Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P); 2583-7907 (E)
Vol.12 No.1, 2023, pp.16-20
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2023.12.1.3552

Phishing Attack Detecting System Using DNS and IP Filtering

Md. Sohidul Islam, Md. Sajjad, Mohammad Mahmudul Hasan and Mohammad Sakib Islam Mazumder
Department of Computer Science, American International University-Bangladesh, Bangladesh
E-mail: msohidul@iut-dhaka.edu

(Received 29 March 2023; Revised 6 April 2023; Accepted 17 April 2023; Available 22 April online 2023)

Abstract - **This study examines the different types of phishing attacks, which are a major threat to digital security. Phishing involves the use of fraudulent messages to deceive recipients, including email spoofing, spear phishing, phone phishing, clone phishing, pharming, HTTP phishing, man-in-the-middle attacks, and fast-flux phishing. Attackers can gather information about their targets from public sources such as social media networks, including work history, interests, and activities. The study developed a filtered website that detects fraudulent links based on the internet protocol (IP), register date, and domain name server (DNS) of each website. While further research is needed to improve the effectiveness of the site, this marks an important step towards enhancing digital security.**

Keywords: **HTTPS, IP, DNS, Phishing, Cyber Security**

I. INTRODUCTION

In the mid-90s the first ever idea of phishing attack was initiated. According to the cyber security report, in 2020 year alone over 80% cyber security breach incidents were phishing attacks. Furthermore, with the COVID-19 pandemic situations when all the operations have shifted to electronic media phishing attacks have significantly outbreak more than ever. Most of these attacks happen via email around 96% of the total attacks [1] [2].

Now-a-days, phishing is the most widely recognized cyber-attack in the digital world. Clients have communicated disappointment with the developing mechanical upheaval, which has fundamentally influenced the present security issues. As of late, episodes of human data spilling have become more normal [3]. In this new period, numerous security frameworks are being created to guarantee that security is given main concern and that anticipation from being hacked by digital lawbreakers is considered. Fundamental anticipation is likewise considered to guarantee network security isn't penetrated. Workers in the network protection field are currently searching for dependable and predictable recognition procedures for phishing sites [3].

Customers confront different security dangers such as cyber offenses due to the widespread use of the internet to execute various activities such as online billing systems, banking transactions, online commerce, password storage, etc. Many cyber-crimes are invisible, such as spam, scam SMS, cyber terrorism, and phishing. Among these cruel assaults, phishing is the most well-known kind of cyber-crime today [4]. According to recent studies, phishing has become one of the most common and most accessible kinds of law-breaking. The frequency of incidents and user vulnerability has increased in recent years, more in tandem with the risk of economic harm [5].

Phishing is an online technique in which dubious methods are used by illegitimate authorities to collect sensitive data. Email phishing, website phishing, spear phishing, spoofing, Tab off his guard, Evil twin phishing, and other phishing assaults will be used [6]. Phishing is also known as a data breach on a website [7]. Phishing is commonly carried out through email spoofing or texting, and it involves tricking the user into entering personal information on a fake website that looks and feels the same. It aims to address the growing number of phishing attacks by raising client awareness and utilizing various anti-phishing tools. Day by day phishing attacks is increasing. Users lost their password, bank account, and credit card details information. URL should be less than 56 characters. If the website URL is not HTTP or HTTPS protocol, then don't sign-up or log in to your account. Fake websites use @ symbol and special characters. Also, Kaggle open-source data set is used for detecting phishing links [8].

Phishing emails are using Email Authentication Protocols, Email Security Warnings, and Machine Learning Techniques for Detecting Malicious Emails. If someone attacks or sends a Phishing link, then a machine learning program and email security warning will be shown on the user interface. Furthermore, OTP platform is used in detecting phishing links [9] [10] [11] [12]. In this paper [13] people are facing phishing attacks. This is a common thing. But they are used for the detection of phishing URL Artificial Neutral networks and Deep Neural Networks. They are using a dataset that contains 37175 phishing and 36400 legitimate web pages to train the system. In this paper [14] they are talking about the e-banking sector, user financial data is being hacked by hackers. Furthermore, author [15] has made lots of techniques and approaches.

