Software Requirement Specifications

SRS – Phishing Website Detection Software

Submitted by
Student Name: Muhammad Zain ul Abideen
Roll no: F22BINFT1E02020
Section: 1E (BS IT)

Submitted to
Supervisor Name: Dr. Musarat Karim

Department of Information Technology
Faculty of Computing
The Islamia University of Bahawalpur

1. Introduction

1.1 Purpose

This SRS describes the requirements of a simple Phishing Website Detection Software that checks a URL and tells whether the website is Safe, Suspicious, or Phishing.

1.2 Scope

The software will:Take a URL as input

Analyze basic features (URL structure, HTTPS, domain pattern)

Detect phishing using simple rules or a basic ML model

Show the result to the user

2. System Overview

The system will have a very simple workflow:

1. User enters a website URL

2. System extracts features

3. System checks the URL against rules/ML model

4. System displays Safe / Suspicious / Phishing

The system will be a small web app or desktop app, depending on implementation.

3. Functional Requirements

FR-1: URL Input

The user can enter any website URL.

The system will check if the URL format is valid.

FR-2: Basic Feature Extraction

The system will check:

HTTPS available or not

URL length

Presence of suspicious characters

Domain looking abnormal (e.g., “paypal-login-secure.xyz”)

FR-3: Detection

System will classify the website as:

i. Safe
ii. Suspicious
iii. Phishing

FR-4: Display Result

System will show a message telling whether the URL is safe or not.

4. Non-Functional Requirements

NFR-1: Usability

The interface should be simple and easy to use.

NFR-2: Performance

The system should give result within 3 seconds.

NFR-3: Reliability

The system should work for most common URLs.

NFR-4: Security

The software will not store any personal data.

5. Assumptions

User will enter a valid URL.

Internet connection will be available for checking website.

6. Future Work (Optional)

Add a browser extension

Add real-time phishing URL database

Add machine learning trained model

Here is ONLY ONE professional Use Case, perfect for your SRS.

7. Use Case

Use Case ID: UC-01

Use Case Name: Submit URL for Phishing Detection

Primary Actor: User

Goal: To check whether a website is phishing or legitimate.

Precondition:

User has access to the system.

Internet connection is available.

Postcondition:

The system displays the detection result and logs the analysis (optional).

Main Flow:

1. User opens the phishing detection system.
2. User enters or pastes the website URL.
3. User clicks on the “Analyze / Detect” button.
4. System validates the URL format.
5. System extracts features from the URL (length, IP usage, domain age, etc.).
6. System runs phishing detection logic (rule-based or ML).
7. System generates the final result.
8. System displays Phishing / Legitimate / Suspicious to the user.

Alternate Flow:

4a. Invalid URL:

If the URL is not in a valid format,

System shows: “Invalid URL. Please enter a correct website address.”

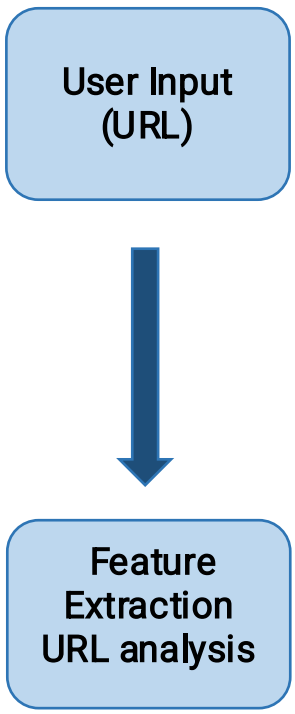
User enters the URL again.

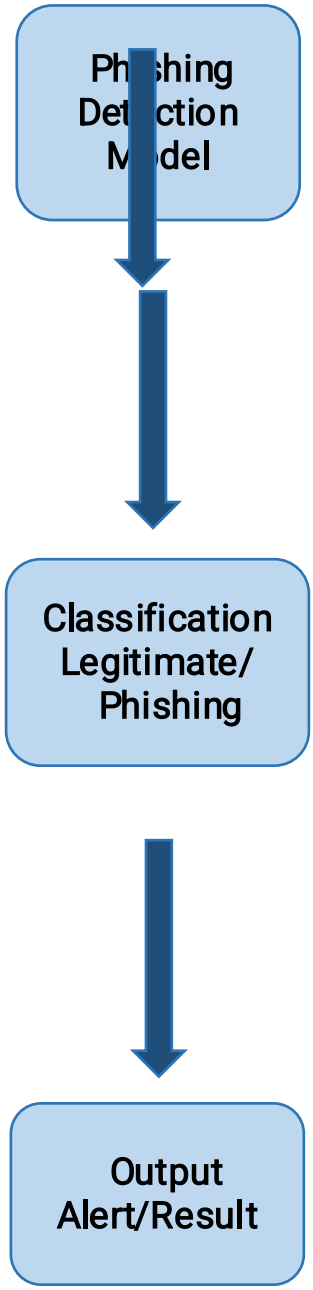
Exceptions:

No Internet: System shows “Network Error.”

Server Down: System displays “Unable to analyze right now.”

8. Diagram




Phishing Detection Model
Classification Legitimate/ Phishing
Output Alert/Result