PRE-SYNOPSIS

AREA OF WORK : Machine Learning and Software Engineering

PROPOSED TITLE : Phishing Website detection using machine learning

TYPE OF APPROACH : Web Application

WORKING MODEL : An individual Web Application.

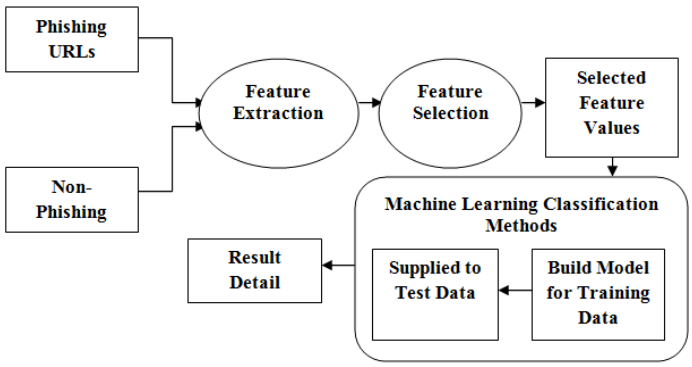
CONCEPT/IDEA :

Concept: A Flask web application that detects phishing websites using machine learning algorithms.
Idea: Develop a Flask web application that utilizes machine learning algorithms to detect and prevent users from accessing phishing websites. The application will analyze various features of a website, such as the URL, domain, content, and SSL certificate, to determine the likelihood of it being a phishing site.

OBJECTIVE :

1. Define a Flask route for handling the web app's endpoint where the user submits a URL for analysis.
2. Create an HTML form on the web app's front-end to collect the URL input from the user.
3. In the Flask route, retrieve the URL submitted by the user.
4. Use a machine learning model trained to detect phishing websites to classify the input URL.
5. Create a point object for each of the four points you mentioned (URL length, domain age, SSL certificate, and content analysis).
6. Analyze the URL length, domain age, SSL certificate, and content to determine the likelihood of the website being phishing.
7. Return the classification result to the user, indicating whether the website is potentially phishing or not.

BLOCK DIAGRAM :



NAME OF TEAM MEMBERS :- Mohd Shariyab [2001220100074]
Praveen Singh [2001220100085]

CS-73

SOURCE OF IDEA :- Self.

Reference:

- Block diagram of our proposed system | Download Scientific Diagram (researchgate.net)
- Welcome to Flask — Flask Documentation (2.3.x) (palletsprojects.com)