PHISHING WEBSITE DETECTION USING MULTILAYER PERCEPTRON

Ammar Odeh, Princess Sumaya University for Technology
Ismail Keshta, AlMaarefa University
Ibrahim Abu Alhaol, Princess Sumaya University for Technology
Ahmad Abushakra, Princess Sumaya University for Technology

ABSTRACT

Phishing is a Social Engineering attack technique that is commonly used to obtain user-sensitive information such as login credentials, credit and debit card information, and so on. A phishing website has the same name and appearance as an official website. Also known as a fake website, which is designed to trick a person into stealing their identity. In this paper, we introduce a novel technique for detecting phishing websites on the client-side using a machine learning technique. We use the extraction framework rule in this system paper to extract the features of a website using only the URL. The proposed algorithm uses a dataset contains 30 different URL characteristics that will be used by this same Multilayer Perceptron Classification machine learning model to determine the website's truthfulness. The model is trained using a dataset containing 11,055 tuples. These processes take place on the client-side. The proposed system introduces a high performance on the 70:30 split ratio.

Keywords: Phishing, Multilayer Perceptron, Whaling Phishing, Confusion Matrix

INTRODUCTION

With proper usage of e-commerce, you can contact customers all over the world without any marketplace limits. As a result, the number of clients who use the Internet to make purchases is rapidly expanding (Abdelnabi, Krombholz & Fritz, 2020; Ali & Ahmed, 2019). Every day, hundreds of millions of dollars are exchanged over the internet. This number enticed scammers to carry out their criminal activities. As a result, internet users were vulnerable to a variety of web threats. As a result, the internet's fitness for commercial transactions is questioned (Ali & Malebary, 2020; Alsariera, Elijah & Balogun, 2020; Chiew, Chang & Tiong, 2015).

It is not an easy effort to keep users safe. From there, it's a phishing scheme. The characteristics of the internet must be considered, with a focus on those who are reasonably seasoned users (Hodžić, Kevrić & Karadag, 2016; Jain & Gupta, 2016; Jain & Gupta, 2017). A considerable amount of personal information, money, and other sensitive data and information are lost as a result of cyberattacks. This problem of phishing attachment has been a study topic in recent years(Karabatak & Mustafa, 2018; Pujara & Chaudhari, 2018). When contacting a bogus website, this has become a popular strategy for attackers. If certain websites are examined further, we can be certain that they contain malicious components, especially when looking at Uniform Resource Locators - URLs. The hackers' goals are to obtain as much personal information, confidential information, financial data, identities, usernames, and other information from victims as feasible using URLs (Natadimadja, Abdurohman & Nuha, 2020; Odeh, Keshta & Abdelfattah, 2021).

Citation Information: Odeh, A., Keshta, I., Alhaol, A.I., & Abushakra, A. (2021). Phishing website detection using multilayer perceptron. *Journal of Management Information and Decision Sciences, 24*(S6), 1-12**.**

Types of Phishing Attacks

In this kind of phishing, an offender sends an email with information about a problem, an update, or a sensitive topic that needs to be altered very away. Once the user clicks the email, all of the information submitted by the end-users is forwarded to the offender (Subasi & Kremic, 2020; Subasi, Molah, Almkallawi & Chaudhery, 2017).

As opposed to random program users, attackers target specific individuals or businesses in this attack. It's a more advanced form of phishing that necessitates an in-depth understanding of an institution's power structure. Unlike phishing, this attack sends emails to specific people.

Whaling Phishing

Whaling phishing, or a whaling phishing attack, is what it's called. It's a type of spear phishing in which attackers target high-profile executives, such as the CEO or CFO, to obtain valuable company information (Bhavsar, Kadlak & Sharma, 2018; Rutherford, 2018). These individuals will have complete access to sensitive data because they have senior positions inside the firm. It will be simple to gather additional information (Moul, 2019; Priestman, Anstis, Sebire, Sridharan & Sebire, 2019).

Smishing

Smishing is when a scammer sends a phishing message *via* SMS text message that contains a harmful link (Choudhary & Jain, 2017; Mishra & Soni, 2019). The phishing emails persuade victims to click on a malicious link, which takes them to a fraud page where their personal information is collected (Sonowal & Kuppusamy, 2018).

Voice phishing

Voice phishing is another name for vishing. It's a type of phone scam in which criminals utilize audio messages to gain confidential info or payment from unsuspecting victims (Kim, Hong & Chang, 2021).

