DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5200

ISSN No. 0976-5697

Volume 9, No. 1, January-February 2018

International Journal of Advanced Research in Computer Science

SURVEY REPORT

Available Online at www.ijarcs.info

SURVEY AND ANALYSIS ON PHISHING DETECTION TECHNIQUES

K. Sumathi
Research Scholar,
CMS College of Science and Commerce Chinnavedampatti,
Coimbatore-49, Tamilnadu, India

Dr. Radha Damodaram
Associate Professor,
CMS College of Science and Commerce Chinnavedampatti,
Coimbatore-49, Tamilnadu, India

Abstract: Social networks are one of the emerging popular platforms for users to interact with each other. User privacy protection on social network is more significant because of availability of huge volume of sensitive data in social network platforms. A conventional information stealing technique is phishing attacks still works in their way to cause a lot of privacy violation incidents. Phishing is a technique where attackers attempt to steal personal information of website users by creating websites that mimic as legitimate website. Phishers steals confidential or sensitive information like credit card pin number, password etc for their personal use or for organizational purpose. Phishing websites often direct users to enter personal information at a fake website which look and feel almost identical to the legitimate one. So it is essential to detect phishing websites in social network platforms. There are various techniques and approaches have been proposed for detection of phishing websites. This survey focus to provide an overview of the literature in phishing detection with various techniques implemented in them, their merits and demerits etc. Comparison based on parameters was also done to prove the efficiency of the various proposed techniques of phishing detection. The comparison results show the best phishing detection method among them.

Keywords: Social networks, phishing, phishers, privacy protection, phishing websites

I. INTRODUCTION

Social engineering [1] is an attack vector which fully depends on human interaction and often involves tricking people into breaking normal security procedures. It defined to psychological manipulation of people into getting confidential information of performing actions. The attack is successful because its victims want to trust other people and are indeed helpful.

Social engineering is the art of getting users to compromise information systems. Instead of technical attacks on systems, social engineers targets humans with access to information, manipulating them into divulging confidential information or even carrying out their malicious attacks through persuasion and influence. Technical protection measures are generally ineffective against this kind of attack.

Phishing [2] is a form of social engineering where an attacker mimics electronic communications to lure users to provide their confidential information. Generally such communications are done through emails that trick user to visit fraudulent websites which in turn to collect private information. In spite of phishing threats are on the rise, until now there is no phishing detection technique or system which perfectly can detect or dynamically can adapt to differentiate between legitimate and phishing websites, this refers to the challengeable nature and to the short life cycle of phishing websites. So detection of phishing websites improves the privacy protection in social networks. There are different techniques and approaches for phishing detection are discussed in this paper.

II. RESEARCH METHODOLOGIES

A PhishGen system is described [3] for phishing prevention and detection that depends on content exemplars to train on in order to effectively identify the threats. PhishGen created dynamic e-mail contents by using generative grammars. It is used as test case for anti-phishing research. Moreover, this system is demonstrated which adapt the existing filters to ensure the delivery of e-mails without the need to white list. This process provides an additional level of realism for phishing attacks during penetration testing.

A Bayesian classifier is introduced [4] to classify the spam and legitimate emails. Naïve bayes classifier is widely used classifier as it is statistical classifier called for known Email filtering. It used classification method to identify the spam mails. In order to determine whether a mail is spam or not, naïve bayes classifier used tokens which means words with ham and spam mails to calculate probability. Based on the probability value, the emails are classified as spam mail or normal mails.

An Intelligent Phishing website Detection and Categorization Model (IPDCM) is proposed [5] to detect the phishing websites. Initially, page feature representation method is studied and heterogeneous classifiers was built based on different features such as title, h1-h6, keyword, description, copyright, link text, frame, img, alt and string. In addition to that, an ensemble classification algorithm is proposed which combined all predicted results from heterogeneous classifiers. Then a hierarchical clustering technique is used to automatic categorization of phishing websites. Thus this method effectively detects and categorizes the phishing website.

