iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.60283

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Phishing - A Common Cyber Menace to Combat

Mrs. Pallavi K V[1], Simran Banu H Shirahatti[2], Soniya Devi T[3], Syed Owais Umair[4], Syed Waseem Ahmed[5]
[1]*Assistant Professor,* [2, 3, 4, 5]*Students, CSE Department, AMC Engineering College, Visvesvaraya Technological University*

Abstract: ***Phishing is the most common type of cyber threat existing today. In this paper the aim is to do a quick survey about phishing. Phishing is an attack made to gain unauthorized access to the sensitive information about a person on internet by impersonating the websites they use. This paper also talks about the several means and mechanisms that exists to combat phishing attacks. The intruders mostly use emails, messages, or websites that appear to be from a trusted source to trick the victims into divulging sensitive information. Phished links are to be detected and the users must be protected from it. To assist enterprises in identifying and mitigating phishing risks, a number industry solutions and technologies are available for phishing link detection. Email security gateways, endpoint protection, URL filtering, cyber suites etc. Most common types of phishing include Email phishing, SMS phishing etc. As mentioned above there are quite a few solutions available but most of it is for the Email phishing, SMS phishing still needs some attention. With the emergence of mobile banking in the recent times, SMS phishing has seen a sudden rise. The study looks into how cooperative data sharing systems and threat intelligence feeds might work together. With the help of this cooperative method, the system can swiftly adjust to new phishing attempts and increase the overall accuracy of link detection by drawing on a communal knowledge base. The study of phishing link detection adds to the continuous endeavours to improve cybersecurity. The developed systems aim to offer a strong defence against the constantly changing landscape of phishing threats by integrating advanced technologies, behavioural analysis, and collaborative intelligence. This will ultimately protect individuals and organizations from the potentially disastrous consequences of phishing attacks.***

Keyword: Phishing, Smishing, Vishing, Cyber Threat, URL Filtering.

I. INTRODUCTION

The most prevalent kind of cyberthreat that exists now is phishing. The purpose of this article is to conduct a brief survey on phishing. Phishing is an attempt to obtain sensitive information about an individual online by pretending to be the websites they visit. This paper also discusses the various tools and defence strategies that are available to stop phishing attempts. To fool victims into disclosing critical information, hackers typically utilize emails, texts, or websites that seem to be from a reliable source. Users need to be safeguarded against phishing links and their links need to be identified. There are several industry solutions and technologies available for phishing link detection to help businesses identify and reduce phishing risks, gateways for email security, endpoint defence, URL filtering, cyber suites, etc. Phishing is most frequently done through email or SMS, among other methods. The word “phishing” comes from the analogy of “fishing” in which cybercriminals cast a wide net in an attempt to trick gullible people into falling for their tricks. Artificial intelligence and machine learning algorithms are widely used to improve the phishing detection capabilities, allowing systems to recognize threats that were previously unknown and adapt to changing methods. To differentiate between trust-worthy and dangerous connections, this entails examining a link’s structure, domain reputation, and content, among other aspects. By enabling users to make educated decisions regarding the trustworthiness of links, real-time notifications and insightful feedback create another line of defence against phishing efforts. This introduction lays the groundwork for examining the cutting-edge tools, processes, and cooperative strategies that support continuous endeavours to improve cybersecurity and shield people and businesses from the damaging effects of phishing attacks.

