**系统设计文档**

目录

[1 文档介绍 3](#_Toc81676264)

[1.1 文档目的 3](#_Toc81676265)

[1.2 项目背景 3](#_Toc81676266)

[1.3 需求概述 3](#_Toc81676267)

[1.4 读者对象 3](#_Toc81676268)

[2 功能设计 3](#_Toc81676269)

[2.1 模块划分 3](#_Toc81676270)

[2.2 功能描述 4](#_Toc81676271)

[2.2.1 数据预处理 4](#_Toc81676272)

[2.2.2 模型训练 4](#_Toc81676273)

[2.2.3 识别代码种类 4](#_Toc81676274)

[2.3 功能设计 4](#_Toc81676275)

[2.3.1 用例图 4](#_Toc81676276)

[3 详细设计 5](#_Toc81676277)

[3.1 后台设计 5](#_Toc81676278)

[4 开发环境 6](#_Toc81676279)

[4.1 开发工具 6](#_Toc81676280)

# 1 文档介绍

## 1.1 文档目的

此文档是识别恶意代码系统的设计文档，旨在通过此文档开发一个高效率、高准确率和通用性好的恶意代码系统。通过此文档，技术人员或者相关对技术了解的客户或者工作人员通过文档可以清晰看到系统实现的逻辑，便于与开发人员进行沟通。

## 1.2 项目背景

当前存在的恶意代码分析系统基本都停留在代码阶段，对于可视化方面并没有较好的系统，因此，本团队旨在将现存的恶意代码分析系统作为模板，安装在viper框架下，并通过viper-web对该系统进行可视化，从而使得用户能够使用界面操作，运行需要的模型，分析相应的恶意代码。

## 1.3 需求概述

为用户提供可视化的界面，并在界面中进行相关操作。用户可以上传和下载训练集和测试集，训练和运行指定的模块，并支持restful操作。同时，将数据集以及模型参数通过高斯数据库进行统一的管理。

## 1.4 读者对象

● 开发人员

● 维护人员

● 测试人员

# 2 功能设计

## 2.1 模块划分

|  |  |
| --- | --- |
| **模块名称** | **子功能描述** |
| 数据预处理 | 数据集下载 |
| 生成灰度图 |
| 模型训练 | 读取数据集 |
| 上传训练参数 |
| 模型训练 |
| 训练结果保存 |
| 识别代码种类 | 切换模型 |
| 查看模型 |
| 上传恶意代码 |

## 2.2 功能描述

### 2.2.1 数据预处理

|  |  |
| --- | --- |
| **功能名称** | **功能描述** |
| 数据集下载 | 从服务器上下载恶意代码数据集 |
| 生成灰度图 | 将恶意代码转换成灰度图并保存在本地 |

### 2.2.2 模型训练

|  |  |
| --- | --- |
| **功能名称** | **功能描述** |
| 读取数据集 | 读取预处理好的数据集 |
| 上传训练参数 | 用户将自己的训练参数写成.json文件上传 |
| 模型训练 | 使用训练集以及训练参数对模型进行训练 |
| 训练结果保存 | 将训练出来的模型参数进行保存 |

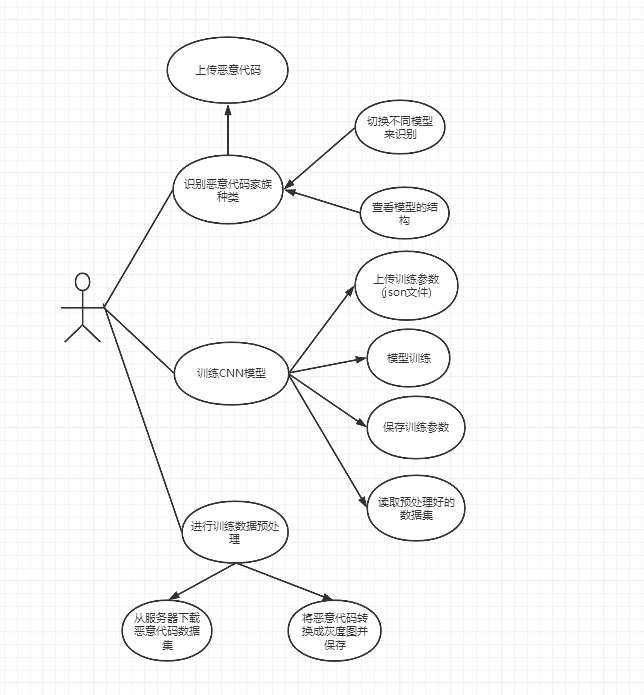
### 2.2.3 识别代码种类

|  |  |
| --- | --- |
| **功能名称** | **功能描述** |
| 切换模型 | 切换不同的识别模型 |
| 查看模型 | 查看当前模型的相关信息 |
| 上传恶意代码 | 将识别的结果上传至服务器中的数据库 |

## 2.3 功能设计

### 2.3.1 用例图

该系统的用例图如下：



# 3 详细设计

## 3.1 后台设计

该系统在服务器的数据库中总共建有2张表，分别为路径表和结果表。

路径表：

路径表主要是存放数据集的路径，前端向后端发送读取请求，后端根据前端请求在数据库中进行查找，得到该数据集的路径，而根据路径将相应的数据集传到前端。

|  |  |  |  |
| --- | --- | --- | --- |
| **列名** | **数据类型** | **说明** | **备注** |
| id | int | 数据集编号 | 自增 |
| file | varchar(1000) | 数据集存放的路径 |  |
| class | varchar(500) | 数据集类别 |  |

结果表：

结果表主要是存放恶意代码识别的结果，前端将结果传送到后端，后端将其保存在数据库中。

|  |  |  |  |
| --- | --- | --- | --- |
| **列名** | **数据类型** | **说明** | **备注** |
| id | int | 恶意代码编号 | 自增 |
| class | varchar(500) | 恶意代码类别 |  |
| time | date | 上传的时间 | 数据库自带属性 |

# 4 开发环境

## 4.1 开发工具

● 操作系统：Ubuntu、openEuler

● 使用框架：viper、pytorch

● 运行环境：python 3

● 数据库系统：openGauss数据库