基本信息

姓　　名：欧阳飞　　性　　别：男

籍　　贯：云南省大理州　　出生年月：1995.10

专　　业：计算机科学与技术　　学　　历：博士

研究方向：AI安全，自然语言处理　　兴趣爱好：爬山、羽毛球

邮箱：fei@cqu.edu.cn

教育背景

- **重庆大学**　计算机学院　计算机科学与技术专业　博士研究生　**2020.09~至今**

导师：向涛（计算机学院院长，国家级人才，国重研首席科学家）

- **重庆大学**　计算机学院　计算机科学与技术专业　硕士研究生（转博）　**2018.09~2020.06**

导师：叶春晓（重庆大学先进技术研究院副院长）

- **云南师范大学**　信息学院　计算机科学与技术专业　本科　**2014.09~2018.06**

学术成果

➢ **科研成果**

[1] **F. Ouyang**, D. Zhang, C. Xie, H. Wang, T. Xiang. "LLMBD: Backdoor Defense via Large Language Model Paraphrasing and Data Voting in NLP". Knowledge-Based Systems, 2025.（SCI一区, IF:7.4）

[2] T. Xiang, **F. Ouyang**, D. Zhang, C. Xie, H. Wang. "NLPSweep: A comprehensive defense scheme for mitigating NLP backdoor attacks". Information Sciences, 2024, 661: 120176.（SCI一区，导师一作）

[3] J. Wang, C. Ye, **F. Ouyang**. "Dynamic data access control for multi-authority cloud storage." 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). IEEE, 2019.

[4] J. Wang, K. Wu, C. Ye, X. Xia, **F. Ouyang.** Wang, Jian, et al. "Improving Security Data Access Control for Multi-Authority Cloud Storage." 2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom). IEEE, 2019.

➢ **授权专利**

[5] **欧阳飞**, 叶春晓, 张亚兵, 邢镔. 基于联邦学习的区块链工业物联网数据共享方法: 202011505923.4[P]. 2022-06-24.

[6] 王健,叶春晓,张鑫,陈鑫,**欧阳飞**. 一种基于区块链的云数据安全共享方法: 201811539328.5[P].2023-04-18.

[7] 向涛,邓治伟,**欧阳飞**. 基于充电桩自组网的数据安全访问方法及装置: 202311364892.9[P]. 2024-07-02.

项目经历

◆ **雷鳗智能科技（重庆）有限公司 | 技术负责人** **2023.09.05~至今**

主要工作内容及成果：

主要职责为执行公司技术战略，领导技术团队进行技术选型、架构设计和项目开发，同时进行技术风险管理和对外技术沟通，最终目标是确保技术与业务目标高度吻合，并通过技术创新驱动公司发展。目前已带领技术团队开发完成雷鳗车充、雷鳗家充等商业化运营管理平台。雷鳗车位等停充一体化项目仍在持续开发维护中。

◆ **国家重点研发项目《多媒体大数据的隐私保护技术》 | 项目参与人员** **2022.12.08~2025.11**

主要工作内容及成果：

主要职责为参与重庆大学子课题研究，核心工作为自然语言处理部分的后门防御技术，深入分析了文本后门攻击的机理与特性。针对此，创新性地提出了两种数据驱动且高效的后门检测与防御方法，显著提升了模型的安全性和鲁棒性。研究成果为学术论文2篇，为保障多媒体大数据环境下的文本信息安全贡献了关键技术。

◆ **绿盟科技成都分公司昆明办事处 | 安全运维人员** **2017.08.01~2017.10.30**

主要工作内容及成果：

主要职责为中国移动云南省公司驻场，参与网络安全管理部门的日常安全运维工作，协助云南农业大学等高校服务器安全审查测试。在国家重大会议期间，保障移动公司及旗下所有服务器、网站正常运行，确保网络及其服务不受攻击。完成了多台服务器极其服务安全审计工作。

荣誉技能

- ✧ 获得研究生推免资格（保送研究生）
- ✧ CISCO 认证 CCNA
- ✧ Oracle 认证 OCA(11g)、OCP(11g)
- ✧ 软件水平考试（中级网络工程师）
- ✧ ISCCC 认证信息安全保障人员
- ✧ 良好的学术论文写作能力与项目文档撰写能力
- ✧ 良好的团队管理、项目管理能力
- ✧ 科研项目编程：Python语言、Pytorch算法框架
- ✧ 商业平台开发语言：java语言、Typescript语言等
- ✧ 熟悉人工智能安全、自然语言处理中的后门等相关算法

自我评价

- **专业背景**：本硕博都为计算机专业，具有较扎实的基础，可以快速适应新的工具和技术。
- **综合品质**：注重细节，有较强的学习能力和抗压能力，在工作中责任心强。
- **科研能力**：具备独立分析解决问题的能力，关注前沿技术，注重研究的创新性与实用性。
- **技术实践**： 熟练掌握人工智能相关算法库，具备将算法转化为代码的实践能力。