A novel approach [6] is proposed to solve Man-In-The-Middle (MITM) which is a phisher behave as a MITM between the user and targeted website. MITM over Secure Socket Layer (SSL) is solved by using genuine website Uniform Resource Locator (URL). These attacks were tackled by proposed hashing the user password with the public key of the server's digital certificate. This method used SSL certificate parameters instead of URL parameters using a client side script, say a browser plugin, before submission to the website. SHA-1 hashing algorithm is used for hashing.

A Case-Based Reasoning Phishing Detection System (CBR-PDS) [7] is introduced to detect the phishing websites.

This system is mainly depends on the CBR which act as a core part of phishing detection system. This system is highly adaptive and dynamic as it can easily detected new phishing attacks. The CBR classifier classified websites with a relatively small dataset but other classifiers required to be trained in advance before classifying the websites. Initially CBR-PDS process checks OPT of current URL and checks whether the OPT is exist or not. If the OPT is present, the proposed CBR-PDS flag it as phishing website otherwise extracts features of that URL and it is formulated a new case to be tested. Then it starts CBR process which retrieves the most similar cases.

A multilayer model called as Phishing Detection using Multi-filter Approach (PhiDMA) [8] is proposed to detect phishing. The main intend of the proposed method is single filter methods is not sufficient to detect various categories of phishing attempts. The proposed PhiDMA model consists of five layers are Auto upgrade whitelist layer, URL features layer, Lexical signature layer, String matching layer and Accessibility Score comparison layer. Each layer acts a filter to detect the phishing websites using a specified dimension. Moreover, accessibility score of web page is incorporated as a phishing indicator. The PhiDMA is attempted by built an accessibility score filter.

A new rule based phishing detection method [9] is proposed for detection of phishing websites. The proposed rule based method consists of two feature sets which are used to find out the identity of web pages. There are four features are used to evaluate the identity of web pages and it also used to determine the access control of page resources elements. The relationship between web page content and URL of a page is determined by using string matching algorithms which is done in the first proposed feature set. The proposed features are independent from third party services. Finally, Support Vector Machine (SVM) is employed to classify the websites based on the feature sets. The extracted rules are embedded into PhishDetector which makes the proposed method is more functional and easy to use.

Multi-label classifier Associative Classification (MCAC) [10] is proposed to detect the phishing websites with high accuracy. The phishing problem is investigated and based on the problems an associative classification data mining method is developed to discover the correlation among features and produces them in simple yet effective rules. The proposed MCAC produce multi label rules from the phishing data generating rules associated with a new class called Suspicious that was not originally in the training data set.

A phishing detection technique called as PhishWHO [11] is proposed to detect the phishing websites based on the difference between actual and target identities of a webpage. PhishWHO comprised of three phases. In the first phase of PhishWHO identity keywords are extracted from the textual contents of the website. For this purpose, a novel weighted URL tokens system based on N-gram model is proposed. Whereas in the second phase of PhishWHO, the target domain name is determined by using search engine and selected the target domain name according to identity-relevant features. In the third phase of PhishWHO, a 3-tier identity matching system is proposed which determine the legitimacy of the query web page.

A system [12] is proposed to identify the phishing websites along with its victimized domain. The proposed system automatically identifies the target domain of every successfully distinguished phishing websites. The feign relationship among the web pages and its associated domains are analyzed through in degree link associations which is used for determination of target domains. In addition, a novel Target Validation (TVD) algorithm is used to verify the correctness of the identified target domain which is also used to reduce the false target prediction of the system.

A multi tier classification model [13] is proposed for phishing email filtering. The proposed method combines multiple classification algorithms to reduce the false positive problems and to reduce the analyzing complexity. This method extracted the features of phishing emails based on weighting of message header and message content. Then based on priority ranking of features, the most discriminative features are selected. Based on the selected features multi-tier classification algorithm classified the emails as legitimate email and phishing email.

A new phishing detection approach [14] is proposed for detection phishing webpages based on kind of semi supervised learning method called as Transductive Support Vector Machine (TSVM). Initially, in this approach features of web pages are extracted which complement the disadvantage of phishing detection based only on document object model (DOM). These features also include color histogram, gray histogram and spatial relationship between sub graphs. By using page analysis method based on DOM objects, the features of sensitive information are examined. The conventional SVM algorithm classified the data by simply train classifier through learning poor and little representative labeled samples whereas the proposed TSVM considered the distribution information implicitly embodied in the large quantity of the unlabeled samples.

