

PROJECT OBJECTIVES

Project Name	Web Phishing Detection
Team ID	PNT2022TMID43023

ABSTRACT

Phishing is the fraudulent attempt to obtain sensitive information such as username, password, bank account details and credit card details for malicious use. Phishing frauds might be the most popular cybercrime used today. There are various domains where phishing attack can occur like online payment, webmail and financial institutions, file hosting or cloud storage and many others. The webmail and online payment sector was targeted by phishing more than in any other industry sector. Several anti-phishing techniques are there such as blacklist, heuristic, visual similarity and machine learning. From this, blacklist approach is commonly used because it is easy to use and implement but it fails to detect new phishing attacks. Machine learning is efficient technique to detect phishing. It is also removes drawbacks of existing approach. We perform detailed literature survey and proposed new approach to detect phishing websites by feature extraction and machine learning algorithm.

Problems:

1. Regression
2. Classification

Data pre-processing:

1. Handling the null values and categorical values.
2. Required the data.
3. Identify the dependent and independent values.
4. Split the dataset into train and test sets.

Analysis the dataset through visualization:

1. Univariate analysis
2. Bivariate analysis
3. Multivariate analysis

Applying algorithm:

1. ML Algorithm

Build the web application:

1. Using flask