需求文档

1 引言

1.1 编写目的

如今，电信诈骗已不断向网络空间发展，呈现出传统犯罪网络化、网络犯罪常态化的趋势下。为有效打击电信诈骗犯罪，保障电信网络安全，某省公安厅积极探索基于 AI、大数据、图计算的反欺诈系统研究，搭建智慧反诈系统，实现对打猫断卡场景、假实名识别场景、高风险人群识别场景在内的多项反诈场景的预警和处理。

1.2 背景

随着互联网技术的蓬勃发展，每个人都使用各式各样的社交网络，新型诈骗方式也随之不断出现。AI 人工智能在诈骗范围中更是应用广泛，比如通

过输入一段语音，从而学习该语音主人的声音，从而实行诈骗。此外，还有AI 换脸，从而进行视频诈骗等等。

根据最新数据显示，2024 年全国电信诈骗案件数量和涉案金额仍呈现增长态势。各级法院审结电信网络诈骗案件 4 万件，涉及 8.2 万人，同比增长 26.7%；检察机关起诉相关犯罪 7.8 万人，同比上升 53.9%。电信诈骗手段不断演变升级，呈现出犯罪组织集团化、犯罪链条专门化、犯罪类型复杂化等特点。许多犯罪分子将诈骗活动延伸至境外，通过跨境作案逃避法律制裁，给司法办案带来极大挑战。例如，AI 诈骗成为新兴且极具威胁的诈骗方式，骗子利用智能 AI 技术，通过声音合成、AI 换脸、转发微信语音、AI 程序筛选受害人等手段实施诈骗，给公众造成了严重的财产损失。如2023 年，内蒙古自治区包头市发生一起使用智能 AI 技术进行电信诈骗的案件，福州市某科技公司法人代表郭先生 10 分钟内被骗 430 万元。

1.3 项目范围

用户角色范围：主要面向本校全体师生。为学生提供电信欺诈相关的防护功能，帮助他们识别和防范各类电信欺诈手段，保护个人财产安全；为教师提供管理和辅助学生防范电信欺诈的工具，同时自身也能获得相应的安全保障。

业务流程范围：以校园内电信欺诈的防范与处理为核心业务流程。首先是数据收集，收集校园内发生的电信欺诈案例、师生反馈信息以及学校与电信运营商、金融机构合作获取的相关数据。接着进行数据分析，运用适合的算法和模型对收集的数据进行分析，识别欺诈模式和潜在风险。然后是预警与处理，针对分析出的风险，及时向师生发出预警，并且提供处理建议和渠道，最后对处理结果进行记录和反馈，不断优化系统。

功能模块范围：包含欺诈信息查询功能，师生可查询常见电信欺诈类型、案例以及防范知识；风险预警功能，当系统监测到疑似电信欺诈行为时，通过短信、校内通知等方式向相关师生发出预警；举报与反馈功能，师生可举报遇到的电信欺诈情况，系统记录并处理反馈信息；个人信息保护功能，提醒师生保护个人信息，防止因信息泄露导致电信欺诈风险；数据分析与统计功能，对欺诈数据进行分析统计，生成报表，为校园反欺诈工作提供数据支持。

数据范围：收集和处理校园内电信欺诈相关的数据，包括但不限于校内发生的电信欺诈案例数据、师生个人的通信和交易数据（在符合隐私政策和获得授权的前提下）、学校与外部机构（如电信运营商、金融机构）合作获取的部分匿名化数据，以及网络上公开的电信欺诈相关信息。

本系统需求涵盖从数据采集、分析处理到欺诈预警、处置反馈的全流程功能。适用于电信运营商、金融机构以及相关监管部门在反电信欺诈业务场景中的应用。在项目开发周期中，从需求分析阶段到系统上线后的维护阶段均适用。

1.4 参考资料

2 任务概述

2.1 项目概述

2.1.1 项目来源及前景

中国信息通信研究院安全研究所的《电信网络诈骗治理与人工智能应用白皮书》发布，智能反诈骗相关项目的开展，市场的需求急需满足。同时未来智能反诈骗系统运用人工智能、大数据等新技术，可以应用于各个领域，如金融、电子商务、社交媒体等。并且随着区块链技术的发展，智能反诈骗系统还可以应用在数字货币交易等高风险领域，确保交易的安全和可靠性。

因此，从长远的角度而言，科学技术的不断发展与机器学习将使智能反诈系统长久在市场中占领一席之地。

2.1.2 业务机遇

从防范角度看，智能反电信欺诈系统能凭借 AI 智能实时监测海量通信和交易数据，精准识别潜在诈骗风险，实现主动防御，有效弥补传统人工防范的不足，是当下防范电信诈骗的关键力量。从监管治理层面，其能为监管部门提供全面准确的数据支持，辅助制定更具针对性的政策法规，完善监管体系，是法律监管与治理的有力补充。

随着《电信网络诈骗治理与人工智能应用白皮书》发布，社会对智能反电信欺诈系统的关注度和需求大幅提升，市场前景广阔。目前多数反诈骗系统技术陈旧，难以应对新型 AI 诈骗，智能反电信欺诈系统凭借先进的技术架构和算法模型，能有效识别新型诈骗模式，具备显著的差异化竞争优势。而且，随着 AI 技术的持续进步，智能反电信欺诈系统可不断拓展应用场景，与自然语言处理、图像识别等技术融合，实现功能创新升级，挖掘更多商业价值。

2.1.3 前景概述

慧反电信欺诈系统在大学生参与下前景广阔。对大学生自身，能保障其财产安全，避免陷入电信诈骗陷阱。在校园场景中，可助力校园安全建设，营造稳定学习环境。参与项目还为大学生提供实践机会，促进创新。随着系统在校园内成熟，其应用场景能逐步拓展到周边社区和社会群体。同时，项目能推动学校、运营商、金融机构等多方合作，整合资源构建更完善的反欺诈体系，提升社会整体防范电信欺诈的能力。

为电信运营商、金融机构及监管部门提供功能完备的智慧反电信欺诈系统。为电信运营商提供通信数据监测、异常行为预警功能；为金融机构提供交易风险识别、可疑交易拦截功能；为监管部门提供数据汇总分析、宏观态势把控功能。这能有效遏制电信欺诈行为，保障公众财产安全，提升各机构反欺诈工作效率，推动社会反欺诈体系的数字化与智能化发展。

2.2 目标用户

主要面向用户是学校的师生。

2.3 设计和实现上的约束

(1)人力和时间的约束：该系统开发过程中需要考虑到人力和时间的约束,相较于一些软件的开发团队来说人员较少时间较短。

(2)技术发展的约束：计算机技术和发展的日新月异，将会给信息处理带来更多手段，同时也会带来更加丰富的信息表达形式，例如现在发展起来的 chatGPT 等等，这就要求软件在设计时要考虑技术变化的可能性，为可能的变化预留一定的处理能力。

3 详细需求描述

3.1.功能需求

反电诈系统应实现以下核心功能：

1.系统管理功能：

系统管理员可以配置和管理系统的整体设置，监控系统运行状态，管理用户权限。配置和管理外部数据接口（如电信运营商、金融机构）和数据同步。管理系统中的诈骗检测规则与策略，确保持续的规则更新和优化。

2.用户管理功能：

系统应支持用户注册、登录、个人信息管理等基本功能。

用户（包括学生和教职工）可以管理个人隐私设置，查看和更新个人信息（如联系方式、预警设置等）。

用户可以查询常见的诈骗类型、案例、预防措施等信息。系统应提供搜索功能，帮助用户快速获取相关的诈骗知识。

系统必须包含保护用户数据的功能，例如加密敏感的通信和交易数据，确保没有经过明确授权的情况下，个人信息不会暴露。

系统应遵守当地的数据保护法规（如 GDPR、CCPA）实施隐私政策。

3.诈骗检测与分析：

系统必须能够收集、处理并分析大量数据，实时检测可疑活动，如不寻常的交易模式或可能存在的电信诈骗行为。

系统应使用基于人工智能的算法检测通信模式（例如，通话记录、短信互动）、金融交易和社交媒体活动中的异常。

4.风险预警与通知：

一旦检测到可疑活动，系统应通过多种通信渠道（如短信、电子邮件或校园内部通知）立即向用户（学生和教师）发出警报。

用户应在潜在诈骗被识别时实时收到警告，并提供如何减轻风险的建议（例如，提醒不共享敏感信息、联系相关部门等）。

5.诈骗信息数据库与查询：

系统应维护一个不断更新的诈骗案例数据库，包括常见的诈骗类型、防范知识以及实际案例。

用户应能够查询该数据库，了解不同类型的电信诈骗，包括钓鱼、语音钓鱼、短信钓鱼和 AI 驱动的诈骗（例如，声音合成、AI 换脸诈骗等）。

6.举报与反馈机制：

系统应提供一个举报系统，允许用户报告怀疑的诈骗案件。系统应安全地存储这些报告，对其进行处理并给予反馈，告知用户所采取的措施。

反馈机制应确保所有举报的诈骗案件都得到处理，并提供处理结果的更新。

7.与外部系统的集成：

系统应能与外部平台（如电信服务提供商和金融机构）进行集成，收集匿名或授权数据，以增强诈骗检测能力（例如，通话数据记录、银行交易）。

这种集成有助于跨平台检查诈骗模式，从而提供更准确的检测。

3.2 性能需求

3.2.1 更新频率

系统应定期更新各类数据。实时数据（如通信记录、交易数据）应在接收后立即处理，处理时间不超过 1 秒。诈骗案例库和防范知识库应每周更新，保证数据的时效性。诈骗检测规则和数据模型，则最少每月更新一次。

3.2.2 时间限制

对于实时监测数据，系统应在接收到数据后的 5 秒内进行处理并生成预警。

用户查询诈骗信息时，系统响应时间不应超过 3 秒。

举报数据的处理时间不超过 24 小时，确保用户能及时获得反馈。

3.2.3 保存规模

系统应能够存储并管理大量的通信数据、交易记录和用户举报信息。数据存储应采用分布式数据库架构，以支持高可扩展性。

系统应支持至少 3 年的数据存储，长期保存数据可归档并压缩处理，确保数据的完整性和安全性，便于对历史诈骗案例进行研究分析和预警。

3.2.4 系统负载

由于反电信诈骗属于长期稳定的需求且无明显受众群体，因此系统应支持至少 10,0000 个并发用户（具体的最大支持数量取决于系统的设计和实现，包括硬件、软件和网络等方面），同时保证数据的实时处理能力。且在高峰期间，尤其是在警报和实时监控关键时刻，性能不受影响，从而确保系统的广泛性和稳定性。

系统应能够处理高数据吞吐量，每分钟处理数千个交易和通信事件。同时系统具有一定的可扩展性和灵活性，以方便根据未来的需求进行扩展和升级。

3.3 质量属性

可用性

系统应提供 99.9%的可用性，确保用户能够随时访问系统，特别是在诈骗预警期间。

系统应具备高可用架构，采用多重备份机制和容灾处理，以防止单点故障影响系统正常运行。

可靠性

系统应保证高可靠性，特别是在诈骗检测和数据处理过程中，误报率应控制在5%以内，漏报率应控制在 2%以内。

系统应具备自动恢复能力，能在出现故障时迅速恢复到正常工作状态。

安全性

系统必须采用强加密算法对用户数据进行保护，确保通信数据和用户个人信息的安全性。

系统应实施严格的身份认证和权限管理，确保只有授权用户才能访问敏感数据。

系统应符合数据保护和隐私相关的法律法规，如《网络安全法》和《个人信息保护法》。

可维护性

系统应使用标准化的开发框架和代码结构，确保代码的清晰性和可维护性。

开发文档和系统日志应详细记录，便于后期的维护和故障排查。

可扩展性

系统应具备良好的扩展性，能够根据未来的用户增长和数据处理需求进行水平扩展。系统架构应支持微服务化，能够轻松扩展各个功能模块而不影响系统的整体性能。

3.4 约束

3.4.1 编程语言和平台限制

系统应使用成熟且高效的编程语言，如 Java、Python 或 Go，结合流行的机器学习框架（如 TensorFlow、PyTorch）进行诈骗检测。

前端可使用 React 或 Vue.js 等现代 Web 框架，后端可采用 Spring Boot 或 Django 等框架进行开发。

系统应支持多平台部署，能够在 Windows、Linux 等主流操作系统上运行，并能够与主流数据库（如 MySQL、MongoDB）兼容。

3.4.2 相关标准和协定

反电信诈骗系统的设计和实施应遵守相关的标准和协议，以确保其符合行业和法律要求，保障系统的安全性、可靠性和合规性。
具体而言国家和地方相关法律法规如《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》以及行业和国际标准如 ISO/IEC 27001 信息安全管理体系等。在开发过程中，我们将充分考虑这些标准和协定的要求，并且进行充分的测试和审核，以确保系统的合规性和可靠性。

3.5 对外接口

3.5.1 与其它系统间接口

电信运营商接口：系统应与电信运营商的通信数据平台对接，获取电话、短信等通信记录，用于实时监控和诈骗检测。

金融机构接口：系统应能与银行、支付平台等金融机构的交易系统对接，分析交易数据，识别潜在的金融诈骗行为。

第三方数据接口：系统应支持与第三方反诈骗平台和数据库对接，实时获取诈骗电话号码、邮箱、IP 地址等信息，用于验证用户行为。

3.5.2 用户交互方式

Web 界面：用户可通过 Web 浏览器访问系统，查询诈骗信息、接收风险预警、提交举报等。

移动应用：为用户提供手机 APP，支持在移动端进行查询、接收通知和管理个人信息。

API 接口：系统提供开放 API 接口，允许其他系统或开发者接入并获取诈骗检测数据，扩展系统功能。

3.6 其它需求

3.6.1 数据需求

通信数据：系统需获取电信运营商提供的通话记录、短信日志等信息。

交易数据：从金融机构获得交易数据，用于识别潜在的金融诈骗。

举报数据：系统需处理来自用户的举报信息，存储举报内容、举报人信息及处理结果。

3.6.2 数据管理及展示

数据存储：所有收集到的数据需存储在安全的数据库中，支持高效查询和处理。

数据分析：系统应提供数据分析和可视化功能，通过报表、图表等方式展示诈骗活动趋势、受害人群体特征等。

数据保护：系统应对敏感数据进行加密存储和传输，保证数据的安全性和隐私保护。