Literature Survey

Shri Krishnaa VN (19D092)

Siddharthan S (19D093)

Shankar Mahadevan G (19D087)

Manivel Prakash V (19D124)

Sanjeev (19D077)

- **Title:** Phishing Website Detection using Machine Learning Algorithms
- **Authors:** Rishikesh Mahajan MTECH Information Technology & Professor, Dept. Information Technology
- **Publication** : International Journal of Computer Applications (0975 – 8887) Volume 181 – No. 23, October 2018
- **Abstract** :Phishing attack is a simplest way to obtain sensitive information from innocent users. Aim of the phishers is to acquire critical information like username, password and bank account details. Cyber security persons are now looking for trustworthy and steady detection techniques for phishing websites detection. This paper deals with machine learning technology for detection of phishing URLs by extracting and analysing various features of legitimate and phishing URLs. Decision Tree, random forest and Support vector machine algorithms are used to detect phishing websites. Aim of the paper is to detect phishing URLs as well as narrow down to best machine learning algorithm by comparing accuracy rate, false positive and false negative rate of each algorithm.

- **Title:** Detecting Phishing Websites Using Machine Learning

- **Authors:** Amani Alswailem computer Science Department, Al-Imam Muhammad Ibn Saud Islamic University, Riyadh, Saudi Arabia. Bashayr Alabdullah Computer Science Department, Al-Imam Muhammad Ibn Saud Islamic University, Riyadh, Saudi Arabia.

- **Publication**：2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)

- **Abstract**：Phishing website is one of the internet security problems that target the human vulnerabilities rather than software vulnerabilities. It can be described as the process of attracting online users to obtain their sensitive information such as usernames and passwords. In this paper, we offer an intelligent system for detecting phishing websites. The system acts as an additional functionality to an internet browser as an extension that automatically notifies the user when it detects a phishing website. The system is based on a machine learning method, particularly supervised learning. We have selected the Random Forest technique due to its good performance in classification. Our focus is to pursue a higher performance classifier by studying the features of phishing website and choose the better combination of them to train the classifier. As a result, we conclude our paper with accuracy of 98.8% and combination of 26 features.

- **Title:** Phishing Website Detection based on Supervised Machine Learning with Wrapper Features Selection
- **Authors:** Waleed Ali Department of Information Technology
- **Publication** : (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 9, 2017
- **Abstract** :—The problem of Web phishing attacks has grown considerably in recent years and phishing is considered as one of the most dangerous Web crimes, which may cause tremendous and negative effects on online business. In a Web phishing attack, the phisher creates a forged or phishing website to deceive Web users in order to obtain their sensitive financial and personal information. Several conventional techniques for detecting phishing website have been suggested to cope with this problem. However, detecting phishing websites is a challenging task, as most of these techniques are not able to make an accurate decision dynamically as to whether the new website is phishing or legitimate. This paper presents a methodology for phishing website detection based on machine learning classifiers with a wrapper features selection method. In this paper, some common supervised machine learning techniques are applied with effective and significant features selected using the wrapper features selection approach to accurately detect phishing websites.

- **Title:** Detection of Phishing Websites using Machine Learning
- **Authors:** Atharva Deshpande , Omkar Pedamkar , Nachiket Chaudhary ,
- Dr. Swapna Borde
- **Publication** : IJERT Volume 10, Issue 05 (May 2021)
- **Abstract** :Phishing is popular among attackers, since it is easier to trick someone into clicking a malicious link which seems legitimate than trying to break through a computers defense systems. The malicious links within the body of the message are designed to make it appear that they go to the spoofed organization using that organizations logos and other legitimate contents.Here, we explain phishing domain (or Fraudulent Domain) characteristics, the features that distinguish them from legitimate domains, why it is important to detect these domains, and how they can be detected using machine learning and natural language processing techniques.

- **Title:** Phishing Website Detection Based on Deep Convolutional Neural Network and Random Forest Ensemble Learning
- **Authors:** Rundong Yang, Bin Wu
- **Publication**： Sensors 2021, 21, 8281
- **Abstract** :Phishing attacks have become a significant concern owing to an increase in their numbers. It is one of the most widely used, effective, and destructive attacks, in which attackers try to trick users into revealing sensitive personal information, such as their passwords and credit card information. A typical phishing attack technique involves using a phishing website, where the attacker lures users to access fake websites by imitating the names and appearances of legitimate websites, such as eBay, Facebook, and Amazon.