Pharming

Pharming is often described as "phishing without the bait." When a user tries to access a website, their computer can either consider a local list of defined host's files or visit a DNS server on the Internet to discover the IP address (Rane, Phansalkar, Shinde & Kazi, 2020). Pharming is typically carried either *via* altering a victim's host's file or exploiting a vulnerability (Arya & Chandrasekaran, 2016; Pan, Wu, Yang & Hwang, 2018).

Infusion of content Phishing replaces the original web site's content with random information and other input fields that look similar to the authentic website so that end-users can trust and give their data readily (Ahmed, Acharjya & Sanyal, 2017).

When phishers construct websites with appealing sounding offerings and get them genuinely indexed by search engines, this is known as Search Engine Phishing. Users come upon these sites when seeking products or services and are duped into handing up their personal information (Tian & Jensen, 2019).

Phishing Detection Model

Blacklisting URLs and IP addresses

A phishing blacklist is a list of phishing URLs that have been flagged as harmful or dangerous by security experts or community members (Vanhoenshoven, Nápoles, Falcon, Vanhoof & Köppen, 2016). PhishTank (Basit, Zafar, Javed & Jalil, 2020) is a free and open-source community with a vast database of websites that may be used as a blacklist. Google also has a Google Safe Browsing API that comes pre-installed with the Google Chrome browser (Kamarudin & Ranaivo-Malançon, 2015).

Machine Learning-Based Techniques

Machine learning-based techniques train a classification algorithm with some features that can tell the difference between a legitimate website and a phishing one. In this case, a website is classified as phishing if its design matches a preset feature set (Brehmer, Kling, Espejo & Cranmer, 2020).

Phishing assaults can be prevented with machine learning based on multidimensional features driven by deep learning. After 12 hours, 47 percent to 83 percent of phishing websites are put on blacklists, and 63 percent of phishing websites have a lifespan of only 2 hours, according to the author. As a result, blacklisting is no longer a viable option (Khanal, Prasad, Alsadoon & Maag, 2020).

Search Engine Based Techniques

SE-based strategies collect identifying elements (e.g., title, copyright, logo, domain name, etc.) from a webpage and utilize a search engine to verify the legitimacy of the webpage. Previous search-based strategies assumed that a valid site would appear toward the top of a search engine's results (Rao & Pais, 2019).

LITERATURE REVIEW

Several research publications have focused on website security; some have altered routing security (Salehi, Boukerche & Darehshoorzadeh, 2016), while others have worked on intrusion detection, intrusion prevention, and smart grid security (Delgado-Gomes, Martins, Lima & Borza, 2015).

The artificial neural network was employed by the authors in (Zhu, Ju, Chen, Liu & Fang, 2020) to detect phishing websites. To determine whether or not the website is phishing, the suggested work employed 17 neurons as input for 17 features, one hidden layer level, and two neurons as output. The data set was divided into two sections: a train set and a test set. The proposed model was 92.48 percent accurate.

PLIFER is a machine learning-based model that was introduced by the authors in (Abdelhamid, Thabtah & Abdel-jaber, 2017). The age of the URL domain is required by this approach. Additionally, ten features are retrieved, and the Random Forests model (RF) is utilized to detect the phishing website. This model was able to identify 96 percent of phishing emails properly. Using labeled data sets, classification algorithms can be used to detect phishing.

Citation Information: Odeh, A., Keshta, I., Alhaol, A.I., & Abushakra, A. (2021). Phishing website detection using multilayer perceptron. *Journal of Management Information and Decision Sciences, 24*(S6), 1-12.

(Chiew, Tan, Wong, Yong & Tiong, 2019) Presents a proposed software collection model Hybrid Set of Features (HEFS) for detecting phishing websites using machine learning methods. The basic feature set is extracted using a cumulative distribution gradient approach. After that, a process known as data perturbation ensemble is used to extract the second set of characteristics. Following that, Random Forests (RF), an ensemble learner, is used to detect phishing websites. According to the findings, HEFS was able to detect phishing traits with a precision of up to 94.6 percent.

The authors of (Al-Sarem et al., 2021) chose the most appropriate components for detecting website phishing and offered two novel machine learning-based selection methods or detection approaches. The AdaBoost classifier and the LightGBM classifier are the two techniques.

These two methods, when combined, produce a hybrid classifier that has been shown to improve the accuracy of single classifiers in detecting web phishing assaults.

