**System Design Document Template**

**Version 1.0**

Malicious URL Detector

**Development Team:**

Sufiyan Irfan (SE-037)

Rehan Mumtaz (SE-036)

Kabeer Ahmed (SE-028)

**Approved By:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Project Advisor

**Table of Contents**

1. **Introduction -------------------------------------------------------------3**

1.1. Purpose -------------------------------------------------------------------------- 3

1.2. Scope----------------------------------------------------------------------------- 3

1.3. Definitions, Acronyms and Abbreviations---------------------------------- 3

1.4. References----------------------------------------------------------------------- 3

1.5. Assumptions and Constraints------------------------------------------------- 3

1.6. Document Overview------------------------------------------------------------ 4

1.7. Audience------------------------------------------------------------------------- 4

1. **System Description ------------------------------------------------------5**

2.1. System Overview--------------------------------------------------------------- 5

2.2. System Hardware Architecture ----------------------------------------------- 5

1. **Architectural Design ----------------------------------------------------6**

3.1. Architectural Goals and Constraints ---------------------------------------- 6

1. **Use-Case Diagram ------------------------------------------------------7**

**1. Introduction:**

**1.1. Purpose**

This document presents a complete architectural overview of the system, depicting many features of the system utilizing a variety of architectural viewpoints. Its purpose is to document and communicate the system's most important design decisions.

**1.2. Scope**

This software will be used by anyone who wants to see whether the site he/she is accessing is malicious or benign. Some of the key features of the system are the following.The software will enable the user to enter the URL and then the software will detect whether

**1.3. Definitions, Acronyms and Abbreviations**

**URLs :** Stands for Uniform Resource Locators.

**Malicious :** which is harmful for the system.

**OWASP Top 10** : The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

**Ransomware Attack :** In this attack the cybercriminal encrypts the victim's data and then demands money to give the decryption key.

**1.4. References**

None.

**1.5. Assumptions and Constraints**

The greatest constraint for the ASM project is time. The time allocated to the development, testing, and documentation of this project, incorporating both the windows and linux Pcs, along with the server-side application and database. Collectively, the development team has very little experience with the Networking Domain, so a significant portion of this time will be dedicated to learning the environment. Consequently, time is an even greater constraint. This may result in fewer features in the initial release,

**1.5.1. Assumptions**

This software will be installed on users' systems and on systems of the security department of an organization.

**1.5.2. Constraints**

Hardware limitation of this application can be unavailability of Internet . If Internet is

not available then the URL will not Scanned properly.