The techniques are the Decision tree algorithm, Simhash algorithm, Web logo approach, machine learning algorithm, fuzzy data mining algorithm, TF-IDF information retrieval algorithm. Which Fuzzy data mining algorithm showed 100% accuracy and the Web logo technique showed 98% accuracy. Some are lacking in this paper which is that no technique can give 100% accuracy. There is also a considerable deficit in their information and evidence. In this paper [16] they talk about more protection against email spoofing in general. We need to keep an eye on the user email password to be encrypted. They also use this authentication protocol to obtain the following security qualities. This paper talk about protection against common blockchain phishing attacks [17]. Blockchain projects are the biggest victims of phishing attacks as a result of increasingly high investment. They have come up with some ways to get protection from phishing attacks. They monitor mail servers, employee, customer, and investor databases, watch the activity on corporate and community sites, and design a DNS alternative in this instance. There are a variety of security measures available to combat Spam issues, but they are not yet fully developed [18]. Many Android apps are also available on the Play Store (Spam Blocker App; Mr. Number - Caller ID & Spam Protection, for example). Using a combination of 30 features, the machine-learning algorithm detected with approximately 99 percent accuracy [19]. And Security Network level protection, authentication, client-side tools, server-side filters and classifiers, and user education are all approaches to phishing attacks.

According to the specific analysis, they looked into the use of ANNs for intrusion detection systems and spam filtering for OSNs platforms. [20] Data mining and heuristics, machine learning, and deep learning algorithms are the protection strategies discussed in this paper. Deep learning (DL) for phishing attack detection, Scenario-based phishing attack detection, Machine learning (ML) for phishing attack detection, and Hybrid learning (HL) based phishing attack detection are all discussed in this work. [21] There are lots of available solutions to the users, but we need to introduce more secure ways for the users to detect valid sites. There was no newer approach to the previous work. We want to propose a more contemporary approach to the phishing detection system to see it by using a filtering website. After reviewing and researching a solution, we think it is the optimum solution for this kind of problem.

This research also can help to get access to seamless browsing as well as getting access to secure websites. If there are any potential threats are found like unavailability of the webpage domain in all indexes, then the system can identify them. To implement this website-led model, we will build a prototype model that will demonstrate the actuality of the proposal.

II. METHODOLOGY

We are presented to digital wrongdoing on this computerized time and phishing is the new instrument to break the delicate data from the clients. By utilizing spam connect, programmers can take the important data. This strategy assumes an imperative part in light of the fact that our computerized impressions are relying upon it. Any thinking twice about computerized security can lead to different issues. For that reason, the given web connection ought to be appropriately looked up each time to guarantee vigorous security. Then again, it is feasible to affirm that the framework is working appropriately with next to no expected blunder.

Here we utilize some investigation of a site. In the wellspring of the web checker's (which is being as a web device) code, you will see the characteristic, examination and so on. By utilizing this examination, it assists with making sense of the peculiar way of behaving of an unusual site. Drifting over joins without clicking them will uncover their genuine objective in the status bar of the program. Web examination, for example, bob rate, page per visit rate, and so on. Numerous boundaries are required while investigating a phishing assault. We can gain proficiency with the size of the assault and the ideal interest group in the query items to be made on the mail entryway as per the accompanying boundaries.

1. Sender's address
2. SMTP IP Address (127.0.0.1)
3. @letsdefend.io (domain base)
4. Let's defend (Besides the Gmail account, an attacker may have sent from the Hotmail account)
5. Subject (sender address and SMTP address may be constantly changing)

In the search results, it is important to learn the recipient addresses and time information besides the mail numbers. If harmful e-mails are constantly forwarded to the same users, their e-mail addresses may have leaked in some way and been shared on sites such as Pastebin.

In our model, we use an API based approach. We need to develop more secure mechanisms for people to recognize valid sites. Previous work had no novel approaches. We offer a more modern way of phishing detection by utilizing a filtering website. After studying and investigating it, we believe it is the best answer for this issue. This four-step process was used by the web-based solution.

A. DNS Filtering

Most people know DNS blocking for its content-based filtering. Businesses can choose which websites employees can access during business hours and set permissions by blocking internet users from opening malicious content at the DNS level. By preventing employees from visiting time-consuming websites at leisure, DNS filtering also protects company productivity. Social media, news, illegal content, gambling, adult sites, and other websites all pose a high cyber risk. DNS content filtering works by sticking to a blocklist of websites set up by the administrator at the endpoint device or network level. A DNS resolver has the ability to deny a user's request to access an unapproved website if the domain name or IP address of the website is not recognized.

