input layer holds the raw image values; the convolutional layer computes the output of the node that is connected to local regions in the input layer; the pooling layer performs a down-sampling process along the three-dimensional dimensions; the fully connected layer calculates the session scores, and the output layer produces the results. Currently, three main techniques are used in CNN for image classification:

1. Unsupervised pre-training of the CNN with supervised fine-tuning,

2. Transfer learning by fine-tuning the CNN models that have been pre-trained on a natural image dataset and

3. Training the CNN from scratch using available pre-trained features [12].

2.3 Developing the IPDSS anti-phishing tool

This section presents the development of the online plugin model of the IPDSS. The development of the tool was performed based on traditional feature engineering, plus the classification algorithm methodology presented in previous section. Features were created based on the URLs, image features and website elements. The CNN and LSTM classifier were trained using one million URLs and over 10,000 images to build the model. A Toolbar concept was developed using a deep learning (DL) algorithm against legitimate, suspicious and phishing websites. The results showed that a voice-generating user warning interface with a green colour status and a text showing a warning was generated within 25 seconds before the page loaded to give the user a warning.

Due to the advances in technology and the adoption of new techniques, phishers have been able to improve their forged websites so that they now have high similarity with legitimate sites in terms of content. In tests, the current state-of-the-art solutions have been able to obtain 70–98% accuracy (see **Table 1**) in identifying

Status	No. of websites	Accuracy %	TP%	TN %	Average result %
Phishing websites	1000	93.5%	93.8%	6.2%	93.28%
Suspicious websites	100	94.5%	94.8%	5.2%	
Legitimate websites	1500	91.8%	92%	8%	

Table 1.
Test results for IPDSS by toolbar application.

legitimate website. However, these solutions must perform well in the real world, so there needs to be a significant improvement of 0.5% or higher [29]. Moreover, their level of accuracy in identifying suspicious websites should be higher still, and their accuracy in detecting phishing websites should be even higher [30].

The IPDSS scheme extractor algorithm is used to extract the necessary elements from the website's user is visiting. The extracted features were used to compare with knowledge model to determine whether the websites are phishing, suspicious or legitimate. The three modules user warning interface has:

i. A red colour status and voice generation with text directive warn the user if the requested site is a phishing web page,

ii. An amber colour status and voice generation with text directive warn the user if the requested site is a suspicious web page and

iii. A green colour status and voice generation with text directive show the user that the requested site is a legitimate web page.

2.4 Testing the IPDSS anti-phishing toolbar

To evaluate the toolbar concept, it was tested on 2600 websites including legitimate, suspicious and phishing websites. First, it was tested on 1000 phishing websites. The LSTM-CNN algorithm runs in the background as a knowledge module. When a URL is typed into the address bar (**Figure 1**), the algorithm inspects whether the requested website is a phishing link by comparing the current URL

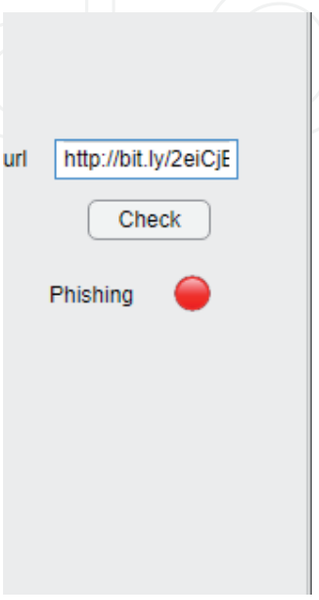

Figure 1.
Application interface for legitimate URL check.

against the stored features in the deep learning classification algorithm. If a match is detected, and it is a phishing site, in order to alert the user a red colour status with a voice-operated user warning interface is activated and a text is generated showing that the status of the URL is "phishing".

The above procedure was repeated up to 1000 times with different URLs, so all the phishing URLs were tested. The performance of the toolbar in each case was observed and recorded, and besides, screenshots were taken to validate the results. An example of a screenshot of a phishing website result is shown in **Figure 1**. This part of the experimental effort was carried out over 8 hours per day for five consecutive days. As regards the time-based assessment of the toolbar's ability to detect a phishing website, the voice-generating user warning interface with a red colour status and a text showing an alert were generated within 25 seconds to warn the user before the page loaded.