A novel approach based on minimum enclosing ball support vector machine (BVM) is proposed [15] to detect phishing websites. The integrity of feature vectors is improved by performing analysis on topology structure of website according to the DOM tree. Then the web crawler is used to extract twelve topological features of the websites are the number of web pages, average number of inbound links, average number of outbound links, average number of internal links, average number of images, average number of CSS files, average number of JS files, average number of forms, average number of input boxes, average number of password boxes, proportion of form links and dynamic webpage proportion. Finally, the feature vectors are detected by using BVM.

An efficacious method [16] is proposed to detect phishing websites through target domain identification. The proposed method is a novel approach which overcomes many difficulties in detecting phishing websites and it also identifies the phishing target that is being mimicked. It is an anti-phishing technique which groups the hyperlinks having direct or indirect association with the suspicious web pages. In order to arrive at a target domain, the domains collected from the directly associated web pages are compared with the web pages which are indirectly associated with suspicious web pages. Then finally, Target Identification (TID) is applied to determine the target domain of the phishing website.

A new solution called as Phishing Alarm [17] is proposed to detect the phishing websites through page component similarity. It utilized features which are hard to evade by attackers. An algorithm is presented which quantify the web pages suspiciousness ratings according to the similarity of visual appearance between web pages. In this proposed solution, Cascading Style Sheet (CSS) is used as the basis to accurately quantify the visual similarity of each page elements. The page elements do not have the same influence to pages so base the proposed rating method on weighted component similarity.

Table I. Comparison based on Approaches

Reference No.	***Approaches used***	***Merits***	***Demerits***	***Performance Measures***
[3]	PhishGen	Highly effective	No guaranteed decrease in click through rates	Z-Score = 2.5344 P-Value = 0.0114
[4]	Bayesian classifier	High accuracy	Content of mails are not considered	Accuracy = 96.46 Precision = 0.95 Recall = 0.87
[5]	Intelligent Phishing website Detection and Categorization Model	Handle 50 pages per second	High computational complexity	Precision = 98.12 Recall = 98.73
[6]	SHA-1	High efficiency	Not experimentally proved	NIL
[7]	Case-Based Reasoning Phishing Detection System	Need not be trained in advance	Failed to implement in integrated web based CBR-PDS system	Accuracy =98.07 F-measure = 0.98 False Positive = 2% False Negative =1.75%
[8]	Phishing Detection using Multi-filter Approach	Can detect all categories of threats	Low accuracy	Accuracy = 92.72% True Positive Rate = 90.54% True Negative Rate = 94.18% False Positive Rate = 5.82% False Negative Rate = 9.46%
[9]	Rule based phishing detection	High accuracy	May not correctly detect and classify the web pages when it content images	True Positive =99.14% True Negative = 97.63% Accuracy =98.65% F-measure = 0.9901
[10]	Multi-label classifier Associative Classification	Enhance classifier predictive performance	Performance based on the generated rules	Accuracy =97.5%
[11]	PhishWHO	Highly effective	Extract insufficient keywords while phishers using visual cloning strategy	Accuracy = 96.10% True Positive Rate = 99.68% False Positive Rate = 7.48% True Negative Rate = 92.52% False Negative Rate = 0.32%
[12]	Target Validation	High accuracy	Threshold value affect the performance	Accuracy = 99.54% True Positive Rate = 99.53% False Positive Rate = 0.45%
[13]	Multi-tier classification	Reduces false positive problems substantially with lower complexity	Considered only static features which may affect the classification performance	Accuracy = 95%
[14]	Transductive Support Vector Machine	More flexible	Low Recall	Accuracy = 95.5% Precision = 96.4% Recall = 90.7%
[15]	Ball support Vector Machine	High precision of detecting	Complex to choose kernel function	True Positive Rate = 0.964 False Positive Rate =0.037 Precision = 0.996 Recall = 0.964 F-value =0.963
[16]	Target Identification	Doesn't require prior knowledge about the site and the training data	Depending on external information repositories in the web	Accuracy = 99.45% True Positive Rate = 99.8% False Positive Rate = 0.9%
[17]	Phishing Alarm	Highly effective	CSS works differently on different browsers	Recall = 97.92% F1-measure = 0.990 Precision = 100%