B. IP Filtering

With IP filtering, you can control what IP traffic can enter and leave your network. It enables the creation of rules that can be used to filter IP packets. The process of deciding which IP packets will be processed and discarded or deleted is known as IP filtering. By filtering packets in accordance with established guidelines, it safeguards the network. With NAT, unregistered private IP addresses can be disguised behind a collection of registered IP addresses. This assists in shielding your internal network from external networks because many private addresses can be represented by a small number of registered addresses. NAT also helps to alleviate the issue of IP address depletion.

C. Valid Website Filtering

Users' web access is controlled by web filtering technology, which controls which websites they can access, the content they can view, and the files they can download. A system, for instance, can control search engines to filter out inappropriate search results, block access to gambling websites, and filter out web pages with illegal content. Web filtering can control employees' online behavior and increase productivity by limiting access to websites that are not relevant to their jobs. Additionally, it serves as the initial line of defense against web threats, preventing users from downloading malicious files or accessing harmful websites. For businesses and organizations, the most common web access control measure is web filtering.

D. Spam Website Detecting

Spam fighting is a way to filter emails. This indicates that it makes use of a technology that is comparable to the one that enables you to automatically organize your email into folders. For instance, you can ask your computer to store all e-mails coming from, say, your favorite social networking site, in a folder called "social networks" by creating a filter in your email software (even if you use online email software). Anti-spam software uses algorithms and calculations to try to distinguish genuine messages from spam messages. This allows the software to either move spam messages to a special "junk mail folder" or simply delete them, depending on the instructions given by the user or server administrator.

However, the anti-spam filtering process is not entirely automated. It also trusts the user. A "white-list" is a list of email addresses that will always be allowed to send you messages and a "black-list" is a list of email addresses that will always be blocked. Both lists can be made by any user. In addition, every time you mark an incoming message as spam or not as spam, your computer looks at the characteristics of the message and "learns" (literally) from them for use in the future. This is done to help spam filters find your account more accurately.

E. Smart Safety Alert

An SSL certificate is a type of digital certificate that enables an encrypted connection and provides website authentication. SSLs, which stand for Secure Sockets Layer, inform users of the internet that a connection is safe and secure. A padlock icon on the left side of the URL address bar indicates that a connection is secure when a website has an SSL certificate. Sites will also display an "HTTPS" address rather than an "HTTP" address.

You may believe that your website has been hacked if you see the message "Not Secure" before your domain name. When this occurs, the browser blocks the page and displays a smart safety alert warning message.

It's undeniably true that emails made out of plain text are exhausting. Thus, mail applications give HTML support, permitting the production of sends that can draw in additional consideration from clients. Of course, this element has a drawback. Aggressors can make messages with HTML, concealing URL tends to that are destructive behind buttons/messages that appear to be innocuous.

Assuming the aggressor look through the space address on the web instrument without containing unsafe substance on it, that address will seem innocuous on our web apparatus, and assuming it slips by everyone's notice, you might be confused with this location to be innocuous. The web apparatus will give the examination result.

III. RESULTS AND ANALYSIS

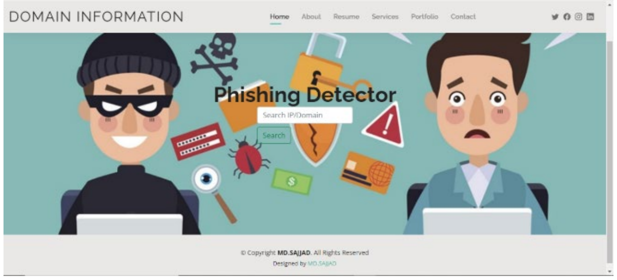


Fig. 1 Index page

In figure 1 above we can see the Front Page of the web tool where we can search for our desired link. On the Domain Information Checker segment, the desired link will be added. Firstly, here is the demo of the valid website. For instance, facebook.com.

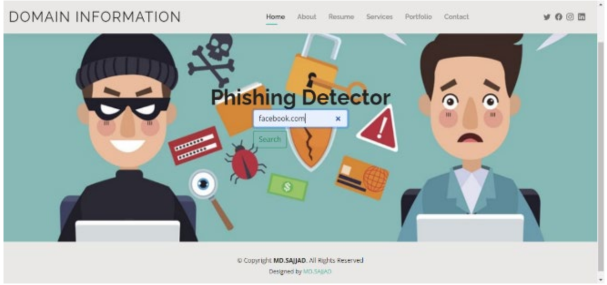
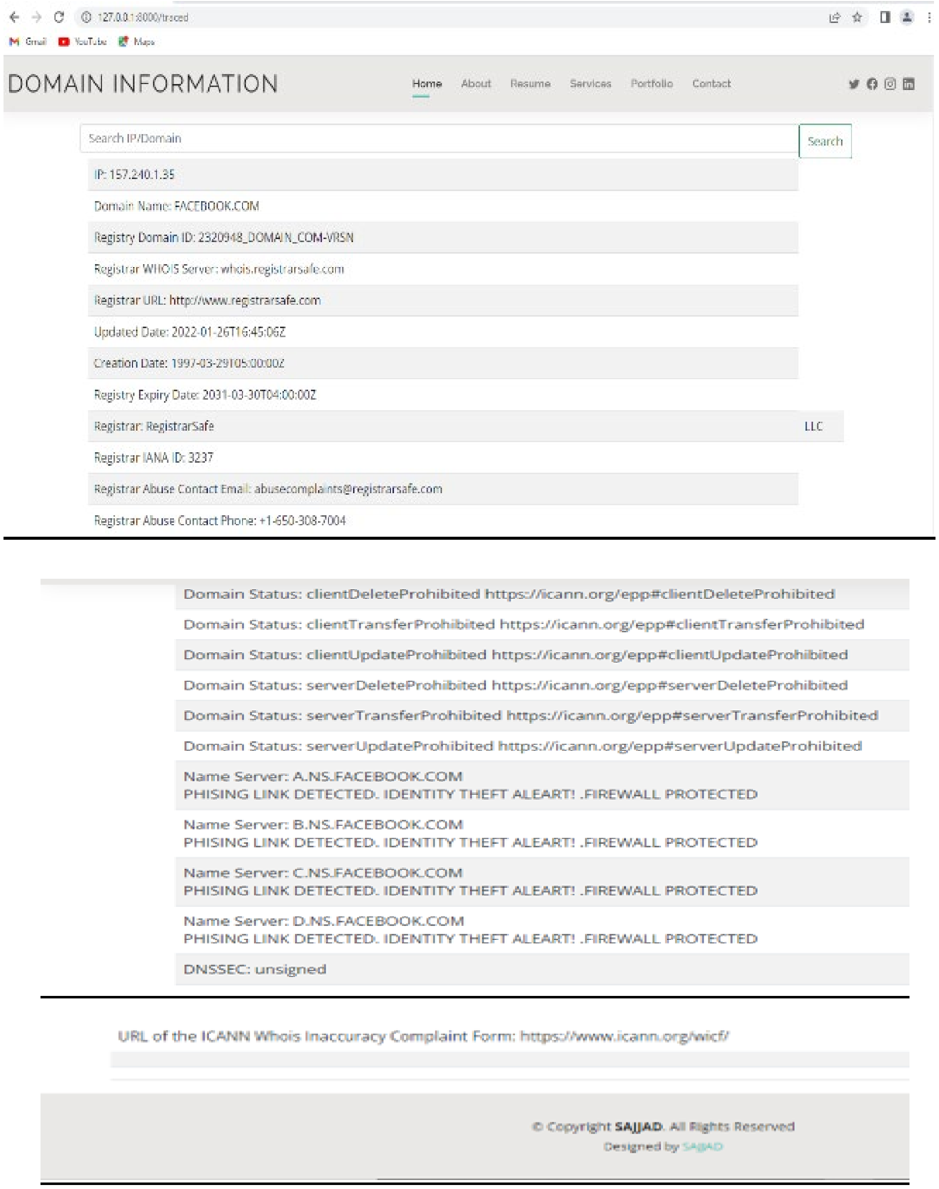


Fig. 2 Valid Link Searching

In figure 2 there is a screenshot of pasted link. On the Domain Information checker segment, we can see the valid link. When it is detected as a valid website, it will show the domain information.