The toolbar also evaluated on 100 suspicious URLs. As previously mentioned, the LSTM-CNN algorithm runs in the background as a knowledge module. The same procedure is followed as in the testing of the toolbar on phishing websites that described in the previous section, but in this test, the algorithm checks whether the URL requested is a suspicious website by relating the newly typed URL against the stored features in the IPDDS. If a match is detected, and it looks like the URL is a suspicious website, the user warning interface included in the model shows an amber colour status and, besides, a text description is generated stating that the URL is "suspicious" (**Figure 2**) in order to alert the user to exercise caution. This process was repeated 500 times on all 100 URLs and the performance was observed and recorded (**Table 1**). An example of a screenshot of suspicious website results shown in **Figure 2**. This task required 8 hours per day over two days to perform because the finding shows that there is a little and a reasonable number of suspicious online websites which make this challenging task as they are short-lived. As regards the time-based assessment of the toolbar's performance in identifying a suspicious website, the voice-generating user warning interface with an amber colour status and a text showing a warning were generated within 25 seconds to alert the user before the page loaded.

The IPDSS was also tested on 1500 legitimate URLs. As stated above, the LSTM-CNN algorithm runs in the background as a knowledge module. The same procedure as that used to test the toolbar's performance on phishing and suspicious

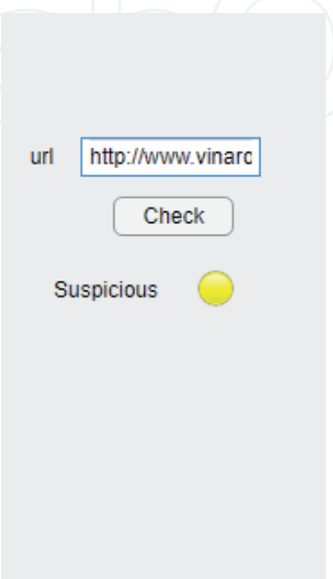

Figure 2.
Application interface for suspicious URL check.

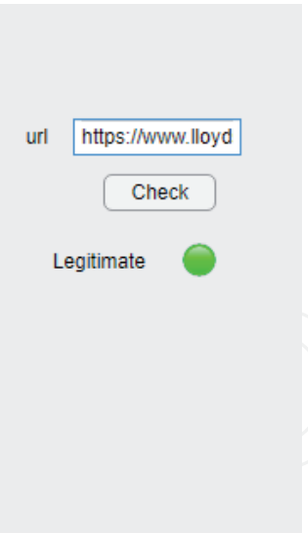

Figure 3.
Application interface for phishing URL check.

websites was used, but in this instance, the algorithm checks whether the URL that has been requested is a legitimate website by relating the newly typed URL in text box against the stored features in the IPDDS. If no match is found, then it is a legitimate website, and the user warning interface displays a green colour status (**Figure 3**). At this point, it is safe for the user to continue in their task with peace of mind that the site to which they are submitting their confidential information is legitimate.

In the experiment, this procedure was repeated 600 times with validation dataset consisting of URLs so that most the URLs were tested to validate the performance of the toolbar and in each case, the result was observed and recorded (**Table 1**). **Figure 3** shows an example of a screenshot of one of the results produced by the toolbar for a legitimate site. As regards the time-based assessment of the toolbar's ability to detect a legitimate website, the voice-generating user warning interface with a green colour status and a text showing the result was generated within 25 seconds before the page loaded.

Overall, the toolbar was able to achieve an average accuracy of 93.28%, as shown in **Table 1**. Then in **Table 1** column 4 roll 2, shows the performance of the phishing detection with 93.8% true positives and in column 5 roll 2, 6.2% true negative this has taken into consideration using 1000 phishing URLs with an accuracy of 93.5% in column 3 roll 2. Also, the toolbar achieved 94.5% accuracy shown on column 3 roll 3, with 94.8% true positives column 4 roll 3 and 5.2% true negative in column 5 roll 3 when tested on 100 suspicious datasets. Meanwhile, when the plugin is tested on 1500 legitimate websites, the phishing detection toolbar achieved 91.8% accuracy column 3 roll 4, was recorded with true positives of 92% column 4 roll 4 and 8% real negative in column 5 roll 4. However, accuracy varies from a minimum of 91% to a maximum of 94%, which caused significant variation in the accuracy results across the testing datasets.