In Table I, there are different approaches for phishing detection are analyzed based on their merits, demerits and performance metrics like accuracy, precision, recall, f-measure, true positive rate, true negative rate, false positive rate, false negative rate, Z- score and P value. From the above table it is known that the target validation method [12] has high accuracy of 99.54% than the other methods. Then phishing alarm [17] has high precision value of 100% than the other methods, Intelligent Phishing website Detection and Categorization Model [5] method has high recall value of 98.72% than the other methods, Target Identification [16] has high true positive rate of 99.8% than the other methods, Rule based phishing detection [9] has high true negative rate of 97.63% than the other methods, Ball support Vector Machine [15] method has low false positive rate of 0.037 than the other methods and PhishWHO [11] has low false negative rate of 0.32 than the other methods.

III. PERFORMANCE ANALYSIS

In this section, the various methods for phishing detection are analyzed in terms of accuracy, precision, recall, true positive rate, true negative rate, false positive rate and false negative rate.

A. Accuracy

Accuracy is described as the closeness of a measurement to the true value. It is given as

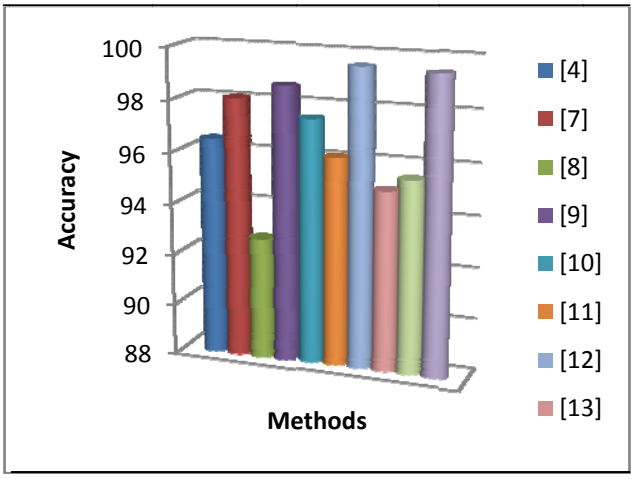

Figure 1. Comparison of Accuracy

Fig. 1, shows the comparison of accuracy between methods are Bayesian classifier [4], Case-Based Reasoning Phishing Detection System [7], Phishing Detection using Multi-filter Approach [8], Rule based phishing detection [9], Multi-label classifier Associative Classification [10], PhishWHO [11], Target Validation [12], Multi-tier classification [13], Transductive Support Vector Machine [14] and Target Identification [16]. From the Fig. 1, it is proved that target validation method [12] has high accuracy than the other methods.

B. Precision

Precision is the closeness of agreement among the set of analysis results obtained.

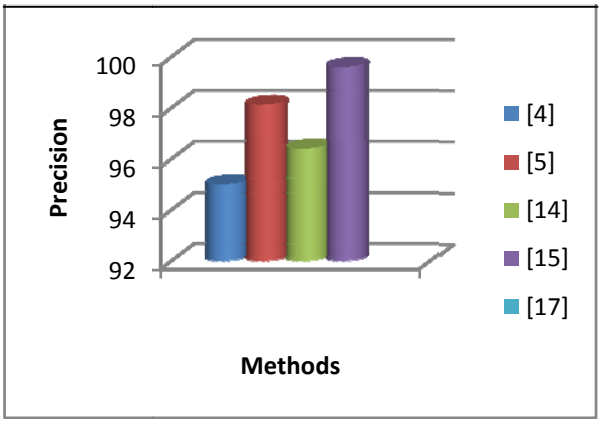

Figure 2. Comparison of Precision

Fig. 2, shows the comparison of precision between methods Bayesian classifier [4], Intelligent Phishing website Detection and Categorization Model [5], Transductive Support Vector Machine [14], Ball support Vector Machine [15] and Phishing Alarm [17]. From Fig. 2, it is known that the Phishing Alarm [17] has high precision than the other methods.

