



PHISHING WEBSITE DETECTION

Guided by:
Mr. S.S. Yuvaraj

Done by:
Narendran G R
20BCM028

AGENDA

- Abstract
- Platform
- Modules
- Use-Case Diagram




ABSTRACT

- Phishing is a cyber attack which involves the use of fraudulent communications to trick victims into revealing sensitive information such as passwords, credit card details and Other personal information
- The attacker may use emails, text messages, or fake websites to deceive
- Types of phishing include:
 - E-mail phishing
 - Spear phishing
 - Smishing
 - Vishing
 - Clone phishing



PLATFORM

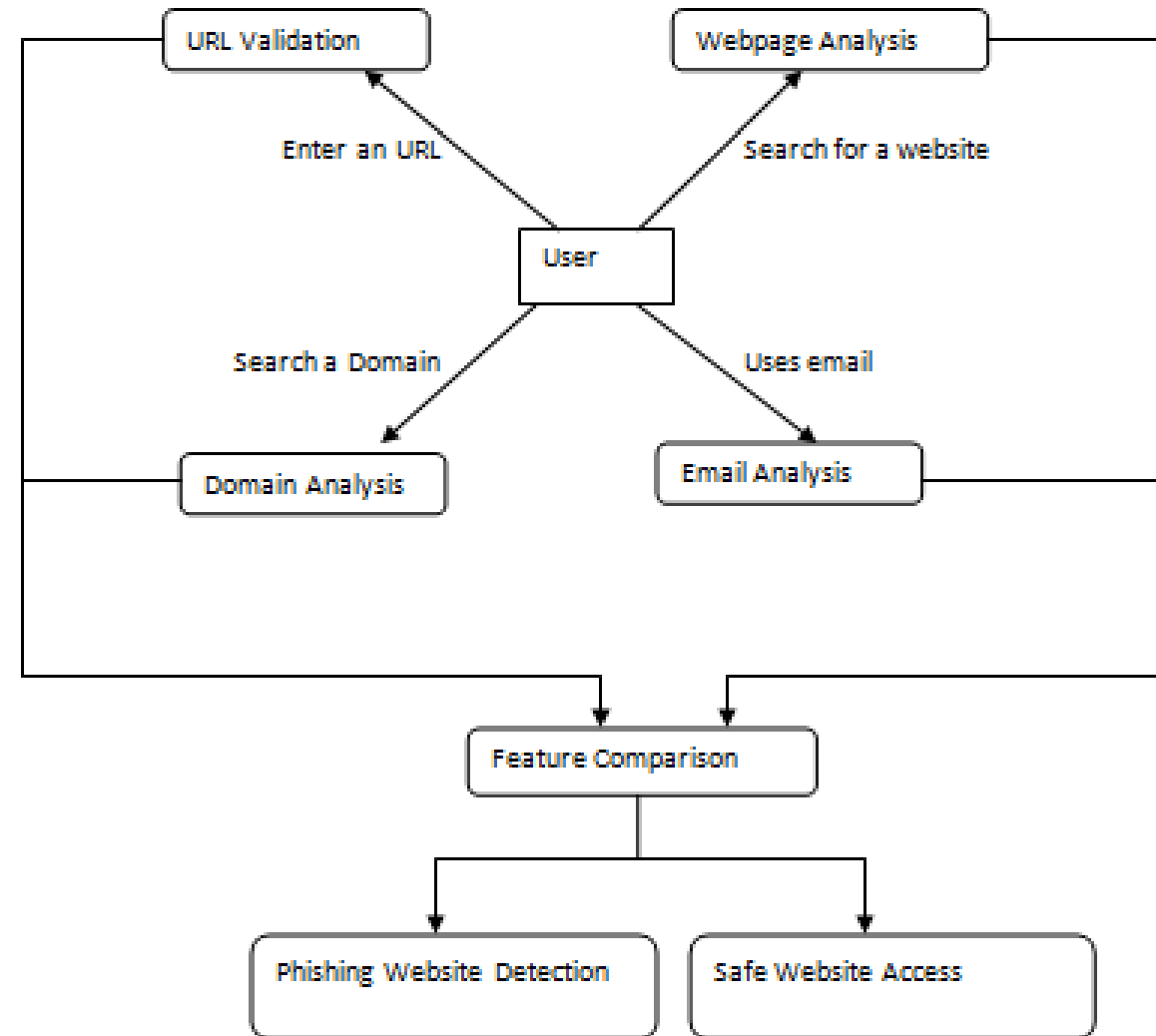
Front-end:	PYTHON 3.7 or above
Back-end:	Microsoft excel



MODULES USED

Name	Description
URL analysis	Analyze URL – identifies suspicious character/pattern - checks typos, misspelling in URL
Webpage analysis	Analyze content of webpage – image copied from legitimate web – hidden fields steal user data
Domain analysis	Identify red flags – recently registered domains – similar to legitimate domain
Email analysis	Suspicious elements – phishing links and attachments – sender address and email content
Machine learning model	Algorithm to analyze datasets of known phishing websites to identify patterns and trends that can be used to detect new phishing websites.
User Feedback	Feedback from users – suspect a website – improve accuracy to other modules – identify new phishing technique

DATA FLOW DIAGRAM





THANK YOU