3. Conclusion

This development also explored the efficacy of the deep learning approach, which is part of the set objective to explore relevant algorithm for the detection of phishing, this revealing the advantages and disadvantages of both the convolutional neural network (CNN) and long short-term memory (LSTM) methods. On the one

hand, the LSTM+CNN algorithm was also used to develop an offline approach for phishing detection but had a smaller detection accuracy of 93.28% compared to that of the ANFIS algorithm.

The reduction in the number of features makes this much faster in terms of time-to-prediction. The protection aspect of the solution is implemented via a user warning interface with various colours representing the category of detection. A green colour indicates a legitimate site, whilst an amber colour represents suspicious ones, and a red colour indicates a phishing site. There is also an audible (voice) warning of relevance to a visually impaired person. The protection interface also advises the user on what to do next such as to terminate the process if it discovers that the site is phishing or suspicious.

The development reflects the effectiveness of the hybrid features approach using CNN, and the LSTM deep learning algorithm is an essential driver to the high model performance. This chapter has contributed to the anti-phishing detection research by present the use of a hybrid feature which include image, frame and text. These three sets of input have just been introduced as single hybrid features for the first time. The three elements are used because they represent the whole structure of a website. Although the scheme performed well, parameter tuning influenced the algorithm in a positive way, and it must be pre-specified to solve a given problem. Ultimately online user confidence will increase in performing transactions online.

The main conclusion of applying the IPDSS approach that is in this development achievement an excellent classification accuracy of 93.28% for identifying phishing websites.

Author details

Moruf Akin Adebowale
School of Computing and Information Science, Anglia Ruskin University, Chelmsford, UK

*Address all correspondence to: akin_mama@hotmail.com

References

[1] H. Sharma, E. Meenakshi, and S. K. Bhatia, "A comparative analysis and awareness survey of phishing detection tools," presented at the 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 19-20 May 2017, 2017.

[2] N. A. G. Arachchilage, S. Love, and K. Beznosov, "Phishing threat avoidance behaviour: An empirical investigation," *Computers in Human Behavior,* vol. 60, no. 2016, pp. 185-197, 2016, doi: http://dx.doi.org/10.1016/j.chb.2016.02.065.

[3] S. Purkait, "Phishing counter measures and their effectiveness – literature review," *Information Management & Computer Security,* vol. 20, no. 5, pp. 382-420, 30 September 2018 2012, doi: doi:10.1108/09685221211286548.

[4] A. Upadhyaya, "Design & development of a plug-in for a browser against phishing attacks," *International Journal of Emerging Technology & Advanced Eng.,* vol. 2, no. 3, pp. 105-111, March, 2012 2012.

[5] Hu J et al. Detecting Phishing Websites Based on the Study of the Financial Industry Webserver Logs. presented at the 3rd International Conference on Information Science and Control Engineering (ICISCE), Beijing, China, 8-10 July. 2016;**2016**

[6] A. Y. Daeef, R. B. Ahmad, Y. Yacob, and N. Y. Phing, "Wide scope and fast websites phishing detection using URLs lexical features," in *3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, 11-12 Aug. 2016 2016: IEEE, pp. 410-415, doi: 10.1109/ICED.2016.7804679.

[7] Hong J. The state of phishing attacks. Communications of the ACM. 2012;**55**(1):74-81

[8] Tan CL, Chiew KL, Wong K, Sze SN. PhishWHO: Phishing webpage detection via identity keywords extraction and target domain name finder. Decision Support Systems. 2016;**88**:18-27. DOI: 10.1016/j.dss.2016.05.005

[9] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," *Expert Systems with Applications,* vol. 117, no. 2019, pp. 345-357, 01 March 2019 2019.

[10] L. Zhou, S. Pan, J. Wang, and A. V. Vasilakos, "Machine learning on big data: Opportunities and challenges," *Neurocomputing,* vol. 237, no. 2017, pp. 350-361, 12 January 2017 2017.

[11] Tyagi I, Shad J, Sharma S, Gaur S, Kaur G. A Novel Machine Learning Approach to Detect Phishing Websites. presented at the 5th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 22-23 Feb. 2018;**2018**

[12] W. Yao, Y. Ding, and X. Li, "Deep Learning for Phishing Detection," in *Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, Melbourne, Australia, 11-13 Dec. 2018 2018: IEEE, pp. 645-650, doi: 10.1109/BDCloud.2018.00099.

