智慧反电信欺诈系统
软件需求规格说明书
（IEEE 830 标准）

第九组

2025 年 4 月

目录

a.引言

a.1 目的

本需求说明旨在对 xx 平台的功能架构及子系统的功能需求、非功能需求进行逐一分析；并对各系统接口、质量需求、文档需求和约束做出可行方案。

本需求规格说明书编写目的：

（1）在需求调研阶段，通过本文档，与系统用户进行系统需求的确认。

（2）在系统设计阶段，通过本文档，指导该系统的概要设计和数据库设计。

（3）在系统开发阶段，通过本文档，帮助相关人员全面了解用户需求与系统功能。

（4）系统测试和联调阶段，通过该文档，是编写测试用例的依据。

（5）在系统实施阶段，实施人员借助本文档完成系统的实施工作。

（6）在系统使用过程中，本文档作为用户使用的辅助说明文件。

（7） 在系统验收阶段，本文档将作为主要验收依据。

a.2 预期读者和阅读建议

预期读者	阅读建议
甲方	需要阅读此文档全部内容，以了解软件的定位是否符合项目预期
开发人员	需要阅读此文档 b、c、d 部分的内容，重点了解软件的功能、运行环境、接口需求、功能需求、非功能需求、其他需求等
软件维护者	需要阅读此文档 b、c 部分的内容，以了解软件的功能、运行环境、功能和用户界面

用户	需要阅读此文档 b、c 部分的内容，以了解软件的基本特性、运行环境、功能和用户界面

a.3 产品的范围

本项目是非盈利性质的社会公益项目，因此本产品的目的是降低电信欺诈对电信公司和用户造成的经济损失和负面影响，同时提高用户满意度，促进社会和谐。本软件为电信用户提供自由诈骗举报平台，在其遇到诈骗时实时启用安全工具，并为其宣传诈骗信息；为警方提供报案信息和反馈结果功能；为软件维护者提供用户管理等功能。

a.4 参考文献

《软件设计文档国家标准 GB8567》

b.综合描述

b.1 产品的前景

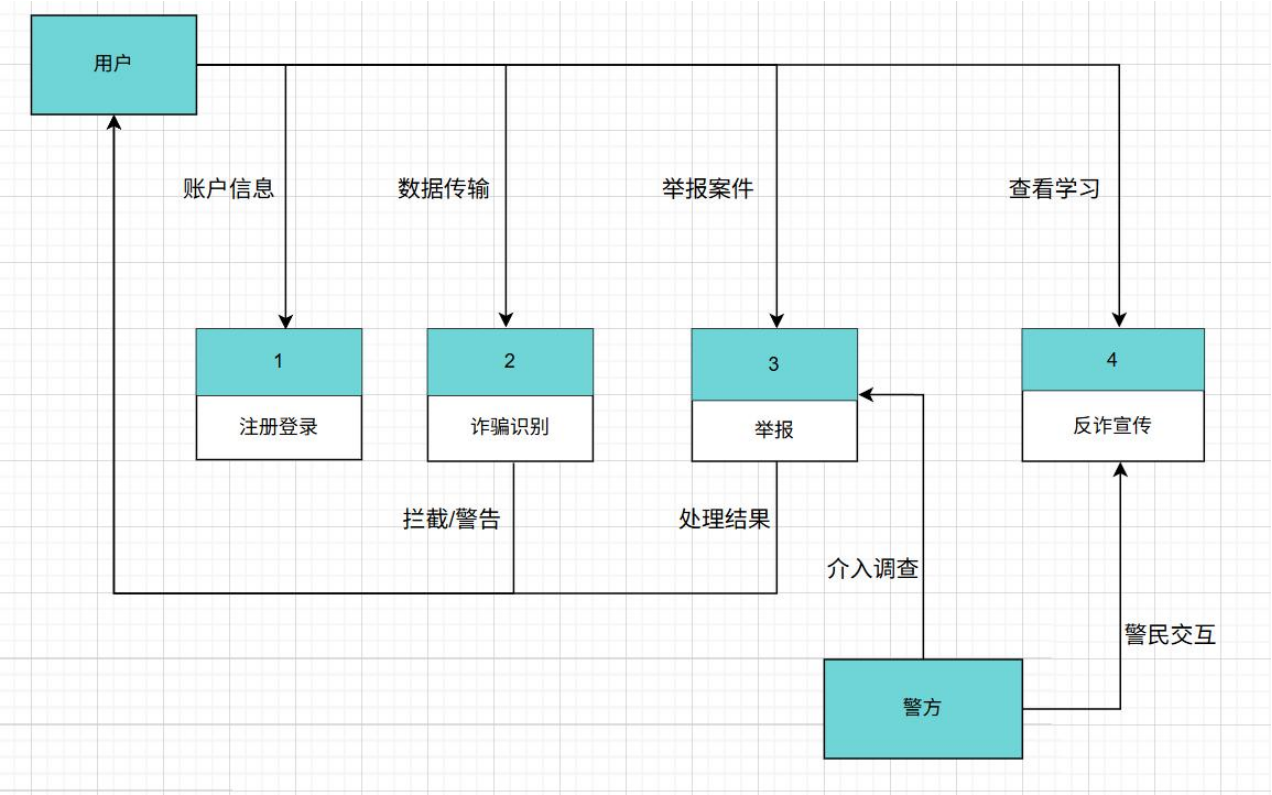
随着互联网技术快速发展，电信诈骗手段日益智能化，AI 换脸、语音合成等新型诈骗方式层出不穷。2024 年全国电信诈骗案件数量同比增长 26.7%，涉案金额持续攀升，校园成为重点受害场景之一。传统人工防范手段已难以应对新型诈骗威胁。

