李淳

chunli@smail.nju.edu.cn · (+86) 158-0894-8255

教育经历

南京大学, **软件工程 博士研究生** 2022 – 至今

导师 潘敏学（青拔）李宣东（国家杰青） **实验室** 软件工程组（SEG）可信软件实验室（DENSELAB）
荣誉与获奖 南京大学优秀研究生 ×2、移动之光数智创新奖学金、江苏省研究生创新计划、中国电科十四所奖学金 ×2、南京大学博士生校长特别奖学金

南京大学, **软件工程 学士** 2018 – 2022

成绩 GPA 排名前 15% **荣誉与获奖** 优秀毕业生、华为奖学金、华为智能基座奖学金、人民奖学金、花旗杯金融创新大赛第一名、美国大学生数学竞赛 Honorable Mention

研究方向

我的主要研究方向包括软件工程、机器学习与可信人工智能。具体而言，我专注利用**人工智能技术赋能可信软件与软件质量保障（AI4SE）**。目前共发表论文 8 篇，包括 CCF-A 类会议/期刊 5 篇，CCF-B 类会议/期刊 1 篇，其中**第一作者长文 5 篇（包括 4 篇 CCF-A 类，一篇 CCF-B 类）**。

发表/投稿论文

(Under Review, CCF-A, 一作) CurriAgent: A Plan-and-Build Framework with Curriculum Planning for Patch Backporting.

(Under Review, CCF-A, 一作) Automated Classification, Root Cause Analysis, and Repair Recommendations for Failed Mobile Testing by Specialized LLM.

(ICSE 2026, CCF-A, 一作) Learning without Forgetting: Towards Continual Learning of Fault Localization Models in Industrial Software Systems.

(TDSC 2025, CCF-A, 一作) Trap: Mitigating Poisoning-based Backdoor Attacks by Treating Poison with Poison.

(FSE 2025, CCF-A, 一作) Improving Graph Learning-Based Fault Localization with Tailored Semi-Supervised Learning.

(ASE 2024, CCF-A, 二作) DroidCoder: Enhanced Android Code Completion with Context-Enriched Retrieval-Augmented Generation.

(ICSE 2025, CCF-A, 一作) Enhancing Fault Localization in Industrial Software Systems via Contrastive Learning.

(ICASSP 2026, CCF-B, 一作) Attack as Defense: Exploiting Backdoor Trigger Towards Unlearnable Examples.

(QRS 2023, CCF-C, 一作) Mobile Test Script Generation from Natural Language Descriptions.

实习经历

研究实习生, 三星电子（中国）研发中心 2023.09-2023.12

- 研究了一个基于深度学习的故障定位模型训练方法，该模型通过对比学习来挖掘通过日志与失败日志中的特征来进行训练，使得模型可以基于日志来实现系统测试的故障定位。
- 该方法包括从日志中提取图结构的程序语义，对图结构进行数据增强，以及基于图结构的点-图对比学习算法和排序头微调。最后将完整的训练-推理流水线部署在测试系统中。
- 以第一作者的身份发表论文在 CCF-A 类会议 ICSE25（直接接收，仅 9%），并出席会议进行学术报告。

研究工作/项目经历

• 故障定位与自动修复

2025.10-至今 **基于渐进式规划的自动补丁回溯智能体框架** **科研项目**

针对回溯问题的特性，通过提升修复方案的复杂度来渐进式的规划如何将新补丁作用到旧版本的代码上，以此来提升 Agent 在补丁回溯任务上的效率和跨语言的能力。通过 Plan 和 Build 两个 Agent 协作，**相比于 SWE-Agent 基线在单测上通**

过率提升 20%。

2024.06-2025.06 基于 LLM 的移动应用失败测试根本原因分析与修复建议 科研项目

在 **OPPO 真实移动应用失败测试的数据集**上对大模型进行双向 pre-training，SFT 来将领域知识与工程师的推理知识注入大模型，并通过 DPO 优化模型捕捉影响分析结论的上下文关键细节内容，让 LLM 可以自动分析失败测试的根因并给出修复建议。**在 OPPO 测试平台上落地，工程师人工评估模型输出结果准确率达到 80%**

2025.01-2025.08 针对基于日志的故障定位模型的持续学习算法研究 科研项目

软件持续迭代，相应的故障定位模型也需要一起更新。该工作首次开发了专门针对故障定位模型的持续学习框架，来使得模型能够高效的随着软件进行迭代而无需重新训练以及缓解灾难性遗忘。**在三星电视产品线的 8 次真实版本迭代上评估，性能超过最佳基线 27%**。

2024.03-2024.09 针对基于图学习的故障定位模型的半监督学习算法研究 科研项目

基于学习的故障定位模型需要标记大量高质量数据，这本身就是一个耗时耗力的故障定位过程。为了缓解数据标记的成本，该工作首次提出了针对上述场景的半监督学习方法，包括基于注意力机制的图增强与基于高斯混合模型与贝叶斯准则的伪标签估计算法。**在仅 8% 标记样本的场景下超过经典基线方法 14% 到 54%**。

2023.09-2024.02 针对基于日志的故障定位模型的训练算法研究 科研项目

系统测试中工程师往往通过日志来进行故障定位。针对日志中信息多且杂乱的场景，该工作首次提出了基于日志的故障定位模型，通过传递性分析的图增强与对比学习来训练故障定位模型。基于对比学习挖掘通过日志与失败日志中的特征，模型能够识别失败日志中的异常程序行为来实现故障定位。**在三星电视测试平台上线，Top-1 准确率超过 70%**。

• 代码生成

2023.12-2024.06 基于 Android 特性驱动 RAG 和微调来增强代码补全模型 科研项目

利用 Android 开发特性与功能关键词高内聚性增强 RAG 与检索排序，并通过微调让模型更好的利用上下文来，提升 Android 场景下的代码补全的有效性。**使得更小规模的模型在补全性能上超越更强的闭源模型或者其他 RAG 框架**。

2023.01-2023.09 基于移动测试意图与大语言模型来生成移动测试脚本 科研项目

利用大语言模型将测试意图与特定的 UI 控件匹配，并通过一个探索模块来自动补全中间的动作，实现从测试意图生成相应的测试脚本。该工作解决了测试脚本容易因 UI 变化而损坏的问题以及降低了人工编写测试脚本的成本。**将移动应用操作指南以及帮助手册作为评估数据集，超越基线 21%**。

• 模型安全

2024.03-2024.06 基于后门触发器来实现不可学数据集保护隐私 科研项目

由于后门触发器主导样本特征的特性，我们通过插入类感知的后门触发器来构造一个不可学数据集，从而防止个人隐私在模型训练过程中遭到滥用。**该方法在性能，跨数据集，跨模型架构，构造成本，扛防御能力等多个维度均超越现有方法**。

2023.02-2023.10 以毒攻毒来防御深度学习模型中的后门攻击 科研项目

从不可信源爬取的数据可能是攻击者精心设计的含有后门的数据。在不干净的数据上训练模型会使得模型含有安全漏洞。我们设计了一种高效的检测与隔离方式，通过触发器主导的攻击特性来通过聚类识别有毒样本，再通过重标记有毒样本和重训练分类头实现后门隐藏。**在只有 0.33% 的性能损失情况下将后门攻击成功率降低至 0.07%**。

• 软件开发

2020.10-2021.05 Nudger 基于分析师网络的投资组合推荐系统 工程项目

作为后端架构负责人，我负责**定义微服务架构和服务边界**。我还通过 **Redis 集成和 SQL 优化**推动了系统性能的提升，同时实现基于 Jenkins 与 Docker 的**持续集成/持续部署**加速软件开发-部署效率。

技能与兴趣

• **科研兴趣**：关注人工智能（LLM，Agent，DL）驱动的可信软件与质量保障以及深度学习安全问题。关注相关领域前沿工作、热爱学习与拥抱新技术。
• **模型训练**：具有工业真实场景与数据下的深度学习与 LLM 的训练与优化经验（包括预训练，微调，强化学习）。掌握 PyTorch，LlamaFactory 等训练与监控工具。
• **工程落地**：具备独立设计与开发一定规模的科研工具与平台的能力，包括将科研项目或者模型结合到测试平台等。具有 Base-based Agent 开发经验，例如 mini-swe-agent。
• **语言与沟通**：具备较强的软件项目团队协作意识和能力，与实验室多位同学合作展开科研。较好的英语写作及交流能力，可独立进行英语学术写作，阅读英语文档。