潘泽欣

AI 应用开发 / AI Agent 工程师 / 全栈开发

电话：15905096042 / (+852)59886643 | 邮箱：xixizaixi@gmail.com（主）/ xixin9988@gmail.com
GitHub：github.com/xixin9988-sys | 求职状态：离职，可随时到岗；可实习/全职（以课程安排为准）

教育背景

2024.09 – 2027.06 | 漳州科技职业学院 | 人工智能技术应用 | 大专（在读/应届）

主修课程：Python 程序设计、数据结构、Web 开发基础等（以实际修读课程为准）

职业概述

在 Amazon、Ozon 做过电商店铺运营，选品、上架、推广、客服、售后这些环节基本都是自己一个人盯过来的，最清楚哪个环节最耗人力。这两年一边做运营，一边自学 AI 应用开发，想做的就是把这类重复的活交给 AI。

现在主要做 AI Agent 的记忆：一个负责存（NanoMemory），一个负责判断能不能信（mem-guard），再把它们接到电商客服场景（OmniCare）。习惯先把问题和边界写清楚再动手；编码大量借助 Claude Code、DeepSeek Harness，但架构、取舍、测试和验收自己把关。

核心技能

- **AI / Agent 开发：**记忆治理（来源标记、信任等级、隔离区）、MCP 协议、DeepSeek Harness 插件、n8n 工作流、Prompt 写法、Claude Code。
- **后端：**Python 3.11+、FastAPI、Uvicorn、Pydantic v2、REST API、SDK / CLI 开发、pytest 单元测试。
- **前端与可视化：**页面开发、交互设计、API 联调、Three.js 3D 场景。
- **电商业务：**商品、订单、库存、支付、物流、售后、客服、数据运营，知道每个环节容易卡在哪。
- **工程习惯：**先写清需求和接口，再补测试和 README；用 AGI 写代码，但自己负责 review 和验收。

核心开源项目

mem-guard | AI Agent 记忆治理中间件 | 独立设计与实现 | Python

- 做 NanoMemory 的时候发现一个新问题：对话里很多内容其实没用，还有些是模型自己猜的，全存进去，AI 以后就会照着错的东西往下答。所以单独做了一层治理，不去改记忆引擎本身。
- 写入时先看这句话是谁说的，分成 user_verified、user_stated、model_inferred、untrusted 四类，再按信任等级放进共享区、私有区和隔离区。
- 记忆本身有状态（正常、冲突、被取代、已隔离），几条规则互相打架的时候，不自己挑一条，而是升级给人确认。核心链路不依赖 API Key 和向量库，可以离线跑、也可以审计。
- 现在 33 项测试通过。污染率从 0.556 降到 0.0 那组数据是我自己造的合成数据，只能说明机制有效，不代表真实业务里的效果。

NanoMemory ｜ 面向 AI Agent 的长期记忆引擎 ｜ 独立设计与实现 ｜ Python / FastAPI

- 起因很具体：用 Claude Code 和 DeepSeek Harness 写东西，聊久了 token 越烧越多，它还会把前面做的事忘掉。以前的办法是把聊天记录存成 txt，开个新窗口再喂一遍，很折腾。
- 所以做了个本地记忆库：三层记忆（Working / Long-term / Episodic）；检索时把 BM25、字符三元组和关系扩展的分数合起来排，再按 token 预算挑出该交给模型的那一部分。
- 做了 REST API、SDK、CLI、MCP Server（7 个工具）和 Streamlit 面板，用 FastAPI + Pydantic v2 实现，可以直接挂到 Agent 上调用。
- 在我自己指定的数据集和设置下，token 用量比全量历史模式少 67%，事实召回 0.86。这是自测结果，不是通用 benchmark。

omnicare ｜ 电商客服与售后多 Agent 系统 ｜ 独立设计与实现 ｜ Python / FastAPI

- 直接来自以前的电商经验：一家店要人盯着选品、上架、推广、客服和售后，最能吃人力的是客服和退款这两块。
- 把问题拆给不同角色：物流查询、售后、商品咨询各走各的 Agent，上面再有一层路由负责分派，不用一个模型硬答所有事。
- 退款这类动钱的动作不让 AI 自己决定：走状态机 + 额度重算 + 人工审批，谁批的、批多少都留审计记录。
- 48 条接口契约测试在 CI 里跑通（SQLite 与 PostgreSQL 16 两套矩阵）。现在还没接真实支付网关，退款只到记账为止，没有真的把钱打出去。

工作 / 实践经验

电商店铺运营（Amazon / Ozon） ｜ 约 2 年 ｜【公司与起止时间待填】

- 负责店铺日常：选品、上架、listing 和图片、定价、活动、库存与物流跟进，一个人管过整店的节奏。
- 客服与售后：处理咨询、退换货、纠纷和差评，把重复的问题整理成回复模板，后来直接做成了自动化流程。
- 用 n8n + Python 把重复的事自动化：批量整理商品信息、生成文案、汇总数据、按规则触发提醒。
- 数据这块主要看转化、退货率和推广花费，按周复盘再调整。

项目实战

电商自动化流程与 3D 业务可视化 ｜ 全栈 / AI 开发 ｜ n8n / Python / Three.js

- 用 n8n 把 AI 模型、业务接口和数据处理串成工作流，订单、库存、客服这些重复操作改成自动触发。
- Python 侧做编排：调不同模型完成内容生成、数据整理和问答，失败的步骤会重试并记录下来。
- 前端用 Three.js 把 3D 场景和业务数据接起来，做成能点、能看的展示页。

自我评价

从电商一线转过来做 AI 应用，习惯先把「要解决什么」想清楚再写代码，不太喜欢为了堆技术而堆技术。技术是自学的，好处是踩过的坑都记得，也愿意把边界和没做到的地方写出来；不足是经验还在积累，复杂业务和大系统还没独立扛过，所以更想把小系统先做扎实。