本项目是基于 AI 和大数据技术的智能化反诈平台，面向高校师生群体，整合通信数据、交易记录等多源信息，构建包含风险监测、智能预警、案例查询、举报反馈等功能的一体化防控系统。系统采用机器学习算法，实现诈骗行为的实时识别与拦截。

具体意义：

1. 提升校园安全：降低师生受骗风险，年预计减少诈骗案件 30%以上
2. 技术创新应用：将 AI 检测技术落地于实际安防场景
3. 社会价值：形成可复制的校园反诈模式，为智慧城市建设提供安全样板
4. 教育功能：通过案例库提升师生防范意识

b.2 产品的功能



图一：产品的功能和模块图

b.3 用户类和特征

涉众	使用目标	主要关注点	约束条件	权限	使用方式	群体数量	优先级
普通用户	诈骗号码识别、诈骗举报及结果跟进、反诈骗案例学习	便捷、有效、安全	登录	获取反诈骗知识、报案及结果查看	注册登录、浏览相关反诈宣传内容、向相关部门举报	10000	1

警方	获取诈骗报案信息	安全、易于获取信息	身份认证	发布反诈骗知识、获得报案信息	注册认证登录、获取反馈举报信息、推送相关反诈内容	20	2
软件维护者	软件开发维护	易于维护	熟悉软件维护的相关工作	后台维护	开发维护、处理系统使用中遇到的问题	10	3