**1.6. Document Overview**

There are four sections in this SSD

* System description
* Architectural design
* Use-Case View
* Data Architecture

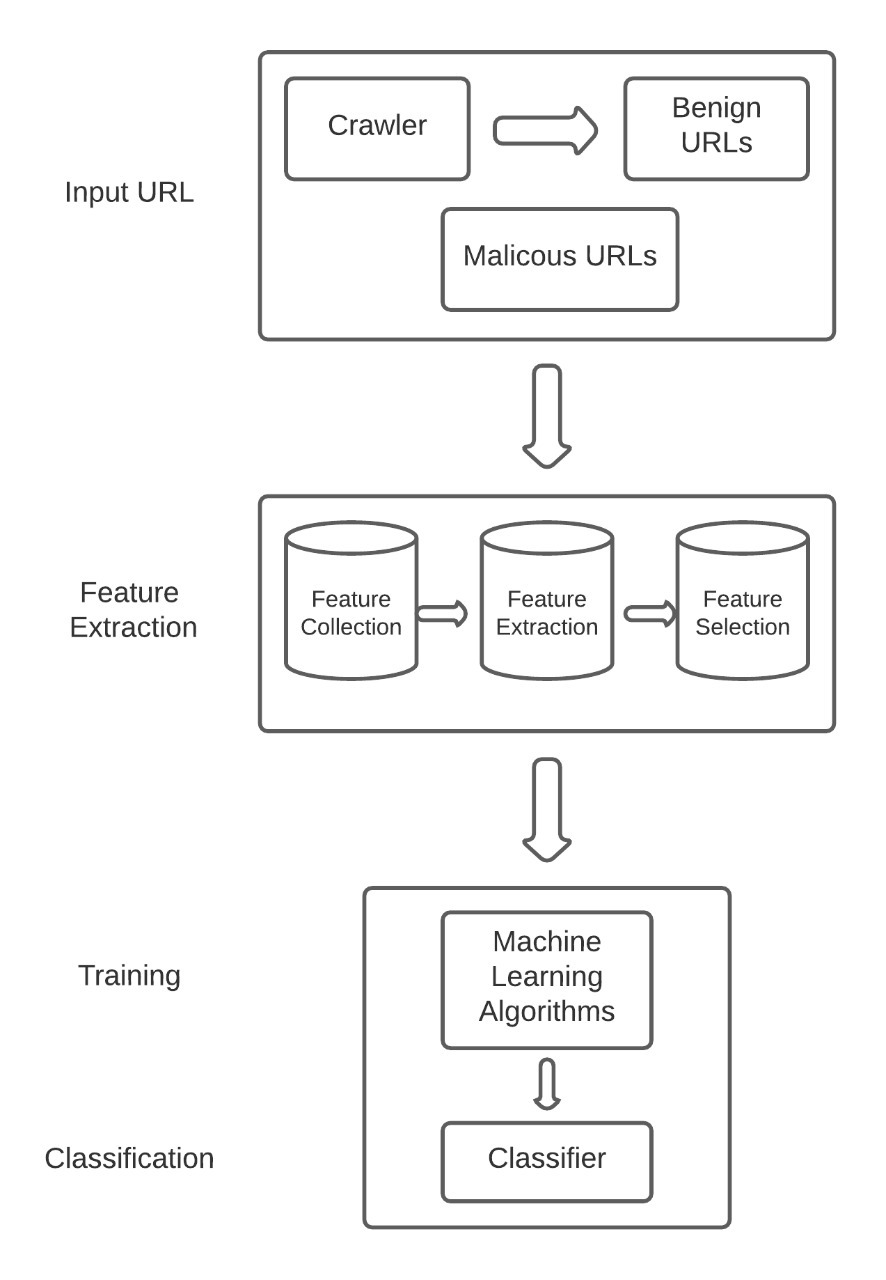
**1.7. Audience:**

The design documentation is in general for anyone who wants to understand the system

# **2. System Description:**

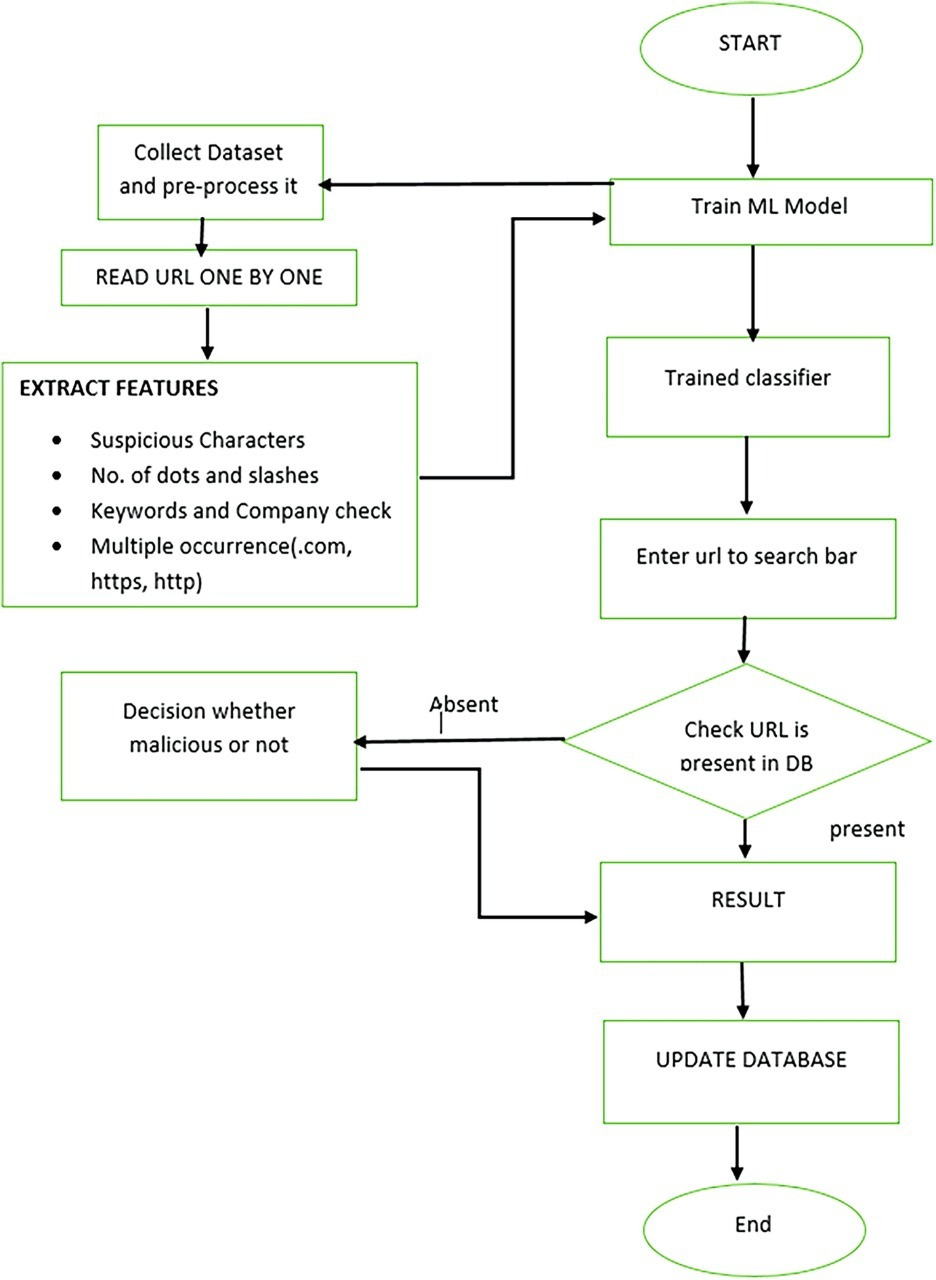
## **2.1. System Overview**

## **2.2. System Hardware Architecture**



## **3. Architectural Design:**

## **3.1. Architectural Goals and Constraints**



**4. USE-CASE Diagram:**