The authors' work in (Pandey, Gill, Nadendla & Thaseen, 2018) was focused on reaching a consensus on the conclusion of the attributes utilized to detect phishing on websites. The authors employed the Fuzzy Rough Set (FRS) theory to determine the most significant attributes to identify incursion on web pages using three standard data sets. To detect phishing, the relevant features were fed into three typical classifiers. Fuzzy Rough Set (FRS) feature selection achieved a maximum accuracy of 95% when Random Forest classification was applied. The Fuzzy Rough Set (FRS) uses three sets of data to develop nine universal phishing detection features. The accuracy value was about 93 percent when these adaptable features were employed to measure the accuracy value, which is equivalent to the Fuzzy Rough Set performance with only a little difference of 2 percent.

Three ensemble learning models based on the Forest Penalizing Attributes (Forest PA) algorithm were proposed by the authors of (Adnan & Islam, 2017). The technique used a weight increment and weight assignment strategy to generate highly resourceful decision trees that took advantage of all attributes in a given batch of data. The experiment's findings reveal exceptionally efficient meta-learners with a 96.26 percent accuracy rate.

The feature extraction technique is used by the majority of existing machine learning techniques, and it is highly accurate in phishing detection. According to, more than 200 traits can be retrieved (Khalid, Khalil & Nasreen, 2014). However, a large number of features increases the size of a classifier, which can lead to overfitting issues. Detecting the optimal features, which are directly related to phishing detection, is another issue for standard machine learning algorithms. This research aims to find the optimal features, which are directly related to phishing detection. The "Decision Tree and Optimal Features based Artificial Neural Network" (DTOF-ANN) (Frosst & Hinton, 2017) technique uses ANN to build the classifier. Each feature's importance is weighed before the best features are chosen. As a result, an ideal feature vector for the classifier is created.

Feature extraction can also be used to train classification algorithms. However, characteristics can be manually defined from URLs and HTML content by specialists for various training and judging purposes. In terms of efficiency, deep learning models outperform standard classification algorithms. Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) are the most extensively used deep learning models. When CNN's and LSTM are employed together, however, they produce greater results (Li, Cheng, Wang & Sun, 2020). The CNN model, for example, learns the properties of URLs and sends them to the LSTM model for a final decision or judgment. Other researchers are inspired by this concept to create a model using a combination of deep learning models. Another model is presented by merging CNNs with the Multi-Head Self-Attention (MHSA) approach (Xiao, Zhang, Hu, Jiang & Xia, 2020), which is similar to the CNN-LSTM model. The CNN model learns the features of URLs, while MHSA aims to learn the weights of those attributes. As a result, the judgment accuracy improves and the performance improves.

Preliminaries

This section presents a concise description of the Multilayer Perceptron as well as the used dataset utilized in this study.

Multilayer Perceptron

The MLP is a special case of a feedforward neural network where every layer is a fully connected layer, MLP concept is used in generic form, in loosely form means a feedforward ANN, and more accurately is used for multiple layers of perceptions. MLP consists of sequential layers of function compositions, the raw data enter from the input layer, then it will generate the input for the next layer (hidden layer(s)). The output of the hidden layer will be input for the output layer to apply the final function, each layer consists of a set of nodes or ‘neurons’, the node receives the input from the previous layer by applying an activation function, the activation function is the identity function for linear regression and the logistic or sigmoid function for logistic regression. By expanding the MLP network in depth and width the function flexibility will be increased. In our experiments, we try to increase the depth and width to find out the best network structure to improve the proposed model performance

Dataset

This dataset phishing websites dataset has been collected mainly from PhishTank archive, Miller Smiles archive, and Google search operators consists of 2456 Instances, with 30 attributes. It is a labeled dataset that has two classes, namely, group 1, group -1, (Mohsen & Sadiq, 2019).

The dataset presented important features to a high efficient predicate phishing website by introducing a rule for each feature.

Table 1
FEATURES OF URL

Table 1 shows a set of main and sub-features.

Table 1
FEATURES OF URL

Main features	Sub features
Address Bar based Features	Using the IP Address
	Long URL to Hide the Suspicious Part
	Using URL Shortening Services “TinyURL”
	URL’s having “@” Symbol
	Redirecting using “//”

	Adding Prefix or Suffix Separated by (-) to the Domain
	Sub Domain and Multi-Sub Domains
	HTTP
	Domain Registration Length
	Favicon
	Using Non-Standard Port
	The Existence of "HTTPS" Token in the Domain Part of the URL
Abnormal Based Features	Request URL
	URL of Anchor
	Links in <Meta>, <Script> and <Link> tags
	Server Form Handler (SFH)
	Submitting Information to Email
	Abnormal URL
HTML and JavaScript-based Features	Website Forwarding
	Status Bar Customization
	Disabling Right Click
	Using Pop-up Window
	IFrame Redirection
Domain-based Features	Age of Domain
	DNS Record
	Website Traffic
	PageRank
	Google Index
	Number of Links Pointing to Page
	Statistical-Reports Based Feature

The Proposed System

Figure 1 shows the system process which starts by reading the URL then the hashing table by using the top-level domain of the URL will be used to accelerate the search process if the URL is on the blacklist or not. If the website belongs to a blacklist then the process will end, otherwise, the website will be suspected. If the website is suspected then the system will extract high relevant features to the class attribute and then filter the selected features to increase the proposed system efficiency and minimize the computational power. And then the suspected website can be classified and store at the whitelist data store or backlist data store to make future URL requests smooth and simple.