II. LITERATURE SURVEY

1) The study on phishing link detection for preventing the attack using machine learning techniques published on March 2021. Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, Imtiaz Khan and team described in the article that this is mainly driven by human involvement in the phishing cycle. Often phishers exploit human vulnerabilities in addition to favouring technological conditions. It has been identified that age, gender, internet addiction, user stress, and many other attributes affect the susceptibility to phishing between people. In addition to traditional phishing channels, new types of phishing mediums such as voice and SMS phishing are on the increase. Furthermore, the use of social media-based phishing has increased in use in parallel with the growth of social media. Concomitantly, phishing has developed beyond obtaining sensitive information and

financial crimes to cyber terrorism, hacktivism, damaging reputations, espionage, and nation state attacks. Research has been conducted to identify the motivations and techniques and countermeasures to these new crimes, however, there is no single solution for the phishing problem due to the heterogeneous nature of the attack vector. This article has investigated problems presented by phishing and proposed a new anatomy, which describes the complete life cycle of phishing attacks. This anatomy provides a wider outlook for phishing attacks and provides an accurate definition covering end-to-end exclusion and realization of the attack.

2) This study reports the dataset utilized and the algorithms used by the researchers in the previous five years in phishing website detection. A set of 537 research items from five electronic libraries were explored; after applying inclusion–exclusion criteria, the number of articles was reduced to 238. In the third exclusion criterion, it was reduced to 80 studies. A study of these 80 articles was performed by setting up research questions, and this was done to align the study in a direction. With the help of these research questions, this study will help to answer which technique, dataset, and algorithm were highly used in the literature and which algorithm or technique is performing best based on accuracy.

3) The article studied attacks using phishing are still one of the biggest dangers facing people and businesses today. Parallel to the expansion of social media, phishing on social media has become more prevalent. In this project, we used different supervised machine learning techniques to detect phishing attacks. We collected a dataset of phishing URLs from an phish Tank and classified the datasets. As a result, the classification model depicts the websites as legitimate or phishing. The XGBoost Classifier has the highest model performance of 94.2% based on the findings from the above mode. This project may be further improved to include the development of browser extensions or a GUI that analyses a URL to determine whether it is real or phishing. Developing effective anti-phishing tactics that shield users from the attack is a crucial first step in minimizing these attacks, even if ongoing security awareness training is the key to avoiding phishing attempts and lessening their impact.

4) The study attempted to contribute to the scientific discourse related to phishing attacks and security-related issues. The data on phishing attacks among individuals with different educational levels in European countries have been examined. First, results indicate that individuals from more developed countries with higher educational levels are more susceptible to being attacked (RQ1). Second, FCM has been useful for dividing European countries into homogenous groups according to the susceptibility to security attacks (RQ2). Third, countries from clusters with the highest level of phishing attacks also were the most susceptible to actual internet fraud, i.e., credit card and identity theft (RQ3). Fourth, countries from clusters with the highest level of phishing attacks also had, on average, higher GDP per capita (RQ4).

5) The authors worked on the phishing attacks that are a massive challenge for researchers, and they continue to show a rising trend in recent years. Blacklist/whitelist techniques are the traditional way to alleviate such threats. However, these methods fail to detect non-blacklisted phishing websites (i.e., 0-day attacks). As an improvement, machine learning techniques are being used to increase detection efficiency and reduce the misclassification ratio. However, some of them extract features from third-party services, search engines, website traffic, etc., which are complicated and difficult to access. In this paper, we propose a machine learning based approach which can speedily and precisely detect phishing websites using URL and HTML features of the given webpage.

