WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Enhancement in Web Phishing Security

Keerthivasan.A, Jayaprakash.J, Darwinsdivakar.A, Abishalom. S. P, Dr. Sabapathi. V

Computer Science and Engineering, UG students, Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala College of Engineering, Avadi

ABSTRACT:

Web Phishing Security aims to protect users from falling as victim to phishing attempts by detecting unusual websites in real-time. Phishing is mainly a form of online identity theft. Phishing is one such type of methodologies which are used to acquire the information. Phishing is a cyber crime in which emails, telephone, text messages, personally identifiable informations, banking details, credit card details and passwords are targeted. It is a sort of social designing assault regularly used to take client information, including login accreditations and credit card numbers. With the enhancements in internet technology, websites are the major resource for the cyber- attacks. There are several counter measures available for avoiding phishing attacks, but phishers are changing their attacking methods from time to time. web developers or website owners do not even have enough knowledge about what is happening on their sites. This paper dealt with testing models by comparing the percentage of safe browsing.

Keywords : *social engineering, Pharming, Clickjacking, phishing anatomy, phishing targets, Cyber Crime.*

Introduction :

Phishing attacks have been one of the main cybersecurity threats in recent years. Phishing – messages sending which aims in obtaining personal data of users (passwords, PIN codes, banking details, etc.), redirecting users to fake or malware websites, launching malicious software on the user's computer. Types of phishing - Spear Phishing, Vishing, Smishing. When carrying out phishing attacks, cybercriminals actively use social engineering methods . Social engineering is a technique of psychological manipulation of human actions based on the use of weaknesses and individual characteristics, while information technology is used only to provide contact. Pharming is a technique that redirects users to wrong websites and then steals personal information. Pharming can be done either by changing the hosts file on a target system or by exploitation of a vulnerability in DNS server software. Click-jacking is a method of tricking users in which an attacker can gain access to a user's computer by directing it into a fake harmless web page or by injecting malicious code into a secure page. The reason for this is that the phishers are diverting the users into a fake webserver. Attackers also use secure browser connections for making their illegal activities. The reason for an increase in phishing attacks is not having the correct tools for preventing these attacks. A recent study found that a group of organizations faced targeted phishing attacks in 2019. From which they experienced many types like spear-phishing attacks, voice phishing , social media attacks, SMS/text phishing , and malicious USB drops. The 2018 annual report has stated that phishing attacks increased in 2018 than in 2017, where all phishing types happened more frequently than in 2017. The number of phishing attacks identified in the first and second quarter of 2019 was notably higher than the number recorded in the previous years. While in the first half of 2020, this number was higher than it was in the previous one according to a report from Anti-Phishing Working Group also know as (APWG) which confirms that phishing attacks are on the rise. These findings have shown that phishing attacks have increased continuously in recent years and have become more convenient and have gained more attention by cyber researchers and developers to detect and mitigate their impact. This article aims to determine the severity of the phishing problem by providing information about the phishing phenomenon in terms of phishing definitions, statistics , comparison of techniques and potential countermeasures. The rest of the article is organized as comparative study. Phishing Definitions provides a number of facts as well as some real-world examples of phishing. The evolution and development of phishing attacks are discussed in Developing a Phishing Campaign. What Attributes Make Some People More Susceptible to Phishing Attacks Than Others explores the susceptibility to these attacks. The proposed phishing anatomy and types of phishing attacks are elaborated in Proposed Phishing Anatomy.

Literature Review :

The approach for identifying digital phishing emails using a dynamic expanding neural network that incorporates reinforcement learning. While there are advanced methods available for detecting phishing attacks, there are still limitations in online detection systems that can lead to gaps in web-based transactions. To address this, the researchers have developed a unique framework that combines a neural network with reinforcement learning to identify phishing attacks in online applications. By utilizing reinforcement learning, the proposed model continuously improves over time and adapts to new phishing behaviour that may emerge. Detection of phishing attacks with high accuracy has been an issue of great interest. Recent developments in phishing

detection techniques have led to find various new techniques which specially designed for phishing detection where accuracy is more important. Phishing problem is widely present as there are several ways to carry out such many attack, which implies that one solution is not adequate to address it.