b.4 运行环境

兼容设备包括搭载 Android 操作系统的移动终端设备以及支持 Android 系统的模拟器。

CPU：双核 2GHz 及以上；

内存：剩余空间应至少 1G 及以上

操作系统：Android 4.0 及以上版本。

b.5 设计和实现上的限制

1.由于支持本软件的操作系统为 Android 操作系统，因此限制开发工具为 Android Studio，开发语言为 Kotlin XML。

2.由于本软件需要连接已知的存储涉嫌诈骗的手机号码的 MySQL 数据库，因此数据库使用 MySQL5.6 及以上版本。

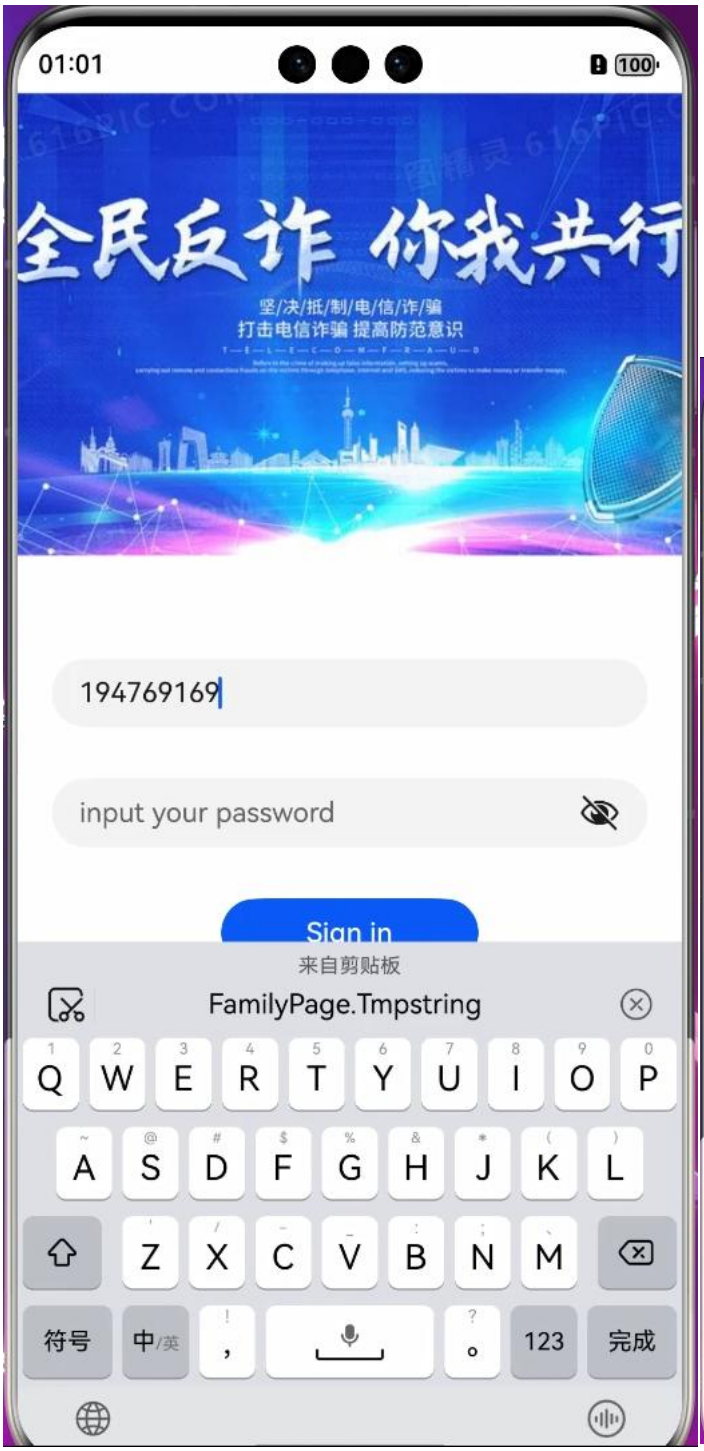
3.中文编码标准使用 UTF-8。

c. 具体需求

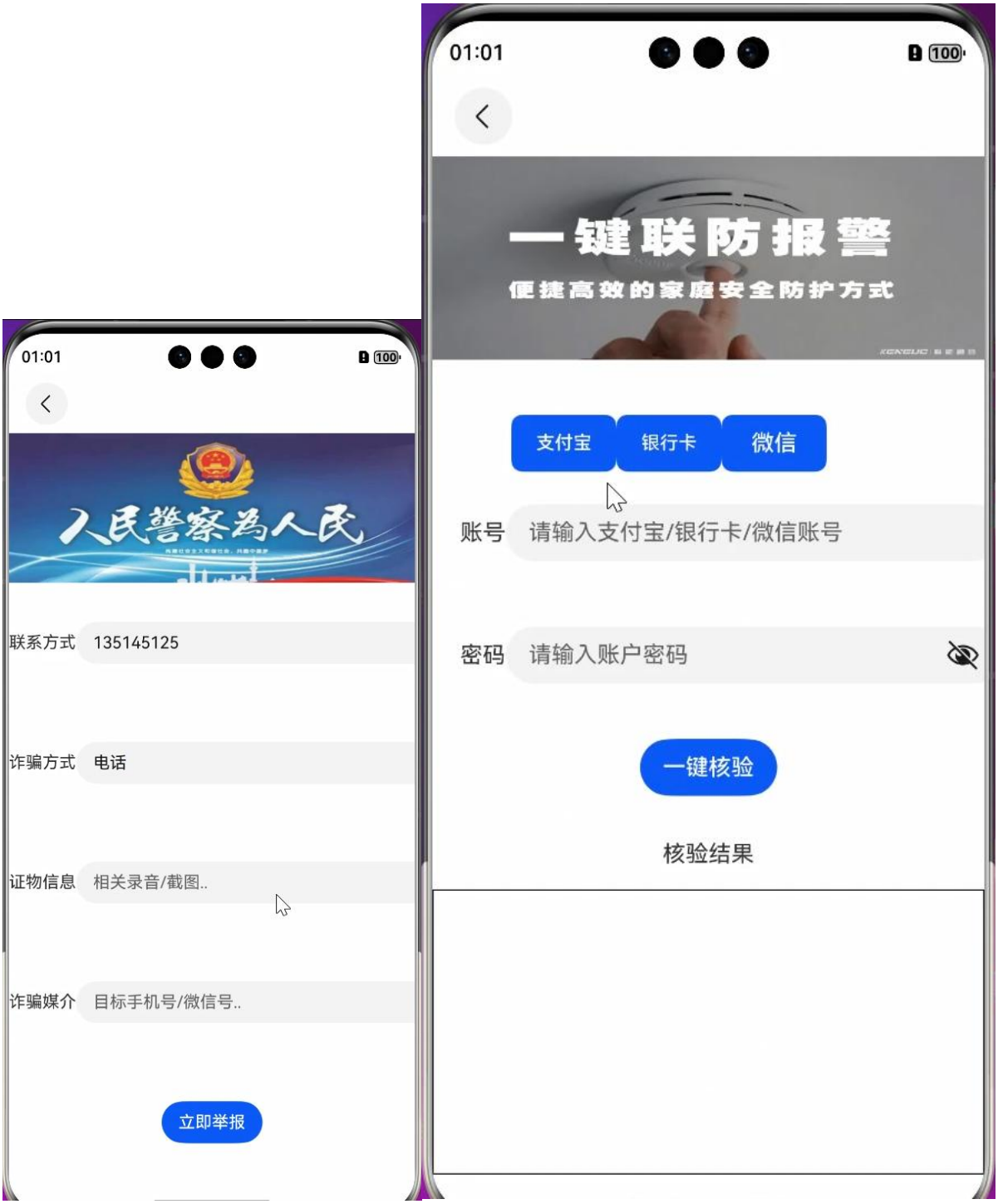
c.1 业务需求及系统特性

业务需求	实现业务需求所需要的系统特性	局部解决方案的对外交互
BR1：帮助用户更方便地对电信诈骗进行举报	SF1.1：能够从用户处获取举报信息，由人工审核后，将被举报违法对象加入数据库，并向用户发送举报成功或失败的信息	外部输入：被举报对象信息；外部输出：举报受理通知
BR2：防止诈骗者通过社交网络对用户进行诈骗	SF2.1：通过访问数据库查询户主是否有违法记录，并向用户发送提醒信息	外部输入：社交账户类型及账号；外部输出：提醒信息，包含该社交账户违法记录
BR3：防止用户被电话诈骗	SF3.1：查询打来的电话是否安全	外部输入：待查询电话号码；内部输出：该号码违法记录
	SF3.2：自动接听可疑来电并记录对话内容后发给用户	外部输入：对话语音；外部输出：处理后的全程对话
BR4：防止用户在不知情情况下进行支付	SF4.1：自动关闭免密支付	外部输入：是否使用支付助手；外部输出：支付助手开启情况
	SF4.2：交易进行时提醒用户交易账户信息	外部输入：支付账户类型及账号；外部输出：交易提醒，包括该账户违法记录
BR5：防止用户收到诈骗短信	SF5.1：根据数据库信息自动拦截可疑短信并向用户发送拦截记录	外部输入：短信发送者手机号；外部输出：拦截信息
BR6：方便用户查询公安局信息系统	SF6.1：联网公安部信息系统，在线浏览记录在案的犯罪人员及犯罪团伙信息	内部输入：公安部信息系统记录的犯罪人员及团伙数据；外部输出：转化了的可读性更强的犯罪人员及犯罪团伙信息

c.2 用户界面


01:01
全民反诈 你我共行
坚/决/抵/制/电/信/诈/骗
打击电信诈骗 提高防范意识
194769169
input your password
Sign in
来自剪贴板
FamilyPage.Tmpstring
符号
中/英
123
完成


01:01
案例
2021年3月20日，事主加了一个QQ群，对方称刷3单可以挣钱。对方给了事主一个网址，让事主在此网站上注册账户及绑定事主的银行卡，用于刷单操作。具体的操作过程是，事主给对方提供的个人账户充值，并将转账截图提交给对方，通过对方审核后，网站账户就会显示余额，然后再通过对方指导，在网站上购买指定的项目，让买多少钱就买多少，这时网站上的账户会显示赚钱了，就可以提现。后继续充值，但无法提现，事主发觉被骗。
针对群体
老年人
中年人
青少年
立即举报
立即报案
家庭联防
诈骗预警
号码查询
诈骗检测
号码标记
财产守护



c.3 硬件接口

支持搭载 Android 4.0 及以上版本系统的设备，使用串口协议与硬件进行数据交互和智能控制。

c.4 软件接口

本产品适用的操作系统为 Android 4.0 及以上版本，连接 MySQL5.6 及以上版本。为在诈骗号码识别时更好识别诈骗号码，产品连接存储已识别为诈骗电话的 MySQL 数据库，需要该数据库提供查找服务。

c.5 通信接口

为保证数据安全，使用 HTTPS 协议与服务器通信，设备主动从服务器获取所需数据。规定采用加密 MD5 加密，数据传输速率为 4-5Mbps。

d.其他非功能性需求

d.1 业务规则

用户只有登录后可正常使用功能。

用户需要提供真实准确的个人信息，并且在使用平台时需遵守法律法规和平台规定的使用规则。

平台需要设立监督机制，对违规行为进行处罚和封禁。

d.2 用户文档

用户手册：纸质，16 开本。

在线帮助。

电子文档，与软件产品一同分发配置。

d.3 软件质量属性

平台需要具有易用性、可靠性和可扩展性等软件质量标准属性，以提高用户的使用体验和满意度：

平台需要提供直观易懂的界面，使用户能够快速上手并完成所需操作；

平台需要定期进行软件测试和更新，确保系统的稳定性和可靠性；

平台需要支持可扩展的架构，以便在未来能够满足更多的需求。

附录 A：词汇表

网络诈骗：以非法占有为目的，利用互联网采用虚构事实或者隐瞒真相的方法，骗取数额较大的公私财物的行为。

国家反诈中心：国务院打击治理电信网络新型违法犯罪工作部际联席会议合成作战平台，集资源整合、情报研判、侦查指挥为一体，在打击、防范、治理电信网络诈骗等新型违法犯罪中发挥着重要作用

监护：对无民事行为能力人和限制民事行为能力人的人身、财产及其他合法民事权益，进行监督和保护的法律制度。履行监护职责的人称为监护人，受到监督和保护的人是被监护人。

附录 B：分析模型

1 结构化分析

1.1 ER 图

确认实体

用户

警方用户

诈骗事件

诈骗分子

智慧反电诈系统

诈骗案例库

反诈宣传

确认属性

用户：账号密码，身份证号，手机号，风险等级

警方用户：账号密码，警员编号，地区

诈骗事件：发生事件，诈骗类型，涉及金额

诈骗分子：身份证号，手机号，地区

反诈宣传：内容类型发布事件

确认关系

用户-诈骗事件：举报

智慧反电诈系统-诈骗事件：识别与拦截

智慧反电诈系统-诈骗案例库：关联分析

诈骗案例库-诈骗事件：参考案例

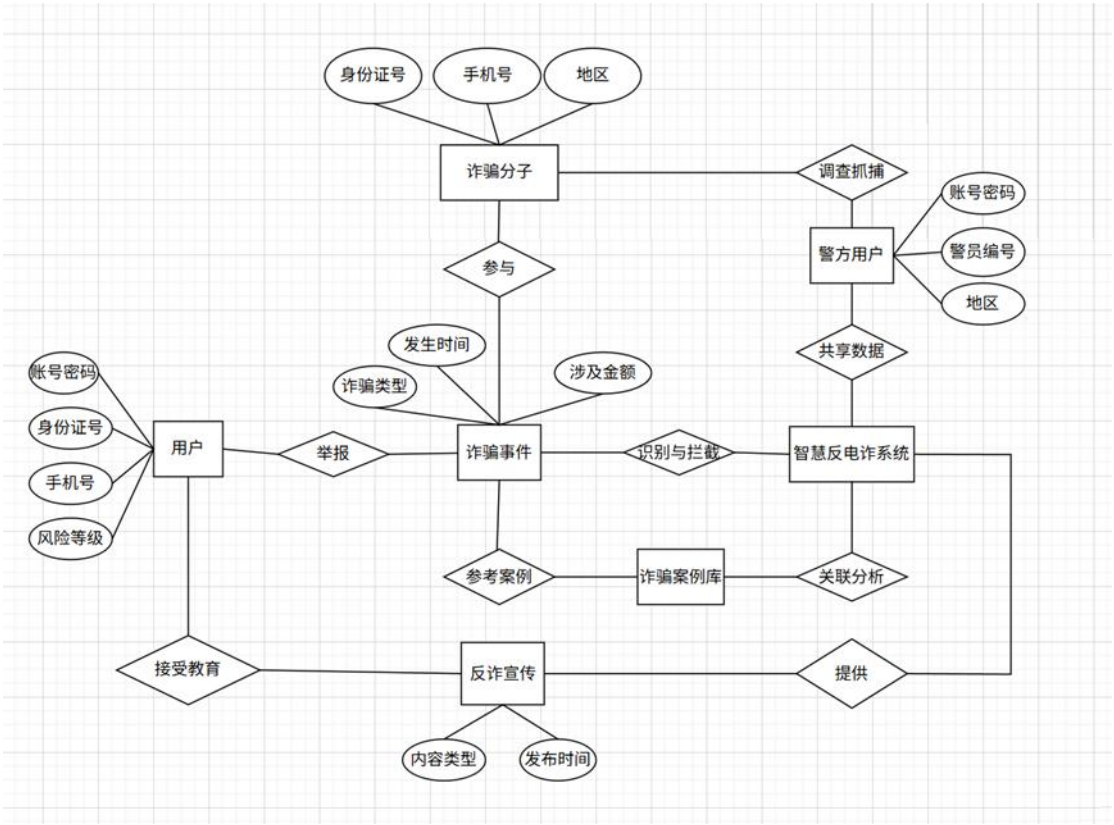
智慧反电诈系统-反诈宣传：提供

反电诈宣传-用户：接受教育

警方用户-智慧反电诈系统：共享数据

警方用户-诈骗分子：调查抓捕

诈骗分子-诈骗事件：参与



1.2 DF 图

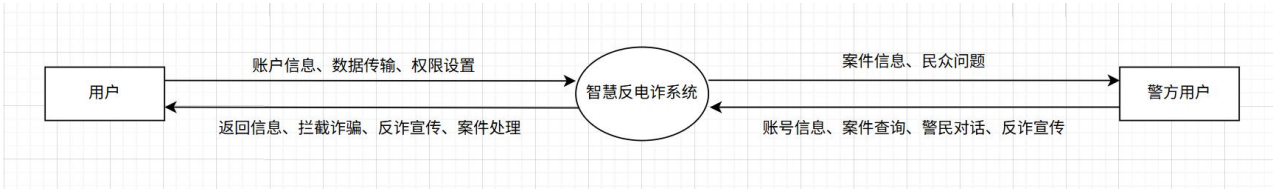
DFD 上下文图

1.用户输入账号信息（手机号、身份证等），完成注册或登录，授予系统必要的权限（如通话记录、短信访问权限）

2.用户设备自动监测来电、短信，实时上传可疑通信数据至反诈系统，系统通过智能分析，识别诈骗电话、钓鱼短信等风险信息，返回拦截提示和反诈宣传信息

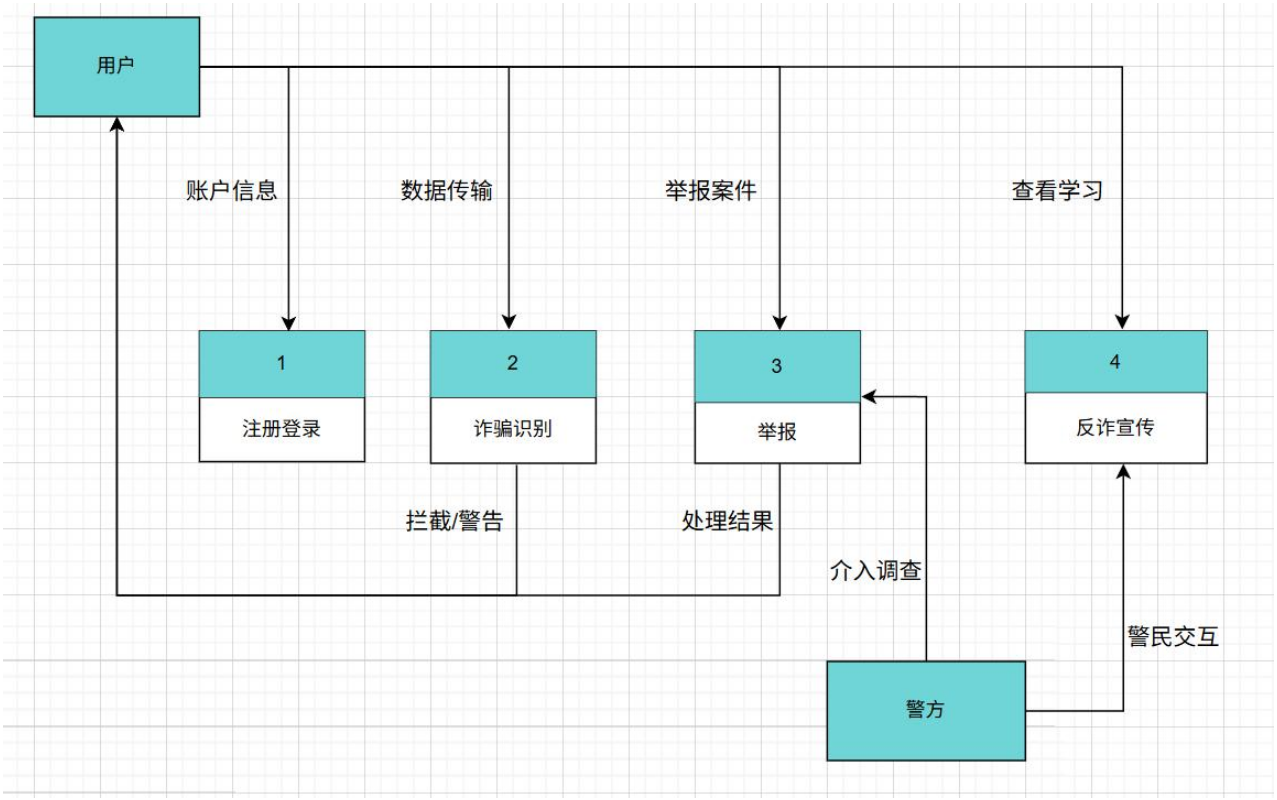
3.警方用户登录系统输入账户信息，可查询案件、进行警民对话、反诈宣传

系统返回案件信息、民众问题至警方用户



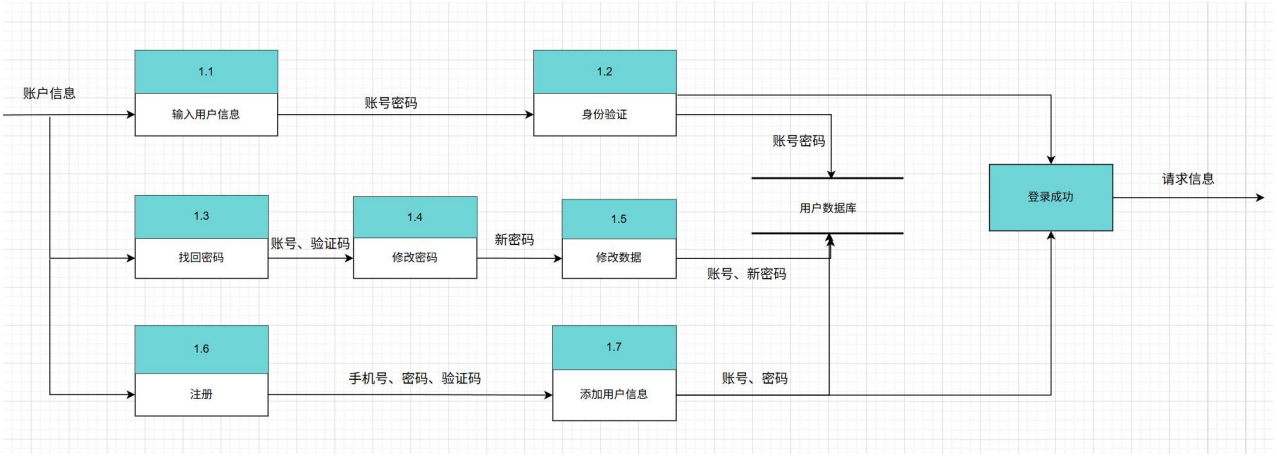
DFD-0 层图

系统主要划分为 4 个功能模块：注册登录、举报、诈骗识别、反诈宣传

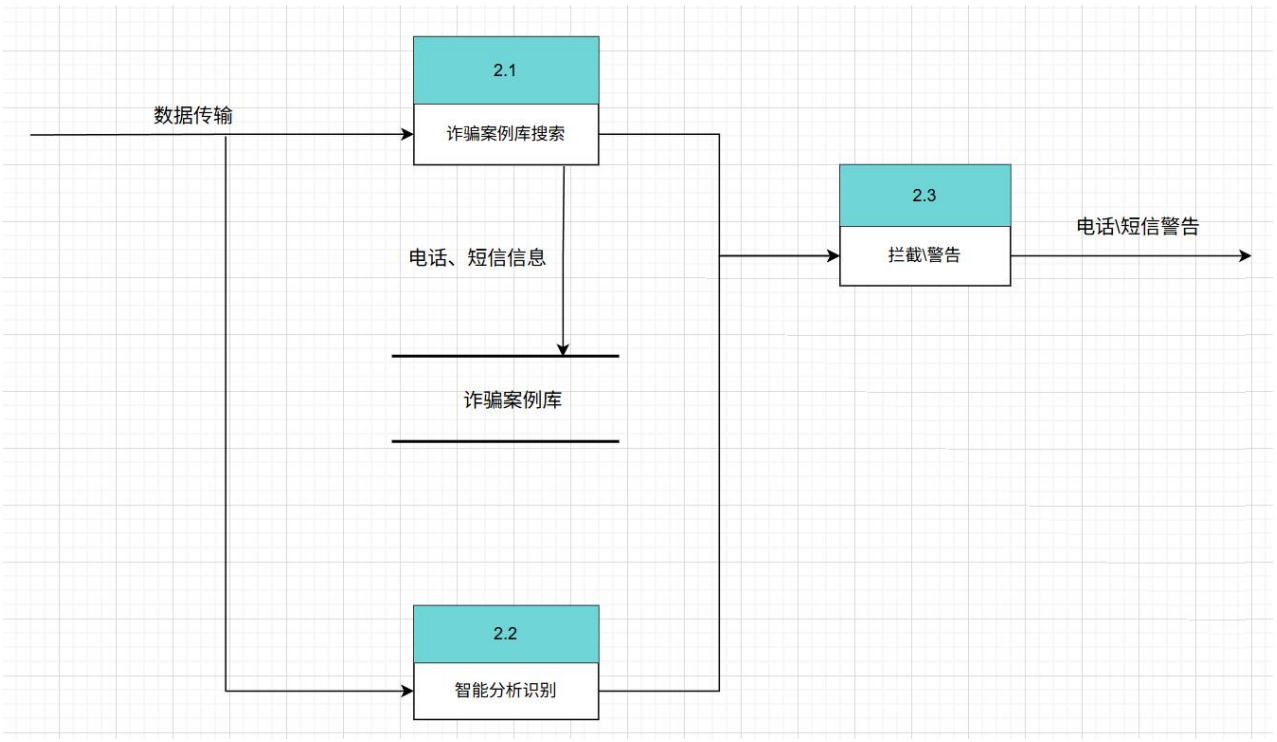

用户
账户信息
数据传输
举报案件
查看学习
1
注册登录
2
诈骗识别
3
举报
4
反诈宣传
拦截/警告
处理结果
介入调查
警民交互
警方

DFD-1 层图

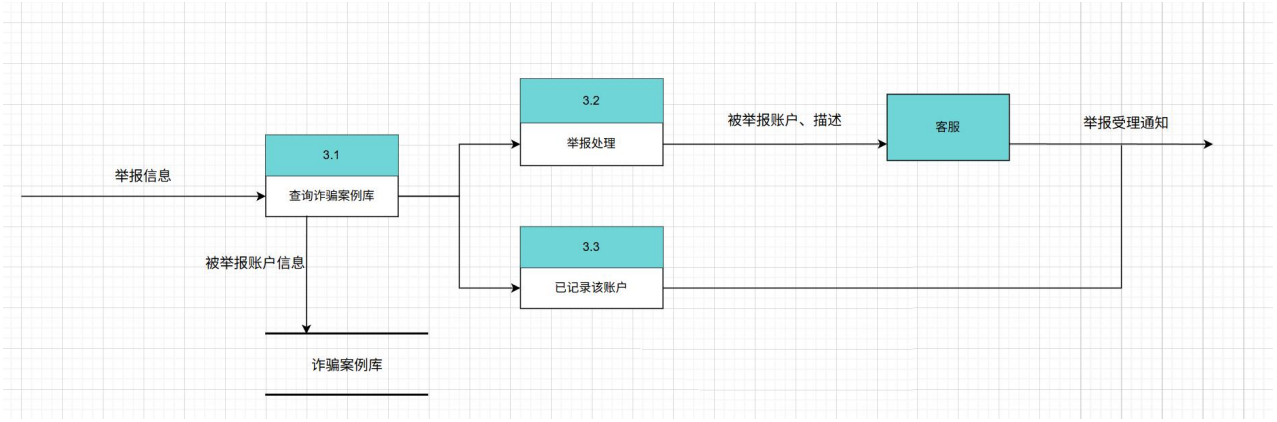
1）


账户信息
1.1
输入用户信息
账号密码
1.2
身份验证
账号密码
用户数据库
登录成功
请求信息
1.3
找回密码
账号、验证码
1.4
修改密码
新密码
1.5
修改数据
账号、新密码
1.6
注册
手机号、密码、验证码
1.7
添加用户信息
账号、密码

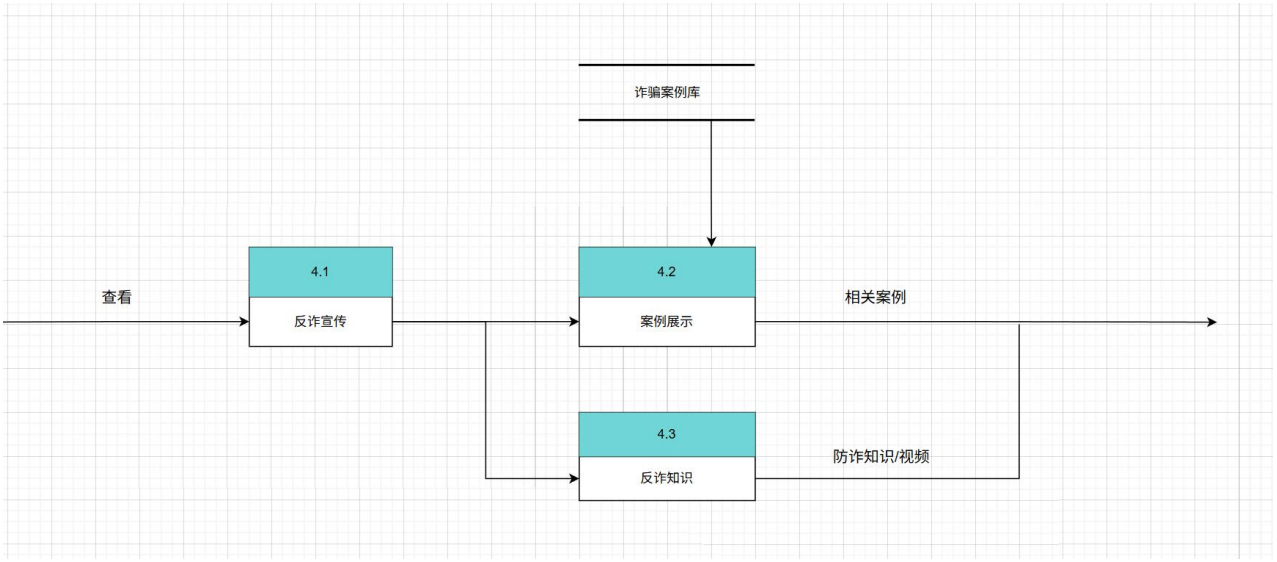
2）


2.1
数据传输
诈骗案例库搜索
2.3
电话\短信警告
电话、短信信息
拦截\警告
诈骗案例库
2.2
智能分析识别

3）


3.2
被举报账户、描述
客服
举报受理通知
举报处理
举报信息
3.1
查询诈骗案例库
3.3
被举报账户信息
已记录该账户
诈骗案例库

4）


诈骗案例库
4.1
4.2
查看
反诈宣传
案例展示
相关案例
4.3
防诈知识/视频
反诈知识

附录 C：数据字典

名称	用户账号
别名	账号
使用地点及方法	登录——输入账号（输入）；找回密码——输入账号（输入）
描述	与其类型账号标准一致（手机号）
格式	字符串

名称	用户密码
别名	密码
使用地点及方法	登录——输入账号（输入）；找回密码——输入账号（输入）
描述	8-16 位字符串，由数字，字母组成
格式	字符串