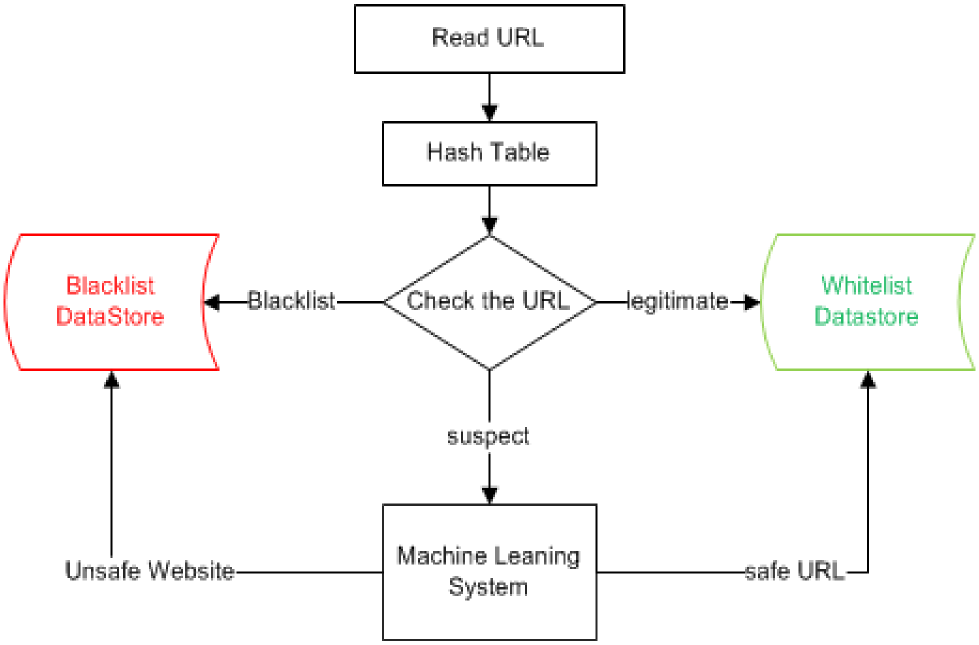

FIGURE 1
URL CLASSIFICATION PROCESS

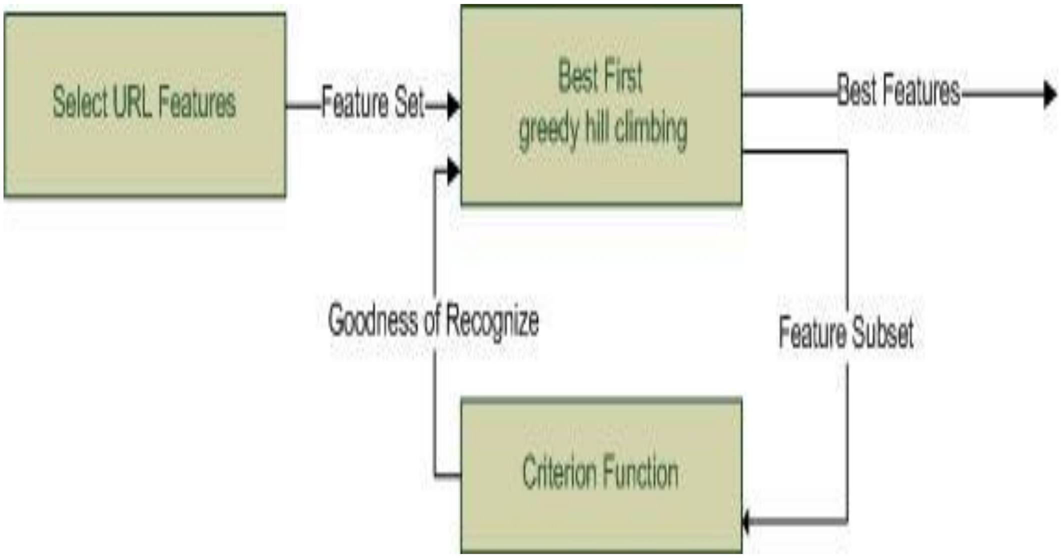

FIGURE 2
FEATURE SELECTION PROCESS

Figure 2 shows the Feature selection procedure by utilizing the best first greedy hill-climbing algorithm to select the best feature and reject all other features in the same categories and try to find out the next feature to improve the efficiency of the proposed model. This greed hill climbing will stop if they are no successor features with better values to the current features. Find out the most related feature to increase the proposed system performance and reduce the machine learning training time.