C. Recall

Recall is described as the fraction of relevant results from the retrieved set of analysis results.

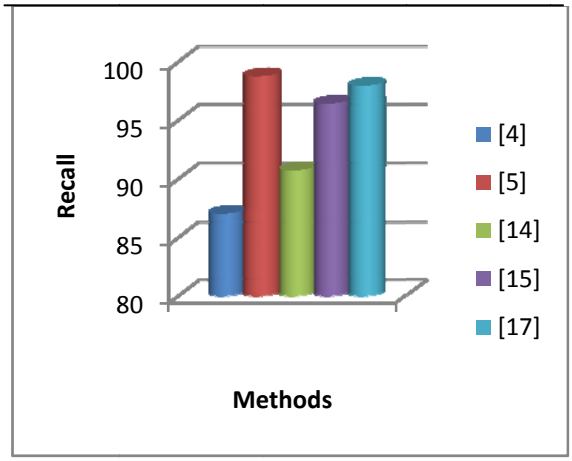

Figure 3. Comparison of Recall

Fig. 3, shows the comparison of recall between methods Bayesian classifier [4], Intelligent Phishing website Detection and Categorization Model [5], Transductive Support Vector Machine [14], Ball support Vector Machine [15] and Phishing Alarm [17]. From Fig. 3, it is known that the Intelligent Phishing website Detection and Categorization Model [5] method has high recall value than the other methods.

D. True Positive Rate

True Positive Rate is computed by using following equation:

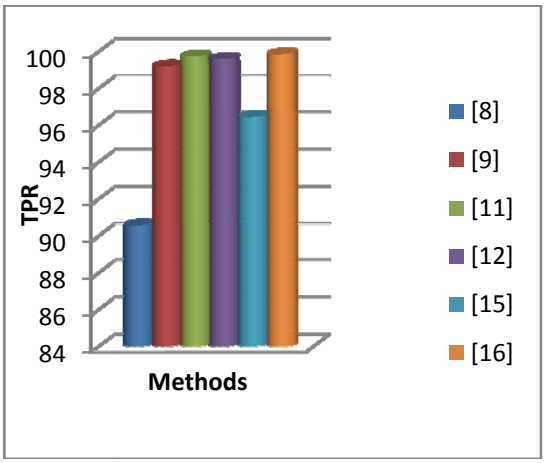

Figure 4. Comparison of True Positive Rate

Fig. 4, shows the comparison of TPR between methods Phishing Detection using Multi-filter Approach [8], Rule based phishing detection [9], PhishWHO [11], Target Validation [12], Ball support Vector Machine [15] and Target Identification [16]. From Fig. 4, it is known that the Target Identification [16] has high TPR than the other methods.

E. True Negative Rate

True Negative Rate (TNR) is calculated by using following equation

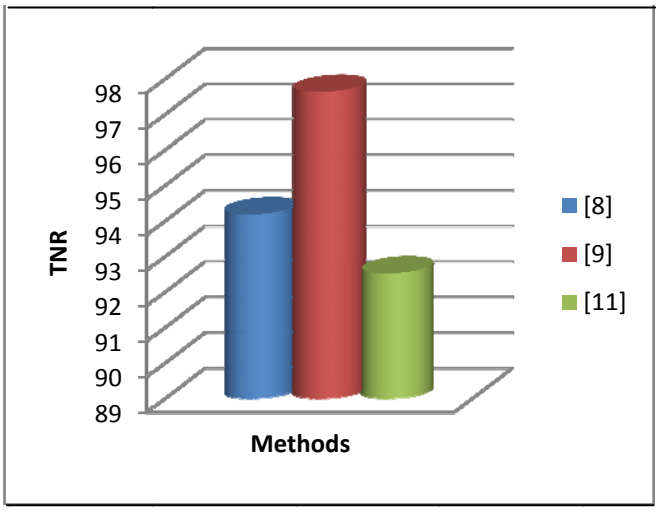

Figure 5. Comparison of True Negative Rate

Fig. 5, shows the comparison of TNR between methods Phishing Detection using Multi-filter Approach [8], Rule based phishing detection [9], and PhishWHO [11]. From Fig. 5, it is known that the Rule based phishing detection [9] has high true negative rate method than the other methods.

