**概要设计说明书**

目录

[1 引言 3](#_Toc81053590)

[1.1 编写目的 3](#_Toc81053591)

[1.2 范围 3](#_Toc81053592)

[1.2.1 系统目标 3](#_Toc81053593)

[1.2.2 主要软件需求 3](#_Toc81053594)

[2 体系结构设计 4](#_Toc81053595)

[3 接口设计 4](#_Toc81053596)

[3.1 用户接口 4](#_Toc81053597)

# 1 引言

## 1.1 编写目的

本说明书的目的是对恶意代码识别系统进行概要的功能说明，以便用户及项目开发人员了解产品大致的设计与实现。以下叙述将结合文字描述、数据流图、变换图等来描述恶意代码识别系统的体系结构设计、接口设计，数据设计等方面。本说明书的预期读者有客户、项目经理、开发人员以及跟该项目相关的其他竞争人员。

## 1.2 范围

### 1.2.1 系统目标

恶意代码识别系统是一款代码判断系统，用户可以上传需要判断的代码至系统内，而后系统会根据用户提供的代码进行判断，并输出相应的结果。

### 1.2.2 主要软件需求

系统功能列表：

|  |  |
| --- | --- |
| **功能点** | **功能描述** |
| 导入数据 | 引入Viper框架中存储的二进制数据 |
| 数据处理 | 对引入的二进制数据进行降噪处理 |
| 数字图像化 | 将二进制数据以8个字节为单位，转换成灰度图，使其成为卷积神经网络识别的数据集 |
| 导入训练集 | 导入需要的训练集 |
| 导入测试集 | 导入需要的测试集 |
| CNN识别 | 通过建立的卷积神经网络模型对恶意代码进行识别 |
| 提供接口访问 | 提供Restful API访问接口 |

功能需求：

实现基于CNN和图像的恶意代码检测模块（基于已有模块）

将检测模块集成到开放恶意代码管理框架中

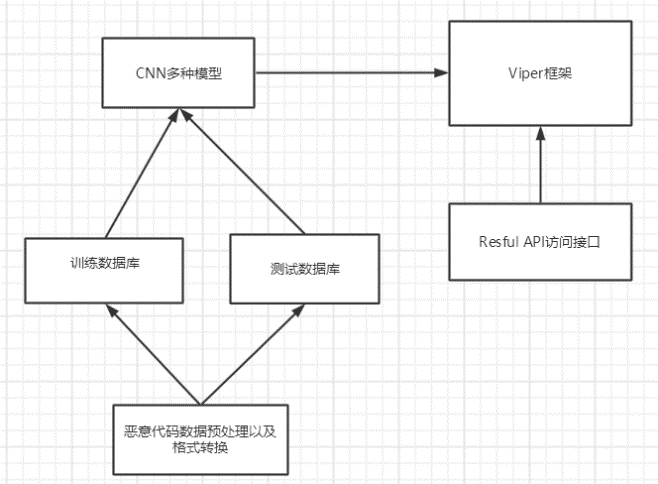
提供Restful API访问接口

非功能需求：

准确率大于75%

使用python3

# 2 体系结构设计



# 3 接口设计

## 3.1 用户接口

GET；从服务器中取出资源

POST：在服务器中新建一个资源

PUT：在服务器更新资源

PATCH：在服务器更新资源

DELETE：从服务器中删除资源

HEAD：获取资源的元数据

OPTIONS：获取资源的信息