$$f(x,y) = e^{-(x^2+y^2)} \quad (1)$$

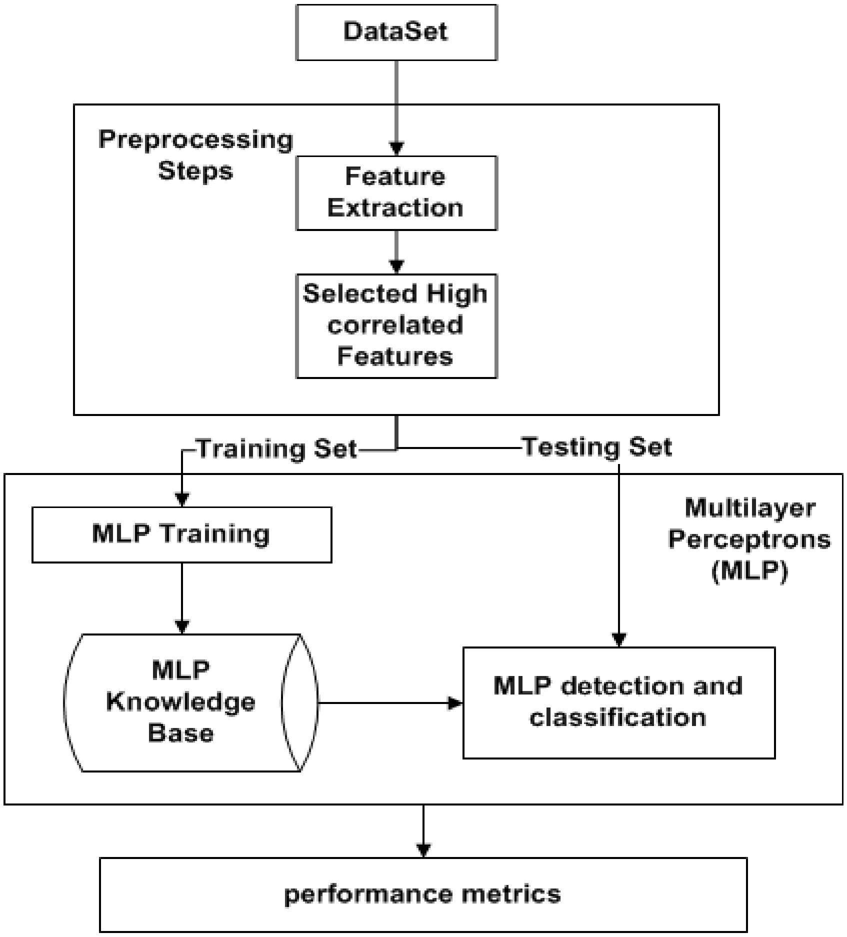

FIGURE 3
PROPOSED SYSTEM BLOCK

Figure 3 shows the proposed system to classify the suspected URL, after reading the URL, the prepossessing stage consists of two sub-stages by extracting the URL features, then the system will select the highly correlated features. The system will split the data into two categories the testing set and the training set then the machine learning knowledge base can generate, then the testing set can be used to evaluate the proposed model. We will evaluate the performance matrix.

The Algorithm consist of the following steps
Step 1: Read URL

```
Step 2: if the link is suspected
Step 3: Preprocessing stage
Step 3.1: Feature extraction
Step 3.2: Selecting the highly correlated feature
Step 4: Split the dataset into two categories (Training set, Testing set)
Step 5: Multilayer Perceptron (MLP)
Step 5.1 a: Apply MLP training (Training set)
Step 5.1 b: Generate MLP Knowledge base
Step 5.2: MLP detection and classification
Step 6: Find the evaluation matrix
End
```