F. False Positive Rate

False Positive Rate (FPR) is calculated by using following equation

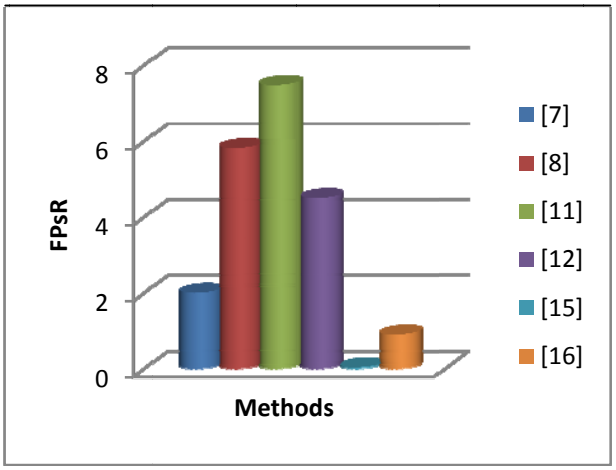

Figure 6. Comparison of False Positive Rate

Fig. 6, shows the comparison of FPR between methods Case-Based Reasoning Phishing Detection System [7], Phishing Detection using Multi-filter Approach [8], SPhishWHO [11], Target Validation [12], Ball support Vector Machine [15] and Target Identification [16]. From Fig. 6, it is known that the Ball support Vector Machine [15] has betters FPR than the other methods.

G. False Negative Rate

False Negative Rate (FNR) is calculated by using following equation

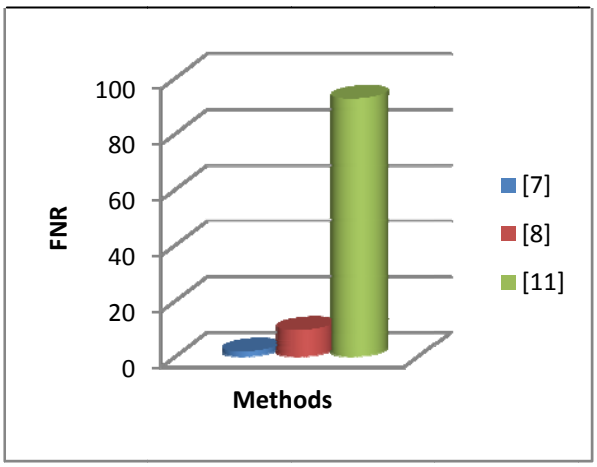

Figure 7. Comparison of False Negative Rate

Fig. 7, shows the comparison of FNR between methods Case-Based Reasoning Phishing Detection System [7], Phishing Detection using Multi-filter Approach [8], and PhishWHO [11]. From Fig. 7, it is known that the Case-Based Reasoning Phishing Detection System [7] has better FNR method than the other methods.

IV. CONCLUSION

Phishing detection and prevention in social network platforms is considered to be the recent ever growing processes that focus on attaining higher values of accuracy. Here this paper provides the recent developments in phishing detection process techniques are analyzed by describing the novel ideas incorporated in them. The analysis of the these schemes provides better understanding of the steps involved in each process thus increasing the scope for finding the efficient techniques to achieve maximum accurate performance. The comparison of the efficient techniques is carried out in terms of accuracy, precision, recall, TPR, TNR, FPR and FNR. This survey also helps in deriving the motivation for our future researches as well.

V. REFERENCES

[1] M. Khonji, Y. Iraqi, and A. Jones, “Phishing detection: a literature survey”, IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2091-2121, 2013, doi: 10.1109/SURV.2013.032213.00009.

[2] R. Basnet, S. Mukkamala, and A. H. Sung, “Detection of Phishing Attacks: A Machine Learning Approach”, Soft Computing Applications in Industry, vol. 226, pp. 373-383, 2008, doi: 10.1007/978-3-540-77465-5_19.