IP: 157.240.1.35

Domain Name: FACEBOOK.COM

Registry Domain ID: 2320948_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.registrarsafe.com

Registrar URL: http://www.registrarsafe.com

Updated Date: 2022-01-26T16:45:06Z

Creation Date: 1997-03-29T05:00:00Z

Registry Expiry Date: 2031-03-30T04:00:00Z

Registrar: RegistrarSafe LLC

Registrar IANA ID: 3237

Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com

Registrar Abuse Contact Phone: +1-650-308-7004

Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited

Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited

Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited

Name Server: A.NS.FACEBOOK.COM
PHISING LINK DETECTED. IDENTITY THEFT ALEART! .FIREWALL PROTECTED

Name Server: B.NS.FACEBOOK.COM
PHISING LINK DETECTED. IDENTITY THEFT ALEART! .FIREWALL PROTECTED

Name Server: C.NS.FACEBOOK.COM
PHISING LINK DETECTED. IDENTITY THEFT ALEART! .FIREWALL PROTECTED

Name Server: D.NS.FACEBOOK.COM
PHISING LINK DETECTED. IDENTITY THEFT ALEART! .FIREWALL PROTECTED

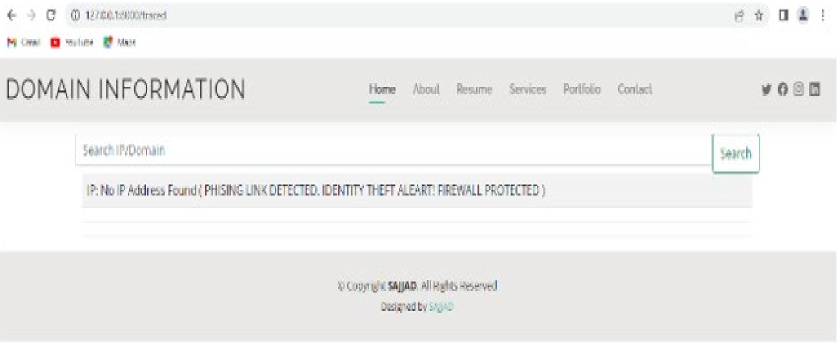
DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

© Copyright SAJJAD. All Rights Reserved
Designed by SAJJAD

Fig. 3 Valid Link Searching Results

Secondly here is the demo of an invalid website. For instance, Facebook.com67f.e33. When it is detected as an invalid website, it will show the domain information. And give a message as an alert like this “IP NOT FOUND OR THEFT ALERT “which mitigates as a successful phishing detection. It means that the given link breaks the requisites of a valid website. Furthermore, it allows the user to set up advanced tracking/generating alerts like tracking, downloads, etc. in just a few clicks.



IP: No IP Address Found (PHISING LINK DETECTED. IDENTITY THEFT ALEART! FIREWALL PROTECTED)

© Copyright SAJJAD. All Rights Reserved
Designed by SAJJAD

Fig. 4 Invalid Link Searching Results

A phishing Attack detecting System is the answer for forestalling abuse of social designing issues. Each modern work should be possible with it. There are a few laggings on the site. As per the overall conversation, the recommended framework has been successfully customized and fabricated, and it has fulfilled the assumptions set out during the venture proposition stage. The framework has been effectively made, and the functionalities have likewise been assembled in view of the experimental outcomes. Our internet-based lives are undependable, and that is the reason, to make it more secure, we really want a detached security framework.

In this project, we use Html, JavaScript, and bootstrap, Laravel, PHP, JSON, and CSS languages. Basically, this is a web-based project, and we use this website for spam link detection. When we get a link, we have to evaluate whether it is valid or not. If it is invalid, then the web tool will easily detect it. And if it is valid, it will show some extra information as well. Such as IP Address, Domain Name, Registry Domain ID, Register URL, Update Date, Creation Date, Registry Expiry Date, Register, Register LANA ID, Register Contact Email, Register Name, Register, Name Server, DNSSEC, and URL of the ICANN Whois Inaccuracy Complaint Form.

In the future, we want to improve this detection system. Currently, we have to paste the link for detection purposes. In the future, we can build an extension tool by using different programming languages. So that it will easily give us the notification in real-time. And in this way, we will try to build mobile-based software. So that people can use this software from different platforms like Android and IOS.

IV. CONCLUSION

This research addresses the growing threat of phishing attacks in our digital lives, and the lack of effective countermeasures to combat this type of cybercrime. Attackers use deceptive techniques to impersonate genuine individuals or organizations, using malicious links or other forms of communication. The study emphasizes the importance of technological security in preventing such attacks. Although the proposed solution may not be foolproof against all types of attacks, the findings suggest that developing a safer infrastructure is feasible. In the future, an upgraded version of this tool could include a pop-up notification feature to alert users of suspicious websites. Ultimately, this web-based solution aims to help users stay vigilant and protected against dangerous attacks in their online activities.

REFERENCES

[1] P. Gillin, The history of phishing [Online]. Available: https://www.verizon.com/business/resources/articles/s/the-history-of-phishing. Accessed on 19 February 2023.