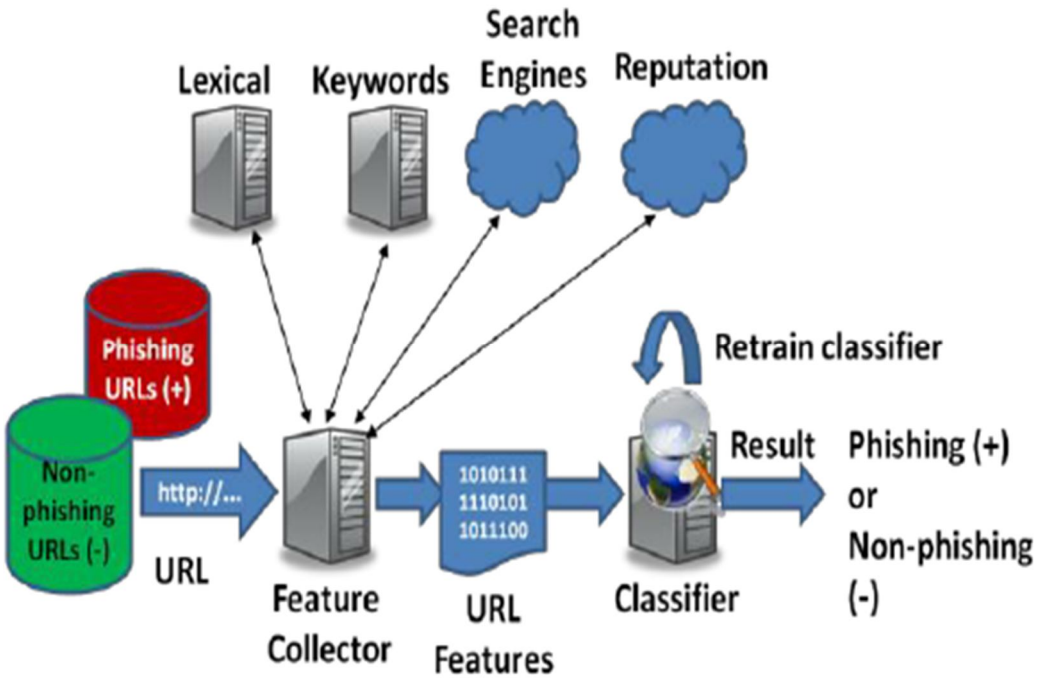
III. METHODOLOGY

The implementation of Domain-based Message Authentication, Reporting, and Conformance (DMARC) is recommended to verify the identity of the sender and lower the possibility of fraudulent emails. By ensuring that emails are really from the claimed sender, DMARC makes it more difficult for attackers to employ phishing tactics.

Encrypting email conversations using secure email protocols, such as STARTTLS, to lower the possibility that hackers would intercept confidential data while it is being sent. Make use of real-time link analysis technologies that have the ability to instantly examine and classify URLs. Put in place web content, filtering tools that are able to prevent users from visiting well-known phishing websites.

These solutions frequently use heuristics to detect suspicious content and rely on databases of dangerous websites that are updated on a regular basis. Keep up with the most recent phishing attacks by working together with threat intelligence sources. It is recommended to regularly update security systems with the most recent threat intelligence in order to improve the detection of novel and developing phishing schemes. Advanced technology, algorithms, and procedures are used in efficient phishing link detection to swiftly and effectively identify rogue URLs. To keep ahead of phishing strategies as they evolve, these mechanisms must be updated and improved on a regular basis.

IV. PROPOSED ARCHITECTURE



V. APPLICATIONS

Cloud service providers can integrate phishing link detection mechanisms into their platforms to identify and block malicious links contained in files stored or shared via their services. This helps protect users' data and prevent the spread of malware within cloud environments. Phishing link detection is essential for online banking and financial services to protect customers from fraudulent websites attempting to steal their login credentials, personal information, or financial data. By detecting and blocking phishing links, these institutions can safeguard their customers' accounts and prevent financial losses. Social media platforms can utilize phishing link detection to identify and remove malicious links shared by users. This helps protect users from falling victim to phishing scams and maintains the integrity of the platform's ecosystem. Web browsers can integrate phishing link detection features to warn users when they attempt to visit a suspicious website. This helps users avoid inadvertently providing sensitive information to attackers and protects them from falling victim to phishing scams. Phishing link detection plays a crucial role in network security by identifying and blocking malicious URLs that may be accessed by users within an organization's network. This helps prevent the spread of malware and the exfiltration of sensitive data.