[3] S. Palka, and D. McCoy, “Dynamic phishing content using generative grammars”, Software Testing, Verification and Validation Workshops (ICSTW), 2015 IEEE Eighth International Conference on IEEE, pp. 1-8, 2015, doi:10.1109/ICSTW.2015.7107458.

[4] S. B. Rathod, and T. M. Pattewar, “Content based spam detection in email using Bayesian classifier”, Communications and Signal Processing (ICCSP), 2015 International Conference on IEEE, pp. 1257-1261, 2015, doi:10.1109/ICCSP.2015.7322709.

[5] W. Zhuang, Q. Jiang, and T. Xiong, "An intelligent anti-phishing strategy model for phishing website detection", Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on IEEE, pp. 51-56, 2012, doi: 10.1109/ICDCSW.2012.66.

[6] Y. Joshi, D. Das, and S. Saha, "Mitigating man in the middle attack over secure sockets layer", Internet Multimedia Services Architecture and Applications (IMSAA), 2009 IEEE International Conference on IEEE, pp. 1-5, 2009, doi: 10.1109/IMSAA.2009.5439461.

[7] H. Y. Abutair, and A. Belghith, "Using Case-Based Reasoning for Phishing Detection", Procedia Computer Science, vol. 109, pp. 281-288, 2017, doi: 10.1016/j.procs.2017.05.352.

[8] G. Sonowal, and K. S. Kuppusamy, "PhiDMA–A phishing detection model with multi-filter approach", Journal of King Saud University-Computer and Information Sciences, 2017, doi: 10.1016/j.jksuci.2017.07.005.

[9] M. Moghimi, and A. Y. Varjani, "New rule-based phishing detection method", Expert systems with applications, vol. 53, pp. 231-242, 2016, doi: 10.1016/j.eswa.2016.01.028.

[10] N. Abdelhamid, A. Ayesh, and F. Thabtah, "Phishing detection based associative classification data mining", Expert Systems with Applications, vol. 41, no. 13, pp. 5948-5959, 2014, doi: 10.1016/j.eswa.2014.03.019.

[11] C. L. Tan, K. L. Chiew, and K. Wong, "PhishWHO: Phishing webpage detection via identity keywords extraction and target domain name finder", Decision Support Systems, vol. 88, pp. 18-27, 2016, doi: 10.1016/j.dss.2016.05.005.

[12] G. Ramesh, J. Gupta, and P. G. Gamya, "Identification of phishing webpages and its target domains by analyzing the feign relationship", Journal of Information Security and Applications, vol. 35, pp. 75-84, 2017, doi: 10.1016/j.jisa.2017.06.001.

[13] R. Islam, and J. Abawajy, "A multi-tier phishing detection and filtering approach", Journal of Network and Computer Applications, vol. 36, no. 1, pp. 324-335, 2013, doi: 10.1016/j.jnca.2012.05.009.

[14] Y. Li, R. Xiao, J. Feng, and L. Zhao, "A semi-supervised learning approach for detection of phishing webpages", Optik-International Journal for Light and Electron Optics, vol. 124, no. 23, pp. 6027-6033, 2013, doi: 10.1016/j.ijleo.2013.04.078.

[15] Y. Li, L. Yang, and J. Ding, "A minimum enclosing ball-based support vector machine approach for detection of phishing websites", Optik-International Journal for Light and Electron Optics, vol. 127, no. 1, pp. 345-351, 2016, doi: 10.1016/j.ijleo.2015.10.078.

[16] G. Ramesh, I. Krishnamurthi, and K. S. S. Kumar, "An efficacious method for detecting phishing webpages through target domain identification", Decision Support Systems, vol. 61, pp. 12-22, 2014.

[17] J. Mao, W. Tian, P. Li, T. Wei, and Z. Liang,. "Phishing-Alarm: Robust and Efficient Phishing Detection via Page Component Similarity", IEEE Access, vol. 5, pp. 17020-17030, 2017, doi: 10.1109/ACCESS.2017.2743528.