Ideation Phase
Literature Survey

Date	19 September 2022
Team ID	PNT2022TMID26156
Project Name	Project - Web Phishing Detection
Maximum Marks	2 Marks

S.No	Topic	Year	Description	Author	Merits	Demerits
1.	**Mitigation of Phishing Attacks**	15 April 2013	This paper aims at a detection of phishing attacks. A high-level overview of various categories of phishing mitigation techniques are also presented, such as: detection, offensive defence, correction, and prevention, which we belief is critical to present where the phishing detection techniques fit in the overall mitigation process.	**Mahmoud Khonji, Youssef Iraqi, Andy Jones**	1.It adds great value to the overall security to an organisation 2. Use of different defence approaches.	1.Increased bandwidth demand. 2.The empirical effectiveness of this solution is bot accurately measured.

2	**Phishing website detection (volume 3)**	02 Februar y 2014	Phishing is a attempt to steal user's personal information through emails and other messaging services. Various researches have been done to prevent this phishing attack. They include firewalls, blacklisting certain domain and fake website detection.	**Feon Jaison, Seeni a Francis**	1.web browsers have integrated an anticipatin g filter into browser itself. 2.Atleast one brand of security software has integrated anti phishing filter.	1.Phishing attacks possess the detection of combination of customer reportage, pots in addition to technique.
3	**Comparison of Phishing Detection Techniques (volume 03)**	20 March 2014	Email has popular topic of discussion in today's world. Each month, more &more attacks are launched at the purpose of making web-users believe that they are dealing with a trusted & reliable entity for the purpose of stealing logon credentials, account information and	**Parth Parmar, Kalpesh Patel**	1.It constructs classificati on n models. 2.Mitigate zero hour attacks.	1.High computation al cost. 2.Higher fp rate than blacklists.

4	**Phishing detection: A recent intelligent machine learning comparison based on models content and features**	July 2017	Phishing possesses the characteristic of a singular fraud framework that uses a singular mixture possessed by designed what objective identify is additional advancement to sensitive in addition to data. Phishing attacks are becoming successful possessed by user awareness.	**FadiThabtah, Neda Abdelhamid, Hussein Abdel-Jaber**	1.Effective when minimal fp rates are required.	1.Mitigation of zero-hour phishing attacks. 2.Excessive queries with heavily loaded servers.
5	**Detection of URL based phishing attacks using machine learning(volume-08)**	27 November 2019	This proposed system predicts the URL based phishing attacks with maximum accuracy. Different machine learning algorithms are used in the proposed system to detect URL based phishing attacks. The hybrid algorithm approach by combining the algorithms will	**Ms. Sophia Shikargar, Dr.S.D. Sawarkar, Mrs. Swati Narwane**	1.Accuracy obtained by using different classifiers in the histogram graphicalnre presentation 2. More secured than previous systems.	1.Use of many classifiers give inaccurate result.

			increase accuracy.			
6	**A Survey of URL based PHISHING detection**	2019	This paper emphasize on URL based phishing detection techniques. It aims to understand the structure of URL based features and surveying their diverse detection techniques and mechanisms. It consist of summary of findings to promote better URL based phishing detection systems.	**Eint Sandi Aung, Chaw ThetZan and Hayato Yamana**	12 Use of more than one algorithm ensures accuracy. 2.Effectiv e phishing detection is achieved using different machine learning algorithm.	1.Classificat ion of structured and unstructured dataset is difficult.
7	**Phishing Detection using Machine Learning based URL Analysis (Volume 09 – Issue 13)**	02 August 2021	This paper tells that we are exposed to greater risks in the form of cybercrimes .URL based phishing attacks are one of the most common threats to the internet users. The goal is to create a survey resources for researchers to learn and contribute in	**Arathi Krishna v, Anusree A, Blessy Jose, Karthika Anil Kumar, Ojus Thomas Lee**	1.Uses performanc e evaluation metrics and confusion matrix adds value to the accuracy. 2.Effective ness is ensured by various performanc e metrics.	1.Choosing the right approach best suited for the specific dataset or application is a challenging task.

			making phishing detection model that yields more results.			
8	**Survey on Phishing Websites Detection using Machine Learning (volume 10)1**	May 2022	Machine Learning is an effective method for combating phishing assaults. This paper examines the features utilised in detection as well as machine learning based detection approaches.	**B. Ravi Raju, Sai Likitha, N Deepa, S Sushma**	1.Uses zero-hour attack detection , Language independency y and accuracy rate ensures phishing detection.	1.It lags in feature selection mechanism.
9	**Applications of deep learning for phishing detection(volume-64)**	23 May 2022	Deep neural network and hybrid deep learning provides best performance . This paper aims at phishing detection approaches were develop among which deep learning algorithms provided promising results. This paper address how deep learning algorithms have been used for phishing detection.	**Cagatay Catal, Gorkem Giray, Bedir Tekinerdoga n, Sandeep Kumar& amp, Suyash Shukla**	1.Effective deep learning methods are used in prevention of phishing attacks. 2.Various methods such as Deep Neural Network and Hybrid deep learning.	1.Challenges in calculation of datasets. 2.Model interpretability is difficult.