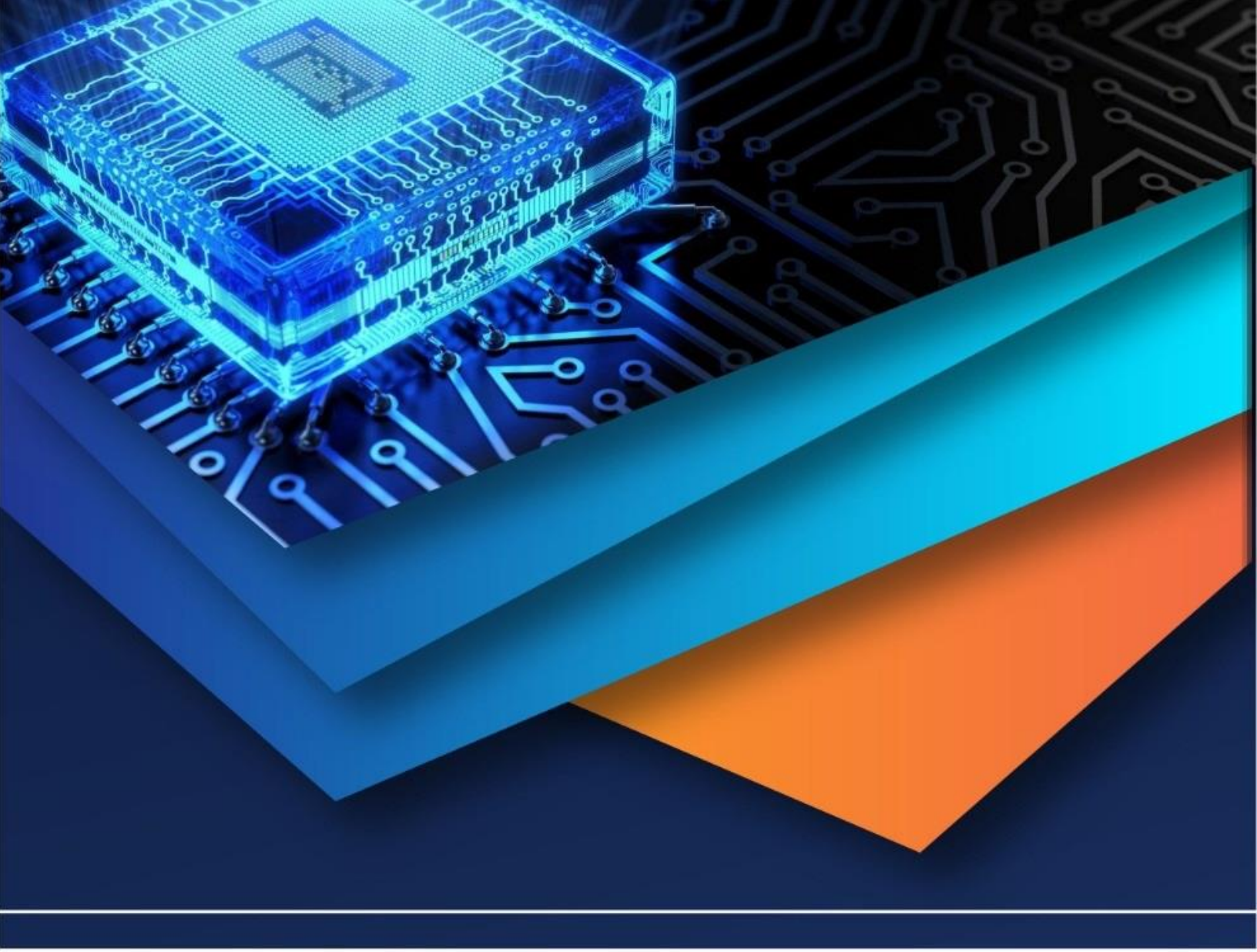
VI. CONCLUSION

Detecting phishing links is crucial in maintaining cybersecurity. Through a combination of technological solutions and user education, organizations and individuals can effectively mitigate the risks associated with phishing attacks. Technological solutions often involve employing algorithms and machine learning models to analyze URLs, email content, and user behaviour to identify suspicious links. However, it's important to complement these measures with ongoing education and awareness campaigns to empower users to recognize and report phishing attempts. By continuously updating detection methods and educating users, we can stay one step ahead of cyber threats and safeguard sensitive information from falling into the wrong hands.

