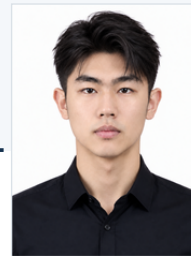


言子奇

AI 全栈应用开发 / Agent 开发 / AI 应用开发 (2027 届本科)

电话 17680232110 | 邮箱 2517468410@qq.com | 个人网站 yanziqi.pages.dev



教育背景 宁德师范学院 · 大数据科学与技术 (本科) 2023.09 — 2027.06

荣誉奖项 中国大学生计算机设计大赛 (大数据应用组) 全国三等奖、福建省一等奖 (2026)

核心技术栈

后端与数据工程: Python (FastAPI / SQLAlchemy / httpx / Pytest)、Node.js (Fastify)、Spring Boot 服务端开发; MySQL 复合索引设计与 EXPLAIN 调优、SQLite 事务持久化、Redis 并发防重锁、Caffeine 进程内缓存、Spark Local、Docker Compose、GitHub Actions 工作流。

前端与全栈协作: Vue 3 复杂状态流转页面 (状态机展示、计划版本 Diff、表单校验)、SSE 流式通信、MediaPipe 浏览器端 33 关键点特征提取; 前后端接口契约设计与联调。

LLM 应用与 Agent 工程: LLM 原生 tools Function Calling (httpx 直连) 与 Cassette 录制回放; RAG 实践 (标题层级分块、BM25 + 向量余弦混合检索、引用校验); Agent 工具调用治理 (鉴权、参数策略、审批、执行指纹、幂等回执、UNKNOWN 对账、审计链); 离线评测基准集、LLM-as-a-Judge 裁判、检索指标与版本回归门禁; 以 Claude / Cursor / Codex 辅助研发。

项目经历

ToolGate 2.0 | Agent 工具执行网关与受控 LLM / RAG 运行时 | 独立开发 2026.09 — 2026.10

技术栈: Python · FastAPI · SQLAlchemy · SQLite · Redis · RAG · Function Calling · GitHub Actions

- 受控工具执行网关:** 场站调价、分层触达、工单关闭等高风险工具调用「鉴权 — 参数策略 — 人工审批 — 执行 — 对账 — 审计」闭环; 参数级三级闸门 ($\leq 15\%$ 放行 / $15\sim 30\%$ 审批 / $> 30\%$ 阻断, 叠加成本底线), 审批绑定参数执行指纹, 参数被改即挂起并告警。
- LLM Agent 运行时:** httpx 直连原生 tools Function Calling, 提交前 Schema 前置校验 (8 类非法输入与身份字段越权全拦); 多轮会话与挂起追问, UNKNOWN 拒绝同目标重试; Cassette 录制回放使评测零真实 Token 消耗。
- RAG 与引用校验:** 6 份运营规范切成 65 个确定性切片, BM25 + 向量余弦混合检索 (典型查询 Top-1 命中 4/4); 编造引用判 unknown、跨文档判 wrong_doc 并转待人工复核 (校验在编排层, 尚未下沉为网关强制门禁)。
- 对抗评测与零回归:** 30 条对抗用例双模式对比, 越权拦截率 $0\% \rightarrow 100\%$ 、期望一致率 $23.3\% \rightarrow 100\%$ 、引用准确率 93.1% ; 全量 329 项测试通过, 138 个源文件 SHA256 比对意外修改为 0、66/66 项验收 ID 完整。

FitAgent | 端侧感知驱动的 AI 健身工作流全栈应用 | 独立开发 2026.09 — 2026.10

技术栈: Vue 3 · Node.js (Fastify) · SQLite · SSE · MediaPipe

- 全栈闭环与验收:** Vue 3 + Fastify + SQLite + SSE 实现「建档 — 体态安全校验 — 方案生成 — 打卡 — 周复盘」本地优先闭环; 138/138 条黑盒业务断言、31 条 HTTP 合约断言与服务重启回查断言通过, 并通过桌面/移动视口构建检查。
- 端侧特征与隐私:** 浏览器本地 MediaPipe 提取静态照片 33 个骨骼关键点, 前置多人、出框、低可见度与视角校验; 服务端仅接收脱敏关键点, 原图不上传、不落盘。
- 人机协同状态流转:** 设计 observed / uncertain / not_observable 三态置信度边界, 观察须用户显式确认才进入计划上下文; 否定与疼痛反馈以追加事件持久化, 计划版本 Diff 链可溯源变化依据。

LearnQA Gate | AI 应用质量评测与发布门禁平台 | 独立开发 2026.09 — 2026.10

技术栈: Python · FastAPI · Vue 3 · LLM-as-a-Judge · 检索指标 · Pytest

- 评测基准与门禁:** 24 条标准任务 + 20 个登记知识来源 + 33 项确定性检查 + 四维复核标准 (正确性、一致性、引用支持、无依据补充), 形成「通过 / 待复核 / 阻断放行」三级发布门禁; 回放候选版本即可复现「通过数上升但新增 blocker」的回归并阻断发布。
- LLM 裁判与检索度量:** LLM-as-a-Judge 四维评分与理由 + A/B 位置交换去偏 (离线对抗用例验证), 裁判只给建议、不参与放行——8 条实盘全部建议 PASS, 本地引用校验仍升级其中 1 条为 BLOCKED; 检索基准 (8 查询 $\times$ 20 来源) Hit@1 87.5%、MRR 0.9375。
- 工程硬化:** 241 项离线测试全绿 (旧版回归子集 124 项可单独复现); 仓储只增、人工复核不能解除 blocker; 评测报告由持久化证据生成并与磁盘逐字节一致。

数据工程与全栈实践 2026.04 — 2026.10

技术栈: Vue 3 · Spring Boot · MySQL · Caffeine · Spark Local

- 长内容工作台 (个人全栈项目):** Vue 3 + Spring Boot + MySQL + Spark Local 构建创作数据治理与分析平台, 白名单统计路由与幂等导入, 结构化 1,010 条来源 / 390 章节 / 382 条复盘记录, 54 项自动化测试通过。
- 数据库与缓存优化:** 99,000 行结构化记录建复合索引后经 EXPLAIN 与 500 次实测: 扫描行数 $99,247 \rightarrow 23$ 、P50 $21.87 \rightarrow 0.32$ ms、吞吐 $43.7 \rightarrow 2,996$ qps; 白名单工具加进程内热点缓存, 命中率 99.90% 。
- Cogniq 可信数据分析系统 (联调与验收):** 参与 Vue 3 与 Spring Boot 核心联调, 梳理「自然语言提问 — 权限约束 — SQL Guard 校验 — 只读执行 — 证据绑定 — 分析报告」可信链路。