Project Objectives

Project: Web Phishing Detection

Phishing costs Internet users billions of dollars per year. It refers to luring techniques used by identity thieves to fish for personal information in a pond of unsuspecting Internet users. Phishers use phishing software to steal personal information and financial account details such as usernames and passwords.

The criminals, who want to obtain sensitive data, first create unauthorized replicas of a real website, usually from a financial institution or another company that deals with financial information. The website will be created using logos and slogans of a legitimate company. The nature of website creation is one of the reasons that the Internet has grown so rapidly as a communication medium, it also permits the abuse of trademarks, trade names, and other corporate identifiers upon which consumers have come to rely as mechanisms for authentication.

Phishing is one of the techniques which is used by the intruders to get access to the user credentials or to gain access to the sensitive data. This type of accessing is done by creating the replica of the websites which looks same as the original websites which we use on our daily basis but when a user clicks on the link he will see the website and think its original and try to provide his credentials.

To overcome this problem, we are using some of the machine learning algorithms in which it will help us to identify the phishing websites based on the features present in the algorithm. By using these algorithms, we can be able to keep the user personal credentials or the sensitive data safe from the intruders.

The main purpose of the project is to detect the fake or phishing websites who are trying to get access to the sensitive data or by creating the fake websites and trying to get access of the user personal credentials. We are using machine learning algorithms to safeguard the sensitive data and to detect the phishing websites who are trying to gain access on sensitive data.

Prediction and prevention of phishing attack is very crucial step towards safeguarding online transactions. The aim is to develop a model to safeguard users from phishing attacks.

Following efficient machine learning algorithms is the main motive in developing this project which will result in an efficient outcome, thereby alerting the users from any phishing sites and safeguarding their personal information.