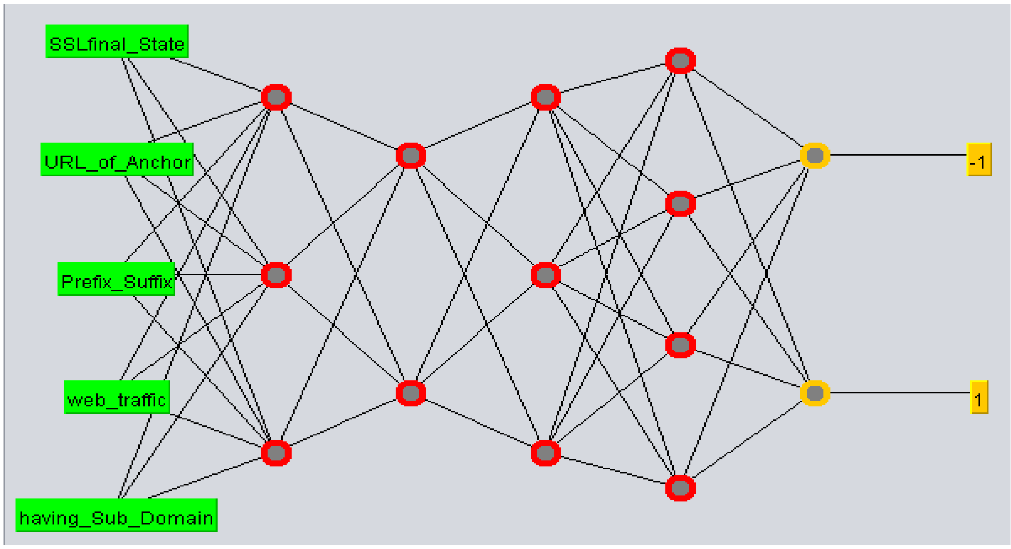

FIGURE 4
MULTI-LAYER PERCEPTION (MLP)

Figure 4 shows the Multi-Layer Perception (MLP) network, which represents the most familiar model in the deep neural network. After extracting and selecting the most correlated features from the dataset and then the input layer of the MLP will read the five high correlated features according to the experiment set shown in the table Experimental parameters.

Table 2
EXPERIMENTAL PARAMETERS

Batch size	**100**
Hidden Layers	2,3,4/2,3,5/2,4,5
Learning Rate	0.3
Momentum	0.2

SIMULATION RESULT

Table 3 shows the confusion matrix used to evaluate the criteria to evaluate the system efficiency. A confusion matrix is a methodology for clarifying a classification algorithm's performance. When you have an unequal number of observations in each class or more than two classes in your dataset, classification accuracy alone can be misleading.

Table 3
CONFUSION MATRIX

	Predicated class	
	Positive	**Negative**
Actual Class	TP	FP
	FN	TN

Table 4 shows the four experiments using different percentages of training data and examination data. The mechanism of the different number of hidden layers was applied to show the highest efficiency. Where the results of efficiency appear high in the ratio of 70:30, where the accuracy has achieved a ratio.

Table 4
SIMULATION RESULTS

Dataset Split ratio	**Hidden Layer**	**Accuracy Score**	**Sensitivity**	**Specificity**
50:50	2,3,4	94.5%	86.7%	92.6%
	2,3, 5	94.7%	86.3%	91.3%
	2,4, 5	95.2%	87.2%	90.1%
60:40	2,3,4	92.1%	87.7%	88.6%
	2,3, 5	93.4%	86.7%	92.6%
	2,4, 5	94.2%	86.7%	92.6%
70:30	2,3,4	97.5%	86.7%	92.6%
	2,3, 5	98.8%	98.5%	97.6%
	2,4, 5	97.9%	87.7%	88.6%
80:20	2,3,4	91.3%	86.7%	92.6%
	2,3, 5	90.5%	86.7%	92.6%
	2,3, 5	92.1%	86.7%	92.6%

CONCLUSION

The phishing threat has emerged as among the most common threats to internet users, organizations, and network operators. Using faked emails or false pages, the attacker(s) acquires the client's confidential data in a phishing assault. Phishing scams, which include multiple hoaxes on the websites, are frequent entrance sites for online social engineering attacks. Phishing websites appear to be genuine, but they are difficult to spot because attackers mimic the form and function of legitimate websites.

This paper presents an intelligent model for efficient phishing detection protocol. It utilizes a Multilayer Perceptron after selecting the highest correlated features from the dataset. A comparative experiment showed in a table based on the number of neurons in the hidden layers and changing the training percentage (50%, 60%, 70%, and 80%).

The proposed approach's performance is evaluated using various evaluation metrics such as specificity, accuracy, and sensitivity. The exploratory experiments demonstrated that the proposed approach outperforms other existing machine learning and neural network classifiers for detecting malicious websites. It is desired that further information gathering will yield more impressive findings. The best performance criteria appeared in 70% of training data with 2, 3, and 5 as a hidden layer.

