

WEB PHISHING DETECTION

PROJECT DESCRIPTION:

Phishing is a form of fraud in which the attacker tries to learn sensitive information such as login credentials or account information by sending as a reputable entity or person in email or other communication channels. The phishing website can be detected based on some important characteristics like URL and Domain Identity, and security and encryption criteria in the final phishing detection rate.

RELEVANT BASE PAPERS:

TITLE	Phishing Website Detection Based on URL	Phishing Website Detection using Machine Learning Algorithms	Phishing – challenges and solutions
METHODOLOGY USED	The methods which has been used are Machine Learning Algorithm, Random Forest Algorithm is applied	The methods which has been used are Random Forest Algorithm and Decision Tree Algorithm is applied	Prevent phishing, Detect phishing, Stakeholder training
ADVANTAGES	<ol style="list-style-type: none">1. To preserve the confidentiality.2. To protect the user from phishing websites.3. To develop a user-friendly environment.4. To prevent or mitigate harm or destruction of computer networks, applications, devices, and data	This paper aims to enhance detection method to detect phishing websites using machine learning technology. We achieved 97.14% detection accuracy using random forest algorithm with lowest false positive rate. Also result shows that classifiers give better performance when we used more data as training data..	This delivers an enhanced level of phishing protection to detect attacks faster, alert users and remediate threats as quickly as possible.
DISADVANTAGES	The limitation is that all features are discrete. The other limitation is that the URL is to be copied and we have to search in the application then it will predict whether it is legitimate or not rather than redirecting the URL link to the application.	In future hybrid technology will be implemented to detect phishing websites more accurately, for which random forest algorithm of machine learning technology and blacklist method will be used	The problem with phishing is that attackers constantly look for new and creative ways to fool users into believing their actions involve a legitimate website or email.

PROBLEM STATEMENT:

A Cloud Based Web Application through Phishing is the most popular attack vector for criminals and has grown 65% in the last year. This application not only helps to detect phishing and also protect the users from unauthorized websites and then explain phishing, how attacks have affected businesses, how this form of cybercrime is growing, and how to defend against them.