[2] By Gatefy, Updated at March 19, 2021 gatefy.com [Online]. Available: https://gatefy.com/blog/key-points-verizon-data-breach-report-dbir-2020/#:~:text=According%20to%20the%20report% 2C%20social,22%25%20of%20cases%20of%20breaches.&text=In%20cases%20of%20breaches%20involving,Personal%20data.

[3] N. Agrawal and S. Singh, "Origin (dynamic blacklisting) based spammer detection and spam mail filtering approach," *2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC),* Moscow, pp. 99-104, 2016.

[4] J. V. Chandra, N. Challa and S. K. Pasupuleti, "A Practical Approach to E-mail Spam Filters to Protect Data from Advanced Persistent Threat," *2016 International Conference on Circuit, Power and Computing Technologies (1CCPCT),* Nagercoil, pp. 1-5, 2016.

[5] A. K. Sharma and R. Yadav, "Spam Mails Filtering Using Different Classifiers with Feature Selection and Reduction Technique," *2015 Fifth International Conference on Communication Systems and Network Technologies,* Gwalior, pp. 1089-1093, 2015.

[6] J. Thomas, N. S. Raj and P. Vinod, "Towards filtering spam mails using dimensionality reduction methods," *2014 5th International Conference- Confluence the Next Generation Information Technology Summit (Confluence),* Noida, pp. 163-168, 2014.

[7] H. AIRashid, R. AIZahrani and E. EIQawasmeh, "Reverse of e-mail spam filtering algorithms to maintain e-mail deliverability," *2014 Fourth International Conference on Digital Information and Communication Technology and its Applications (DICTAP),* Bangkok, pp. 297-300 2014.

[8] G. R. Kumar, S. Gunasekaran and V. A S, (2018). URL Phishing Data Analysis and Detecting Phishing Attacks using Machine Learning in NLP, *International Journal of Engineering Applied Sciences and Technology (IJEAST),* 70-75.

[9] B. Miller, Proposals for Holistic Security in Preventing Email Phishing Attacks.

[10] A. Ferreira and P. M. V. Marques, "Phishing Through Time: A Ten-Year Story based on Abstracts," *In ICISSP,* pp. 225-232, January 2018.

[11] S. Nasiri, M. T. Sharabian and M. Aajami, "Using combined one-time password for prevention of phishing attacks," *Engineering, Technology & Applied Science Research,* Vol. 7, No. 6, pp. 2328-2333, 2017.

[12] V. Bhavsar, A. Kadlak and S. Sharma, "Study on phishing attacks," *Int. J. Comput. Appl.,* Vol. 182, pp. 27-29, 2018.

[13] O. K. Sahingoz, S. I. Baykal and D. Bulut, "Phishing detection from urls by using neural networks," *Computer Science & Information Technology (CS & IT),* pp. 41-54, 2018.

[14] A. Alsayed and A. Bilgrami, "E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities," *Int. J. Of Emerg. Techn. and Adv. Activ,* Vol. 7, No. 1, pp. 109-115, 2017.

[15] G. J. W. Kathrine, P. M. Praise, A. A. Rose and E. C. Kalaivani, "Variants of phishing attacks and their detection techniques," In *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), IEEE*, pp. 255-259, April 2019.

[16] C. Parulekar, "Minimize phishing attacks: Securing spear attacks," *International Research Journal of Engineering and Technology*, Vol. 6, No. 6, pp. 3054-3058, 2019.

[17] A. A. Andryukhin, "Phishing attacks and preventions in blockchain based projects," *In 2019 International Conference on Engineering Technologies and Computer Science (EnT), IEEE,* pp. 15-19, March 2019.

[18] A. K. Jain, S. K. Yadav and N. Choudhary, "A novel approach to detect spam and smishing SMS using machine learning techniques," *International Journal of E-Services and Mobile Applications (IJESMA)*, Vol. 12, No. 1, pp. 21-38, 2020.

[19] C. Singh, "Phishing Website Detection Based on Machine Learning: A Survey," *In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE,* pp. 398-404, March 2020.

[20] Aldwairi, M., & Tawalbeh, L. A. (2020). Security techniques for intelligent spam sensing and anomaly detection in online social platforms. *International Journal of Electrical and Computer Engineering*, Vol. 10, No. 1, pp. 275.

[21] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommunication Systems*, Vol. 76, No. 1, pp. 139-154, 2021.