胡皓阳

：hhynb@njust.edu.cn ：https://github.com/ALIENHHY ：https://alienhhy.github.io/

教育经历

香港大学 2025.09 – 2026.12

硕士 计算机科学 将于 2025 年 9 月入学 中国香港

南京理工大学 2021.09 – 2025.06

本科 网络空间安全 GPA：85.25/100（前12%） 成绩单链接： 江苏无锡

- 专业技能：Python、C++、工作流、深度学习、机器学习、数据分析与可视化、Linux、网络安全...
- 英语能力：CET-4、CET-6、雅思6.5分，可适应日常交流和文献阅读，能将英语作为工作语言

公开成果

*：这些作者贡献相同，是共同第一作者 C=会议, J=期刊, P=专利, A=其他发表

[C.1] Yican Geng*, **Haoyang Hu***, Zhaoxuan Ge and Zhichao Lian. Network Intrusion Detection Algorithm Based on LightGBM Model and Improved Particle Swarm Optimization. In 2024 IEEE Cyber Science and Technology Congress (CyberSciTech), DOI: 10.1109/CyberSciTech64112.2024.00021

[P.1] 黄婵颖，姚昌济，**胡皓阳**，颜克冬，《一种基于国密算法和联邦学习的新闻推荐方法及系统》，CN118094008A，在审。

[P.2] **胡皓阳**，《一种导盲手杖及其控制方法》，CN111110531A，已授权。

[P.3] **胡皓阳**，《一种导盲手杖》，CN212235240U，已授权。

[A.1] **胡皓阳**，彭真，《人工智能发展的ESG风险与机遇》，腾讯KM，2024年12月。

[A.2] **胡皓阳**，彭真，《人工智能全球治理态势观察》，腾讯KM，2024年11月（被评为“KM好文”）。

项目经历

列举部分

本科毕设：面向文本大模型的威胁性分析研究 2024.11 – 至 今

- 专注于开拓针对大语言模型的高级越狱攻击，优化 TAP 和 PAIR 等算法，实现高效的对抗性提示生成；
- 在本地部署 Ollama 大模型服务，优化攻击策略和算法，使其能够在中文语言模型等复杂环境下发挥作用；
- 开发针对大语言模型越狱攻击的工具包，旨在提高对模型安全研究的理解和能力，并为防御策略提供见解。

AISDR：基于人工智能的药品注册辅助技术研究 2024.06 – 至 今

- 开创性地提出了行业内首个量化的药品注册流程框架，完成了数据收集处理，构建了第一个全面的数据集；
- 利用LLMs进行特征筛选，并结合随机森林等其他机器学习模型得到各阶段和最终的预测结果；
- 结合特征工程和最终结果，设计推荐触发器，为客户在预测失败时提供改进建议；
- 我们以该项目为基础创办了**南京云之秘境科技公司**，目前正专注于撰写高质量学术论文。

OptiCrow：基于机器学习的物联网网络入侵检测系统研究 2024.02 – 2024.09

- 通过 GA 和 PSO 算法对 LightGBM 模型的超参数进行寻优，大幅提升网络入侵流量预测的效率和准确性；
- 将 Levy 飞行等变异算法引入 CSA，同时对 EHO 结果进行二进制化处理，提高全局搜索性能和计算效率；
- 初步研究成果被 CyberSciTech 2024 会议接收，当前正在进行后续深入研究，致力于发表更高质量的论文。

Efficient-FedRec-SM：基于联邦学习与SM算法的新闻推荐系统 2023.09 – 2024.01

- 参与研究生课题项目，专注于保护联邦学习框架中的梯度传输安全；
- 使用国密算法 SM2 和 SM9 对梯度数据进行加密和数字签名，确保数据传输的安全性和完整性；
- 凭借该项目荣获全国密码技术竞赛三等奖，并成功申请发明专利。

SafeGuide：基于计算机视觉的智能导盲杖 2018.09 – 2023.12

- 使用Python和Arduino开发，应用YOLO、时间差等算法，集成障碍识别、避障和报警等多功能；
- 成果已授权一项发明专利和一项实用新型专利，曾多次在竞赛中获奖。

工作经历

南京云之秘境科技有限公司：联合创始人 2024.11 – 至 今

腾讯（深圳）科技有限公司：ESG 协同办公室 2024.09 – 2024.12

- 探索公司AI治理、网络安全和隐私保护方向：
  - 行业洞察与研究：深入研究人工智能治理、网络安全和隐私保护，分析行业趋势和相关公司的同行战略；
  - 数据分析和报告：收集、分析和可视化 ESG 数据，协助起草高质量的分析报告，支持数据驱动型决策；
  - 调研成果分别发表了《人工智能全球治理态势观察》和《人工智能发展的ESG风险与机遇》两篇文章。
- 开发AI驱动的提效工具：
  - 开发工作流日报系统：每日自动收集、筛选信息，生成新闻日报，并发送至同事的邮箱，已投入使用；
  - 开发专业写作 Agent：构建 ESG 知识库，依托腾讯元器平台，训练 ESG 专用写作 Agent，已投入使用；
  - 图像识别：使用 ResNet 实现“鹅民环保行动派”小程序的图片识别功能，积累 5000+ 用户。

中国电信股份有限公司：云网维护中心 2024.01 – 2024.02

四川神琥科技有限公司：技术部 2023.07 – 2023.08

杭州默安科技有限公司：玄甲实验室 2022.07 – 2022.08

获奖情况

列举部分

- 竞赛获奖：
  - 全国大学生数据分析大赛国家级一等奖 2023.12
  - 全国密码技术竞赛国家级三等奖 2023.11
  - “泰迪杯”数据挖掘挑战赛国家级三等奖 2023.06
- 校内荣誉：
  - 南京理工大学优秀学生奖学金一等奖（前4%） 2024.09 & 2024.04
  - 南京理工大学成功奖学金 2024.09
  - 南京理工大学优秀学生干部（1/70） 2024.09 & 2024.04
  - 南京理工大学超越奖学金 2024.05
  - 南京理工大学三好学生（6/70） 2023.11
  - 南京理工大学优秀学生奖学金三等奖（前15%） 2023.09 & 2023.05 & 2022.09

其他

列举部分

- 学生活动：
  - 南京理工大学学生代表大会常任代表 2024.05 – 至 今
  - 南京理工大学 2021 级网络空间安全专业团支部书记 2021.09 – 至 今
  - 南京理工大学网络空间安全学院羽毛球队 & 篮球队成员 2021.09 – 至 今
  - 南京理工大学暑期社会实践活动省级重点项目负责人 2023.07
  - 南京理工大学暑期社会实践活动校级重点项目负责人 2022.07
- 机器人获奖： 我参加过 8 个赛季 VEX-EDR（现在叫 VEX-V5）竞赛
  - 世界机器人大赛 RoboCom 精英赛季军 2018.08
  - 亚洲机器人锦标赛中国区选拔赛 VEX 机器人工程挑战赛亚军 2016.08
  - 世界机器人锦标赛 VEX 机器人工程挑战赛金奖 2016.04
  - 亚洲机器人锦标赛 VEX 机器人工程挑战赛金奖 2015.12
  - 亚洲机器人锦标赛中国区选拔赛 VEX 机器人工程挑战赛总冠军 2015.08