[13] G. Montavon, W. Samek, and K.-R. Müller, "Methods for interpreting and understanding deep neural networks," *Digital Signal Processing,* vol. 73, no. 2018, pp. 1-15, 24 October 2017 2018.

[14] Vazhayil A, Vinayakumar R, Soman K. "Comparative Study of the Detection of Malicious URLs Using Shallow and Deep Networks," presented

at the 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bangalore. India. July 2018;**10-12**:2018

[15] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F. E. Alsaadi, "A survey of deep neural network architectures and their applications," *Neurocomputing*, vol. 234, pp. 11-26, 2017/04/19/ 2017, doi: https://doi.org/10.1016/j.neucom.2016.12.038.

[16] CireşAn D, Meier U, Masci J, Schmidhuber J. Multi-column deep neural network for traffic sign classification. Neural Networks. 2012;**32**:333-338, 2012

[17] H. Le, Q. Pham, D. Sahoo, and S. C. Hoi, "URLnet: Learning a URL representation with deep learning for malicious URL detection," presented at the arXiv preprint arXiv:1802.03162, Washington, DC, US, 2 March 2018, 2018.

[18] Y. Guo, Y. Liu, A. Oerlemans, S. Lao, S. Wu, and M. S. Lew, "Deep learning for visual understanding: A review," *Neurocomputing*, vol. 187, no. 2016, pp. 27-48, 26 November 2015 2016.

[19] Arachchilage NAG, Love S. Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior. 2014;**38**:304-312, 2014

[20] Arachchilage NAG, Love S. A game design framework for avoiding phishing attacks. Computers in Human Behavior. 2013;**29**(3):706-714. DOI: 10.1016/j.chb.2012.12.018

[21] A. Oest *et al.*, "Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis," presented at the APWG Symposium on Electronic Crime Research (eCrime), San Diego, CA, USA, 15-17 May 2018, 2018.

[22] Zareapoor M, Seeja K. Feature Extraction or Feature Selection for Text Classification: A Case Study on Phishing Email Detection. International Journal of Information Engineering and Electronic Business. 2015;**7**(2):60-65. DOI: 10.5815/ijieeb.2015.02.08.

[23] T. M. Breuel, A. Ul-Hasan, M. A. Al-Azawi, and F. Shafait, "High-performance OCR for printed English and Fraktur using LSTM networks," in *12th International Conference on Document Analysis and Recognition*, Washington, DC, USA, 25-28 Aug. 2013 2013: IEEE, pp. 683-687.

[24] M. Sundermeyer, R. Schlüter, and H. Ney, "LSTM neural networks for language modeling," in *Thirteenth annual conference of the international speech communication association*, Portland, OR, USA, 9-13 September 2012 2012: ISCA, pp. 194-197.

[25] Greff K, Srivastava RK, Koutník J, Steunebrink BR, Schmidhuber J. LSTM: A search space odyssey. IEEE transactions on neural networks and learning systems. 2017;**28**(10): 2222-2232

[26] Y. Yu, Z. Gong, P. Zhong, and J. Shan, "Unsupervised Representation Learning with Deep Convolutional Neural Network for Remote Sensing Images," in *International Conference on Image and Graphics*, Cham, 2017: Springer, pp. 97-108.

[27] Z. Xu, S. Li, and W. Deng, "Learning temporal features using LSTM-CNN architecture for face anti-spoofing," in 2015 *3rd IAPR Asian Conference on Pattern Recognition (ACPR)*, Kuala Lumpur, Malaysia, 3-6 November 2015 2015: IEEE, pp. 141-145.

[28] Arel I, Rose DC, Karnowski TP. Deep Machine Learning - A New Frontier in Artificial Intelligence Research [Research Frontier]. IEEE Computational Intelligence Magazine. 2010;**5**(4):13-18. DOI: 10.1109/MCI.2010.938364

[29] Shirsat SD. "Demonstrating Different Phishing Attacks Using Fuzzy Logic," presented at the Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore. India. April 2018;**20-21**:2018

[30] (2018). *Phishing attacks: defending your organisation*. [Online] Available: https://www.ncsc.gov.uk/phishing