REFERENCES

[1] Zainab, C. Hewage, L. Nawaf, I. Khan, Front. Comput. Sci. 3, 563060 (2021).S. Chanti, T. Chithralekha. “Classification of anti-phishing solutions." SN Comput. Sci 1, 1- 18 (2020).
[2] Asadullah Safi a , Satwinder Singh, “A systematic literature review on phishing website detection techniques” Journal of King Saud University – Computer and Information Sciences 35 (2023) 590–61.

[3] Dinesh P.M, Mukesh M, Navaneethan B, Sabeenian R.S, Paramasivam M.E, and Manjunathan A, "Identification of Phishing Attacks using Machine Learning Algorithm", E3S Web of Conferences 399, 04010 (2023) ICONNECT-2023.
[4] Mirjana Pejić Bacha , Tanja Kamenjarskaa *, Bersilav Žmuka, "Targets of phishing attacks: The bigger fish to fry" International Conference on Industry Sciences and Computer Science Innovation; Procedia Computer Science 204 (2022) 448–455.
[5] Ali Aljofey, Qingshan Jiang, Abdur Rasool, Hui Chen, Wenyin Liu, Qiang Qu, Yang Wang, "Using XGBoost learning curve of logarithms and classisfication of links based on dataset" Int J Mach Learn Cybern. 2019;10(8):2163–75.
[6] Buber, E., Demir, Ö., & Sahingoz, O. K. (2021). "Feature selections for the machine learning based detection of phishing websites". In 2021 international artificial intelligence and data processing symposium (IDAP) (pp. 1-5). IEEE.
[7] S.P. Kumar. "An Emerging Solution for Detection of Phishing Attacks, in Cybersecurity Threats with New Perspectives". Intech Open, (2021).
[8] B. Abdul, M. Zafar, X. Liu, A.R. Javed, Z. Jalil, K. Kifayat. Telecommun. Syst.76, 1 (2021).
[9] Simoiu, C., Zand, A., Thomas, K., & Bursztein, E. (2020, October). "Who is targeted by email-based phishing and malware? Measuring factors that differentiate risk". In Proceedings of the ACM Internet Measurement Conference (pp. 567-576).
[10] Microsoft (2020). "Exploiting a crisis: how cybercriminals behaved during the outbreak". Available at: https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis how-cybercriminals-behaved-during-the-outbreak/ (Accessed August 1, 2020).
[11] A.M. Nazmul, D. Sarma, F.F. Lima, I. Saha, S. Hossain. "Phishing attacks detection using machine learning approach", in third international conference on smart systems and inventive technology (ICSSIT), 1173-1179. (2020).
[12] Jain, A.K., Parashar, S., Katare, P., Sharma, I., 2020." PhishSKaPe: a content based approach to escape phishing attacks". Procedia Computer Sci. 171 (2019), 1102– 1109. https://doi.org/10.1016/j.procs.2020.04.118.
[13] W. Liu, G. Huang, L. Xiaoyue, Z. Min, X. Deng. "Detection of phishing webpages based on visual similarity", In Special interest tracks and posters of the 14th international conference on World Wide Web, 1060-1061. 2020.
[14] P. Josna, K.A.F. Fathima, S. Gayathri, G.E. Elias, A.A. Menon. "A comparative study of machine learning models for the detection of Phishing Websites", in International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS), 1-7, (2022).
[15] Rao, R.S., Pais, A.R., Anand, P., 2020. "A heuristic technique to detect phishing websites using TWSVM classifier. Neural Comput". Appl. 33 (11), 5733–5752. https://doi.org/10.1007/s00521-020-05354-z.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY