

2026 睿抗机器人开发者大赛

CAIP 强脑赛道智能算法及应用赛项

金融反诈智能守护赛题规则文件

一、项目概览

1. 赛题名称

金融反诈智能守护

2. 赛题简介

随着金融科技迅猛发展，各类电信网络诈骗、虚假金融信息、钓鱼网站等新型犯罪手段层出不穷，严重威胁人民群众的财产安全和社会稳定。本赛题聚焦金融反诈核心场景，要求参赛团队融合机器学习、深度学习、自然语言处理、计算机视觉、知识图谱、流式数据处理等人工智能技术，设计并实现能够有效识别、预警、劝阻金融诈骗的智能化系统或模块。鼓励参赛者结合银行、支付机构、电商平台等真实业务场景及金融业务逻辑与风控原则，提出具有创新性、实用性和安全性的解决方案，为构建全民反诈防线贡献智慧。

二、竞赛交流群

QQ 交流群号：344828618（验证信息格式：学校+姓名）

咨询老师联系方式：徐老师 13858014284（工作日 9:00-17:00）

三、赛题目标

1. 技术挑战

金融交易数据中欺诈行为的实时识别与动态异常检测；虚假信息及钓鱼联络的多模态深度识别与新型对抗样本防御；智能反诈交互系统的精准自然语言理解、复杂多轮对话管理及知识图谱动态推理；系统在高并发混合云部署、泛终端接入场景下的低延迟响应与全生命周期数据安全合规保障。

2. 成果预期

人才培养：掌握多元异构数据预处理、高维特征工程构建、机器学习/深度学习模型训练与轻量化优化、多模态自然语言处理、流式数据处理、对抗样本防御等核心技能，具备金融反诈场景下的技术落地与系统研发能力；

产业转化：推动银行、支付机构、电商平台等金融场景的全链路反诈能力升级，适配混合云部署、泛终端接入的金融科技新架构，为金融智能风控、智能反诈交互、网络安全防护等领域提供可落地、可迭代、高适配的创新技术方案，助力金融机构构建智能化、体系化的反诈防护体系。

四、参赛要求

1. 团队要求

以队伍形式报名，每队 1-3 人（含队长），队长为团队联系

人；支持跨院校、跨专业组队，但不允许跨省组队，队长所在单位即为参赛单位。

2. 设备规范

参赛团队自备开发所需的计算机及相关硬件设备；若作品需部署在移动端或嵌入式设备，需在作品中注明并提交适配方案。

五、竞赛场地及道具

1. 场地规格

线上初赛不设实体场地；现场决赛在指定竞赛场地进行，提供标准答辩展示区及网络环境。

六、竞赛任务

参赛团队可从以下方向中任选其一完成作品

● 方向一：欺诈交易智能识别

该任务针对金融交易全链路风险防控场景，聚焦第三方支付跨时段、跨渠道异常交易检测需求。参赛团队**需自建或模拟包含多源异构金融交易数据的仿真环境**，支持跨时段、跨渠道的交易行为生成，涵盖正常交易与体现多样性、隐蔽性及团伙协作性的欺诈交易两类场景。系统需对仿真交易流数据进行实时识别与动态异常检测，在交易发生的同时完成风险评估与欺诈判定，并输出识别结果与风险等级。鼓励融合行为画像、设备指纹、交易网络、用户社交关联等多维度特征构建识别模型，并说明特征的来

源、构建方式及其在识别中的作用。系统应具备高准确率与低误报率，适配流式数据处理框架（如 **Kafka + Flink**），具备自适应学习与模型迭代能力，能够根据新增仿真欺诈样本动态优化识别效果。鼓励基于图神经网络或其他图分析方法实现欺诈链路挖掘，识别团伙式欺诈结构，并支持检测结果的可解释性与溯源分析，便于人工研判与策略调优。系统设计需适配混合云部署场景，具备高并发、低延迟的业务处理能力，参赛团队需提交系统架构图、关键技术选型说明及性能测试方案。

● **方向二：虚假信息 and 钓鱼链路识别（系统设计与特征库驱动方向）**

针对金融机构全场景舆情监控与风险拦截需求，要求参赛团队设计并实现一套基于规则引擎与特征库驱动的虚假信息及钓鱼链路识别系统。系统需通过构建多维特征库、设计识别规则与研判逻辑，实现对金融领域虚假内容及钓鱼链路的有效识别、风险定级与预警响应。参赛团队需自建多维特征库，涵盖文本、图像、音频、URL 特征、网页/小程序结构、链路传播轨迹等维度，说明各维度的设计逻辑与提取方式；基于此设计规则引擎或决策树模型，通过规则匹配与权重计算输出多维度可信度评估与风险等级判定，并支持新增欺诈模式的快速接入。系统需具备新型对抗样本防御能力，能够识别 URL 混淆、文本变形、图像伪装等

常见对抗手法；同时支持真实业务场景下的实时拦截与预警，输出可解释的研判依据辅助人工决策。系统应具备灵活迭代机制，通过规则更新、特征库扩展等方式持续适配新型欺诈手法，鼓励设计未知手法挖掘模块。系统需适配网页、小程序、移动端等泛终端接入场景，保障低延迟响应与数据安全合规。

● 方向三：面向反诈教育的智能客服（对话系统）

针对学生群体及泛个人用户的反诈科普与实时风险劝阻场景，开发具备游戏化交互 + 智能研判功能的多模态智能反诈对话系统，以多轮智能对话形式普及刷单返利、游戏交易、冒充公检法、虚假投资、校园贷等常见骗局的防范知识。系统需提供反诈知识普及、风险行为实时劝阻、可疑链接 / 内容一键举报、风险场景智能研判等全流程交互服务。参赛团队需**自建反诈知识库**，以结构化、半结构化或规则化形式组织骗局特征、手法、典型案例、防范建议及法律法规等内容，支撑问答、推理与劝阻话术生成。系统设计**规则引擎或轻量级意图识别模块**，依据关键词、句式、上下文识别用户意图并匹配知识内容，支持新增骗局快速接入。系统应具备**风险行为实时劝阻能力**，结合风险特征规则对疑似受骗行为进行研判，输出场景化、个性化的劝阻话术与防范建议。提供**可疑链接/内容一键举报入口**，通过 URL 特征匹配、关键词黑名单等规则进行初步研判与反馈。交互层面融入积分、

勋章、闯关、情景模拟等游戏化元素，鼓励设计典型骗局情景模拟模块。可融合语音交互、情感分析等多模态技术，适配网页、小程序、移动端等泛终端接入，保障低延迟响应与数据安全合规。

七、成绩评定

1. 评分细则

项目	分值	评分标准
完成度	20 分	方向一： 仿真环境与实时检测能力（5） 流式数据处理框架（5） 是否具备自适应学习与模型迭代能力（5） 是否依据多维度特征构建（5）； 方向二： 多维特征库构建（5） 规则引擎与风险定级（5） 对抗样本防御与实时预警（5） 迭代机制与泛终端适配（5）； 方向三： 反诈知识库构建（5） 规则引擎与意图识别（5）

		风险劝阻与举报功能（5） 游戏化交互与泛终端适配（5）
创新性	20 分	解决方案在算法、架构、交互方式等层面的独创性与创新性
实用性	20 分	方案在真实金融环境中的落地可行性、工程化实现程度与业务适配度
成熟度	20 分	系统稳定性、可扩展性、代码与文档规范性
安全性	20 分	全生命周期数据加密、隐私保护措施，系统自身安全防护能力，混合云部署环境下跨平台数据传输、节点运行的安全保障措施
团队表现	10 分（额外加分项）	答辩逻辑清晰度，团队协作默契度，问题应答能力

2. 违规处置

- （1）经查实抄袭或侵犯他人知识产权，取消参赛资格；
- （2）作品及演示材料中出现学校、指导教师姓名或其他赛事标识，取消参赛资格；
- （3）现场演示发生过度人为干预，视情况扣 5-15 分。

3. 统分办法

各评委独立打分后取平均分作为最终成绩。

4. 特殊情况处理（如成绩并列）

若出现成绩并列，优先比较“完成度”得分；若仍并列，比较“创新性”得分。

八、竞赛流程

1. 场地适应

如有需要，可在赛前一日进行场地适应，参赛团队可测试设备及网络环境。

2. 检录规则

参赛团队须携带报名时使用的有效身份证件进行现场核验，未通过检录者不得参赛。

3. 赛场规则

比赛期间禁止使用手机等通讯设备；

禁止与其他团队交流或干扰比赛秩序；

遵守现场工作人员安排。

4. 离场规则

完成答辩及演示后，需整理个人物品并有序离场。

5. 紧急情况

如遇设备故障等突发情况，可向工作人员示意，经确认后给予最多 5 分钟故障处理时间。

九、赛项安全

1. 安全管理

参赛团队需确保作品及演示过程不涉及违法违规内容，不传播虚假信息，不进行网络攻击行为；作品的技术实现与数据使用遵守金融数据安全合规相关要求。

2. 应急预案

现场配备技术支持人员及医疗急救箱；如遇突发公共卫生事件，按组委会统一部署执行

3. 评审保障

（1）评审专家组

组成人员：由大赛专家委员会提名，涵盖高校教授、行业专家、企业技术骨干等。

职责：制定评审标准、审核评审流程、处理评审争议、监督评审执行。

（2）评审工作组

组成人员：由大赛承办单位工作人员、技术支持人员组成。

职责：组织实施评审会议、维护评审系统、记录评审过程、整理评审材料。

（3）监督组

组成人员：由主办单位指派人员、秘书处成员及省级教育主

管单位成员（针对省赛）组成。

职责：监督评审过程是否合规，受理投诉举报，出具监督报告。

十、其他说明

1. 规则最终解释权归组委会所有；
2. 技术细节更新以赛前睿抗官网/公众号发布的为准。