"Relationship between Phishing Techniques and User Personality Model of Bangkok Internet Users" , Chat Chuchuen and Pisit Chanvarasuth. This paper discusses the relationship between user personality types and several phishing techniques. Since personality type is known to have an impact on trust, in this analysis it is posited to also have an impact on effective phishing attempts. This paper tests the relationships between four phishing approaches (link manipulation, filter evasion, website forgery, and spear phishing) and four personality traits (dominance, influence, steadiness, and conscientiousness).

"Study on Phishing Attacks" by Vaishnavi Bhavsar, *et al*., Aims in study of Social Engineering which is being used by the phisher to steal victim's personal data and the account details. This research paper gives a fair idea of phishing attack, the types of phishing attack through which the attacks are performed, detection and prevention towards it.

"Identification of Phishing Attacks using Machine Learning Algorithm" by Dinesh *et al.,* Aims in use the dataset produced to predict phishing websites to build machine learning algorithms and deep neural networks. In order to create a dataset from which the necessary URL- and website content-based attributes may be extracted, both phishing and innocuous URLs of internet sites are collected. Each model's performance level is assessed and contrasted.

"Phishing Attacks: A Recent Comprehensive Study and a New Anatomy" done by Zainab Alkhalil, *et al.,*which initiate proposed technical solutions for detecting and blocking phishing attacks can be divided into two major approaches: non-content based solutions and content-based solutions.

"Phishing website detection using novel machine learning fusion approach" by Lakshmanarao.A *et al.,*Imposed a study on applied various machine learning algorithms logistic regression, decision tree classifier, random forest classifier, AdaBoost, gradient boosting classifier for the phishing detection. dataset from the UCI machine learning repository, applied two priority algorithms PA1, PA2. Based on the results of priority based algorithms final fusion model was decided. With a fusion classifier achieved an accuracy of 97%.

"Phishing Attacks and Protection Against Them" authored by Michael A. Ivanov *et al.,*The article describes the specifics of phishing emails and also Advices on phishing protection by two-factor authentication, including the usage of hardware tokens that generate a unique password for the current session.

"Defences Against web Application Attacks and Detecting Phishing Links Using Machine Learning" proposed by Aya Hashim *et al*.,Developed mitigation techniques for various web application attacks in which each attack considered has one to three mitigation techniques implemented. This project aims to enhance the detection of phishing websites using machine learning technology. It also took into considerations developing the best technique for detection in which a compar ison is made between three machine learning algorithms and deep learning using Long short term memory also detection accuracy was achieved using LSTM.

"Phishing Detection: Analysis of Visual Similarity Based Approaches" , Ankit Kumar Jain and B.B. Gupta.They have presented a survey on phishing detection approaches based on visual similarity. This survey gives a better loop on phishing website, various solution, and future scope in phishing detection. Many approaches are discussed in this paper for phishing detection ,but most of the approaches still have limitations like accuracy, countermeasure against new phishing websites, failing to detect embedded objects, etc. These approaches use various features of a webpage to detect phishing attacks, such as text similarity, font colour, font size, and images appeared in webpage.

Methodology:

Existing System/Methods:

In a group of existing systems we have been studying about the working of each models to improve the efficiency of working to guard against the phishing attacks. In such condition there are a number of concepts which is already in progress to monitor and eliminate the phishing and to make a safe browser for users to work over the internet/websites.

Many number of algorithm have been proposed and tested by cyber security researchers to enhance the systematic approach of the models to eliminate threats caused by phishers. In the previous section about various types of phishing and techniques that is being used by cyber individuals to test and estimate the capacity of systems which can be recovered from phishing attacks by proposing a number of algorithms and percentage of recovery each algorithm obtains in phishing attacks. Let examine models in phishing security by comparing two methods or algorithms.

Support Vector Machine Algorithm:

SVM provides a detection system to prevent the users from phishing as victim. The dataset is created using Phish tank for phishing URLs and non-phishing URLs which have been taken from browser history. Specified features are pulled out from the training dataset and used for sorting the URLs to phishing and non – phishing category. By using SVM classification algorithm, phishing URLs are detected. This method detect phishing URLs, but sometimes when the URL contains a feature which is not available in algorithm features, so system can give probable result. In further the features can be improved to effect the results according to URLs tested to gain proper output. binary classification has been used because we have had two different types of URLs phishing or non-phishing. In this method,

1) Long URL: hide mistrustful parts in the address bar.

2) Dots: A true URL have 5 dots. If a web page contains more than 5 dots it is considered as phishing URL.

3) IP Address: IP addresses can be used instead of Fully Qualified Domain Name (FQDN).

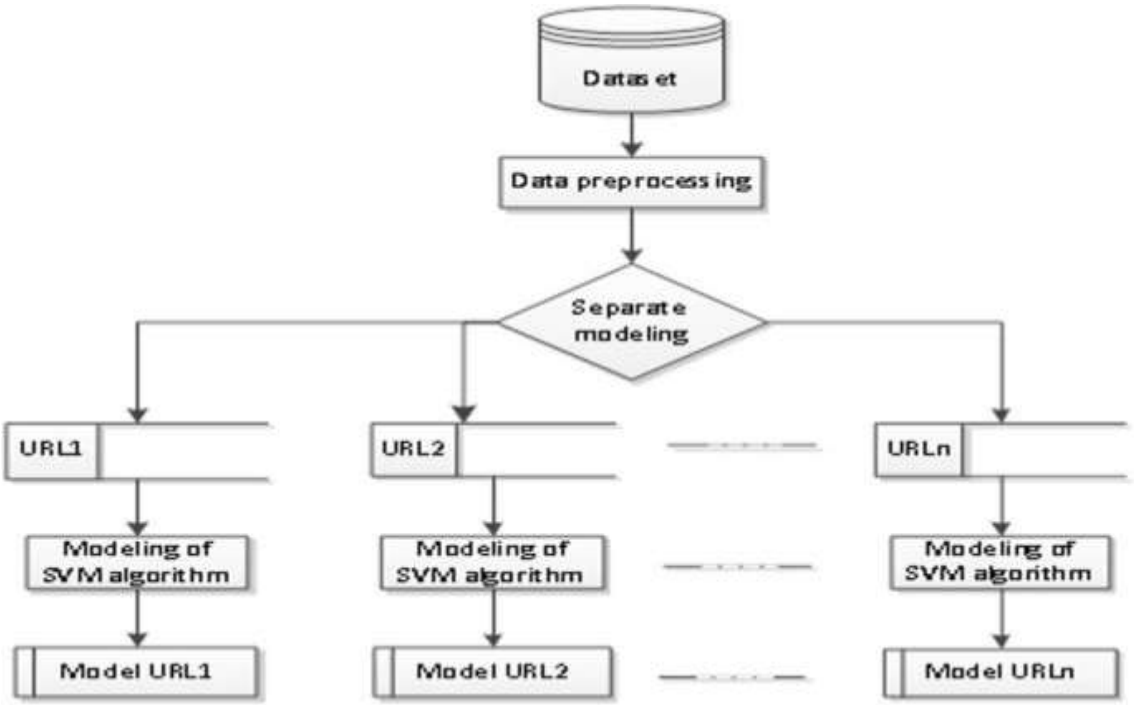
For security reasons true websites do not use this method so if an IP Address exists in a web page link, it is declared as phishing.

4) SSL Connection: web pages that have SSL Connection(HTTPS) can be considered non-phishing.

5) (@) Symbol: Phishers may use @ symbol to give the impression of a true internet address. Using @ symbol in the URL ignores what is there before @. This allows the phishers to write a valid URL before @ to hide the fake URL.

6) Dash (-) symbol: The dash symbol is not commonly used in real URLs. Phishers add dash (-) symbol to misguide the user about the originality of the web page.

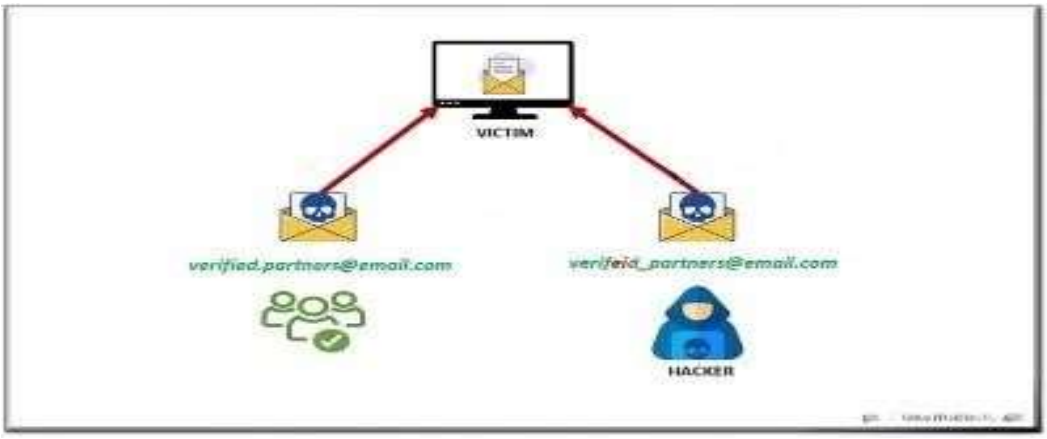
Dia.1



Whaling:

Whaling is one of the types of phishing, in this type of phishing the attacker aims at a rich and benificial status of the victim or user; the attacker takes out all the information of the victim using different medium such as social media accounts and then attacks the victim. The victims of this type of attack are also called as “Whales” or “Big Phish”. whaling is a more sophisticated and personalized approach. In whaling attacks, cybercriminals often conduct extensive research to gather information about their target, including job roles, relationships, and recent activities. They then craft highly convincing and false phishing emails that appear as true and relevant to the targeted individual. These emails may contain seemingly authentic content, such as urgent requests, executive-level communications, or references to recent events, to trap the victim into specific actions, such as clicking malicious links, downloading attachments, or revealing confidential information. The whaling attacks often exploiting the trust and authority of high-profile targets, making them more vulnerable to handle.

Dia.2



Simulation:

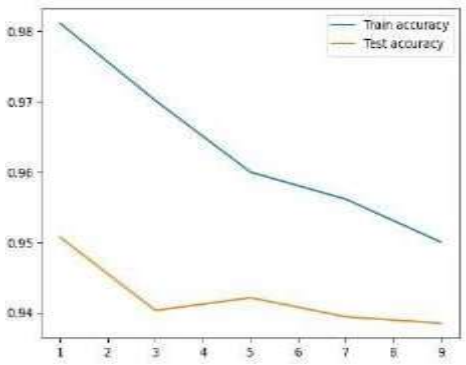
Clearly define the objectives of the phishing simulation. Identify specific testing tools and security controls, or evaluating incident response procedures. Determine the scope of the simulation, number of data set involved and the types of phishing scenarios simulated. Choose specific targets or values within the inputs to simulate phases. Modify to the common communication patterns. Develop authentic-looking phishing emails with compelling content. Use professional language, logo(s), and email signatures. Include elements such as urgency, authority, and social engineering tactics to increase the engagement. Use various attack vectors, including email, social media, or other communication channels relevant to your organization Test different links of fake login pages, malicious attachments, or requests for sensitive information. Consider using specialized phishing simulation tools that automate the process and provide metrics for analysis. Tools like Go-Phish, Social-Engineer Toolkit (SET), or others can assist in creating and tracking phishing campaigns. Monitor participants' responses to the simulated phishing emails. Analyze the data to identify trends, areas for improvement, and successful mitigation strategies. Offer personalized feedback to participants based on responses.

Use the insights gained from the simulation to improve security measures, update policies, and enhance employee training programs. Consider implementing technical solutions, such as advanced email filtering, to strengthen defenses against phishing attacks. Regularly practice phishing simulations helps organizations stay proactive in their cybersecurity efforts and enhances the overall flexibility of the workforce against evolving threats. Through the stages of study about problems faced and solved are from particular kind of threats. we are here to compare support vector machine method and whaling method to show the accuracy of results these methods give by simulating them.

Implementation:

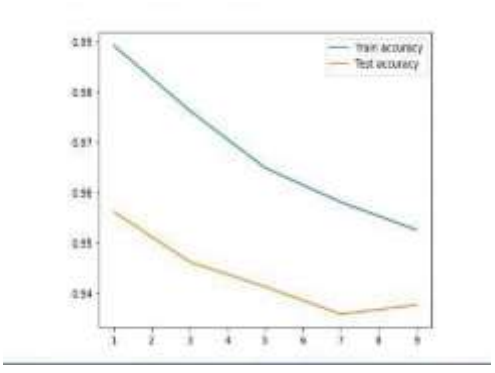
Collect many datasets to perform simulation in which the performance of algorithm can be examined to access it for further enhancement. The specified datasets are loaded in a container to perform algorithmic simulation to generate output sources untill the capacity of algorithm is reached. Now, support vector machine model is said to be implemented to simulator to start the simulation process and so the input is feeded into the system for working . The SVM classifier model generates a amount for result and shows a little effective in percentage of input loaded. Whaling method have a set of data values which is imported to the simulator system to run the input datasets. Here this algorithm takes a long duration of time as compared to SVM classifier model . So, the study for comparison of both models have some limits to work under a sheduled time.

SVM GRAPH



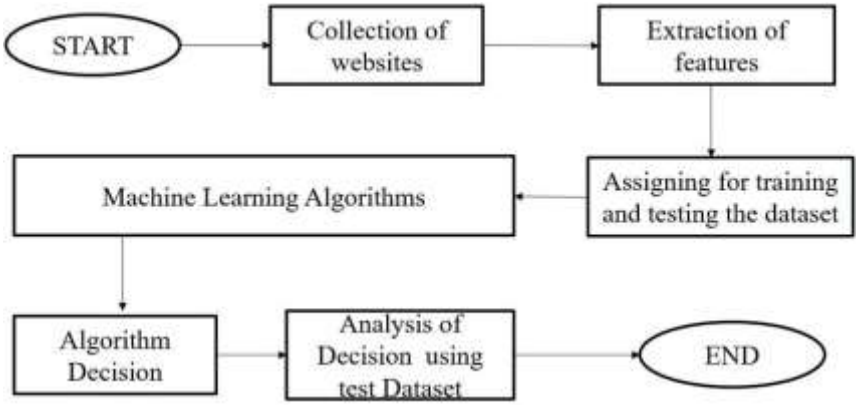
Dia.3

WHALING GRAPH



Dia.4

Block Diagram :



Dia.5

Result :

From the study of SVM classifier and whaling algorithm the training and test accuracy of both algorithm have a difference in output . The output ranges have been recorded in a line chart to check the training accuracy and test accuracy of both models to compare and refer SVM as the best model.

Conclusion :

Hence, the study on comparison of algorithms to choose the better model has be declared that SVM model best suits for future improvement in phishing security. Also to encourage the field of phishing security to make high standards to increase jobs and to improve knowledge.

References :

Journal reference:

- Opara.C, Chen.Y and Wei.B.2023; Look before you leap: Detecting phishing web pages by exploiting raw URL and HTML characteristics. Expert Systems With Applications. 2023; doi:https://doi.org/10.1016/j.eswa.2023.121183.
- Chuchuen, C., & Chanvarasuth, P. (2015). Relationship between Phishing Techniques and User Personality Model of Bangkok Internet Users. Kasetsart Journal of Social Sciences, 36(2), 322–334. Retrieved from https://so04.tci-thaijo.org/index.php/kjss/article/view/243314
- Vaishnavi Bhavsar, Aditya Kadlak, Shabnam Sharma .. Study on Phishing Attacks December, 2018. International Journal of Computer Applications 182(33):27-29 DOI:10.5120/ijca2018918286
- Alkhalil Z, Hewage C, Nawaf L and Khan I Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. (2021). Front. Comput. Sci. 3:563060. doi: 10.3389/fcomp.2021.563060
- Ankit Kumar Jain, B. B. Gupta, "Phishing Detection: Analysis of Visual Similarity Based Approaches", *Security and Communication Networks*, vol. 2017, Article ID 5421046, 20 pages, 2017.
- Mughaid, A., AlZu'bi, S., Hnaif, A. *et al.2022.* An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Comput* **25**,3819–3828(2022).
- Ayesha Arshad, Attique Ur Rehman, Sabeen Javaid, Tahir Muhammad Ali, Javed Anjum Sheikh, Muhammad Azeem. 2021 . A Systematic Literature Review on Phishing and Anti-Phishing Techniques. Pakistan Journal of Engineering and Technology, PakJET Multidisciplinary & Peer Reviewed Volume: 04, Number: 01, Pages: 163- 168, Year:2021
- Wosah Peace Nmachi , Thomas Win. 2021. phishing mitigation techniques: a literature survey. International Journal of Network Security & Its Applications (IJNSA) Vol.13, No.2, March 2021.
- Bhavani, P. Amba and Chalamala, Madhumitha and Likhitha, Pinnam Sree and Sai, Chanda Pranav Sai,2022.Phishing Websites Detection Using Machine Learning (September 2 2022). Available at SSRN: https://ssrn.com/abstract=4208185 or http://dx.doi.org/10.2139/ssrn.4208185
- Ahmed M.AbdelSalam, Wail S.Elkilani, Khalid M.Amin.. 2014 , An Automated approach for Preventing ARP Spoofing Attack using Static ARP Entries. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014.
- YANG LIU, KAIKUN DONG, LAN DONG, BIN LI. 2008, Research of the ARP Spoofing Principle and a Defensive Algorithm. WSEAS TRANSACTIONS on COMMUNICATIONSVolume 7Issue 5 May 2008pp 413–417

- Rishikesh Mahajan, Irfan Siddavatam. 2018, Phishing Website Detection using Machine Learning Algorithms. International Journal of Computer Applications (0975 – 8887) Volume 181 – No. 23, October 2018 .

Conference reference:

- Mohd Sarifuddin bin Othman, Muhammad Nomani Kabi, Ferda Ernawan, Wang Jing. An Enhanced Model for Increasing Awareness of Vocational Students Against Phishing Attacks, IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS 2019) 29 June 2019, Selangor, Malaysia pp.no.10 – 14.
- Dinesh P.M, Mukesh M, Navaneethan B, Sabeenian R.S, Paramasivam M.E, and Manjunathan A . Identification of Phishing Attacks using Machine Learning Algorithm . (2023),E3S Web of Conferences 399, 04010
- A.Lakshmanarao, P.Surya Prabhakara Rao, M.M.Bala Krishna.. Phishing website detection using novel machine learning fusion approach, Proceedings of the International Conference on Artificial Intelligence and Smart Systems. 2021 (ICAIS-2021) IEEE Xplore Part Number: CFP21OAB-ART; ISBN: 978-1-7281-9537-7.
- Michael A. Ivanov, Bogdana V. Kliuchnikova, Ilya V.Chugunkov, Anna M. Plaksina.. Phishing Attacks and Protection Against Them, IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus) | 978-1-6654-0476-1/20/$31.00 ©2021 IEEE | DOI: 10.1109/ElConRus51938.2021.9396693 . (2021)
- A. Hashim, R. Medani and T. A. Attia. *2020.* Defences Against web Application Attacks and Detecting Phishing Links Using Machine Learning, *International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, Khartoum, Sudan, 2021, pp. 1-6, doi:10.1109/ICCCEEE49695.2021.9429609.
- Dogukan Aksu, Abdullah Abdul wakil, M. Ali Aydın. 2017, Detecting phishing websites using support vector machine algorithm, 2nd World Conference on Technology, Innovation and Entrepreneurship (WCTIE-2017), V.5-p.139-142