REFERENCES

Abdelhamid, N., Thabtah, F., & Abdel-jaber, H. (2017). *Phishing detection: A recent intelligent machine learning comparison based on models content and features.* Paper presented at the 2017 IEEE international conference on Intelligence and Security Informatics (ISI).

Abdelnabi, S., Krombholz, K., & Fritz, M. (2020). *Visualphishnet: Zero-day phishing website detection by visual similarity*. Paper presented at the Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security.

Adnan, M.N., & Islam, M.Z. (2017). Forest PA: Constructing a decision forest by penalizing attributes used in previous trees. *Expert Systems with Applications, 89*, 389-403.

Ahmed, N.S.S., Acharjya, D., & Sanyal, S. (2017). A framework for phishing attack identification using rough set and formal concept analysis. *International Journal of Communication Networks and Distributed Systems, 18*(2), 186-212.

Al-Sarem, M., Saeed, F., Al-Mekhlafi, Z.G., Mohammed, B.A., Al-Hadhrami, T., Alshammari, M.T., & Alshammari, T.S. (2021). An optimized stacking ensemble model for phishing websites detection. *Electronics, 10*(11), 1285.

Ali, W., & Ahmed, A.A. (2019). Hybrid intelligent phishing website prediction using deep neural networks with genetic algorithm-based feature selection and weighting. *IET Information Security, 13*(6), 659-669.

Ali, W., & Malebary, S. (2020). Particle swarm optimization-based feature weighting for improving intelligent phishing website detection. *IEEE Access, 8*, 116766-116780.

Alsariera, Y.A., Elijah, A.V., & Balogun, A.O. (2020). Phishing website detection: Forest by penalizing attributes algorithm and its enhanced variations. *Arabian Journal for Science and Engineering, 45*(12), 10459-10470.

Arya, B., & Chandrasekaran, K. (2016). A Client-Side Anti-Pharming (CSAP) approach. *Paper presented at the 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*.

Basit, A., Zafar, M., Javed, A.R., & Jalil, Z. (2020). A novel ensemble machine learning method to detect phishing attack. *Paper presented at the 2020 IEEE 23rd International Multitopic Conference (INMIC)*.

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on phishing attacks. *Int. J. Comput. Appl, 182*, 27-29.

Brehmer, J., Kling, F., Espejo, I., & Cranmer, K. (2020). MadMiner: Machine learning-based inference for particle physics. *Computing and Software for Big Science, 4*(1), 1-25.

Chiew, K.L., Chang, E.H., & Tiong, W.K. (2015). Utilisation of website logo for phishing detection. *Computers & Security, 54*, 16-26.

Chiew, K.L., Tan, C.L., Wong, K., Yong, K.S., & Tiong, W.K. (2019). A new hybrid ensemble feature selection framework for machine learning-based phishing detection system. *Information Sciences, 484*, 153-166.

Choudhary, N., & Jain, A.K. (2017). Comparative analysis of mobile phishing detection and prevention approaches. *Paper presented at the International Conference on Information and Communication Technology for Intelligent Systems.*

Delgado-Gomes, V., Martins, J.F., Lima, C., & Borza, P.N. (2015). Smart grid security issues. *Paper presented at the 2015 9th International Conference on Compatibility and Power Electronics (CPE)*.

Frosst, N., & Hinton, G. (2017). Distilling a neural network into a soft decision tree. *arXiv preprint arXiv:1711.09784*.

Hodžić, A., Kevrić, J., & Karadag, A. (2016). Comparison of machine learning techniques in phishing website classification*. Paper presented at the International Conference on Economic and Social Studies (ICESoS'16)*.

Jain, A.K., & Gupta, B. (2016). Comparative analysis of features based machine learning approaches for phishing detection*. Paper presented at the 2016 3rd international conference on computing for sustainable global development (INDIACom)*.

Jain, A.K., & Gupta, B.B. (2017). Phishing detection: Analysis of visual similarity based approaches. *Security and Communication Networks, 2017*.

Kamarudin, A.N.A., & Ranaivo-Malançon, B. (2015). Simple internet filtering access for kids using naïve Bayes and blacklisted URLs. *Paper presented at the International Knowledge Conference*.

Karabatak, M., & Mustafa, T. (2018). *Performance comparison of classifiers on reduced phishing website dataset. Paper presented at the 2018 6th International Symposium on Digital Forensic and Security (ISDFS).*

Khalid, S., Khalil, T., & Nasreen, S. (2014). A survey of feature selection and feature extraction techniques in machine learning*. Paper presented at the 2014 science and information conference*.

Khanal, S.S., Prasad, P., Alsadoon, A., & Maag, A. (2020). A systematic review: Machine learning based recommendation systems for e-learning. *Education and Information Technologies, 25*(4), 2635-2664.

Kim, J.-W., Hong, G.-W., & Chang, H. (2021). Voice recognition and document classification-based data analysis for voice phishing detection. *Human-Centric Computing And Information Sciences, 11*.

Li, Q., Cheng, M., Wang, J., & Sun, B. (2020). LSTM based phishing detection for big email data. *IEEE Transactions on Big Data*.

Mishra, S., & Soni, D. (2019). SMS phishing and mitigation approaches. *Paper presented at the 2019 Twelfth International Conference on Contemporary Computing (IC3).*

Mohsen, K.S., & Sadiq, A.T. (2019). Random forest algorithm using accuracy-based ranking. *Journal of Computational and Theoretical Nanoscience, 16*(3), 1039-1045.

Moul, K.A. (2019). Avoid phishing traps. *Paper presented at the Proceedings of the 2019 ACM SIGUCCS Annual Conference*.

Natadimadja, M.R., Abdurohman, M., & Nuha, H.H. (2020). A survey on phishing website detection using hadoop. *Jurnal Informatika Universitas Pamulang, 5*(3), 237-246.

Odeh, A., Keshta, I., & Abdelfattah, E. (2021). Machine learningtechniquesfor detection of website phishing: A review for promises and challenges. *Paper presented at the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*.

Pan, H.-T., Wu, C.-C., Yang, C.-Y., & Hwang, M.-S. (2018). The weaknesses of the virtual password authentication protocol with cookie. *Paper presented at the IOP Conference Series: Materials Science and Engineering*.

Pandey, A., Gill, N., Nadendla, K.S.P., & Thaseen, I.S. (2018). Identification of phishing attack in websites using random forest-svm hybrid model. *Paper presented at the International conference on intelligent systems design and applications.*

Priestman, W., Anstis, T., Sebire, I.G., Sridharan, S., & Sebire, N.J. (2019). Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ health & care informatics, 26*(1).

Pujara, P., & Chaudhari, M. (2018). Phishing website detection using machine learning: A review. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3*(7), 395-399.

Rane, S.S., Phansalkar, K.A., Shinde, M.Y., & Kazi, A. (2020). Avoiding phishing attack on online votig system using visual cryptography. *Paper presented at the 2020 International Conference on Computer Communication and Informatics (ICCCI).*

Rao, R.S., & Pais, A.R. (2019). Jail-Phish: An improved search engine based phishing detection system. *Computers & Security, 83*, 246-267.

Rutherford, R. (2018). The changing face of phishing. *Computer Fraud & Security, 2018*(11), 6-8.

Salehi, M., Boukerche, A., & Darehshoorzadeh, A. (2016). Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks. *Ad Hoc Networks, 50*, 88-101.

Sonowal, G., & Kuppusamy, K. (2018). Smidca: An anti-smishing model with machine learning approach. *The Computer Journal, 61*(8), 1143-1157.

Subasi, A., & Kremic, E. (2020). Comparison of adaboost with multiboosting for phishing website detection. *Procedia Computer Science, 168*, 272-278.

Subasi, A., Molah, E., Almkallawi, F., & Chaudhery, T.J. (2017). Intelligent phishing website detection using random forest classifier. *Paper presented at the 2017 International conference on electrical and computing technologies and applications (ICECTA)*.

Tian, C.A., & Jensen, M.L. (2019). Effects of emotional appeals on phishing susceptibility. *Paper presented at the Proceedings of the 14th Pre-ICIS workshop on information security and privacy*.

Vanhoenshoven, F., Nápoles, G., Falcon, R., Vanhoof, K., & Köppen, M. (2016). Detecting malicious URLs using machine learning techniques. *Paper presented at the 2016 IEEE Symposium Series on Computational Intelligence (SSCI).*

Xiao, X., Zhang, D., Hu, G., Jiang, Y., & Xia, S. (2020). CNN–MHSA: A convolutional neural network and multi-head self-attention combined approach for detecting phishing websites. *Neural Networks, 125*, 303-312.

Zhu, E., Ju, Y., Chen, Z., Liu, F., & Fang, X. (2020). DTOF-ANN: An artificial neural network phishing detection model based on decision tree and optimal features. *Applied Soft Computing, 95*, 106505.

Citation Information: Odeh, A., Keshta, I., Alhaol, A.I., & Abushakra, A. (2021). Phishing website detection using multilayer perceptron. *Journal of Management Information and Decision Sciences, 24*(S6), 1-12**.**