方帅举

性　　别：男　　出生日期：1999 年 05 月

电　　话：17719142965　　邮　　箱：fangsj_study@163.com

期望城市：深圳　　意向岗位：大模型、网络安全相关

教育经历

2022.09-2025.6　　**河南科技大学**　　**计算机科学与技术-硕士**

主修课程：高级计算机网络、高级算法设计与分析、高级计算机系统结构、大数据技术分析、可信计算技术、神经网络与应用、图像处理与分析等。

2018.09-2022.07　　**鲁东大学**　　**地理信息科学-本科**

主修课程：地理信息系统、遥感数字图像处理、算法与数据结构、C++、GIS 软件设计、空间数据库等。

项目经历

2022.09—2023.05　　“晒我的”APP 开发

项目描述：

”晒我的“是河南省网络空间安全应用国际联合实验室自主研发的，专注科技成果第三方服务的公共服务平台。该平台承担公共服务职能以及虚假信息传播控制、社交机器人检测、多模态虚假信息检测、多模态敏感信息识别等科研项目的实验平台。

项目职责：

1. 系统开发：负责”晒我的“软件即时通信系统设计与实现、视频模块总体设计与实现、主题模块设计与实现、推荐系统设计与实现、算法嵌入等开发功能；
2. 系统运维：负责”晒我的“软件整体运行、维护、监管等日常维护内容。

2023.06—2025.03　　工业互联网软件系列设计与实现

项目描述：

针对工业互联网安全的系列软件（包括网站、PC 软件、Android、IOS），读取当前局域网多种设备及流量信息，通过嵌入多种算法模型，实现对局域网内各设备的安全防护。

项目职责：

1. 系统开发：负责”雒盾·工业互联网“软件原型系统设计与实现；
2. 项目管理：负责”雒盾·工业互联网“软件整体进度监管、人员分工安排；
3. 项目配置：负责”雒盾·工业互联网“APP 端详细页面设计、服务器配置、数据库配置等。

2024.10—2025.03　　大模型安全检测平台设计与实现

项目描述：

针对大模型安全问题，提出多种防御策略，包括多模态大模型内容安全检测、大模型内生安全检测等功能，实现对多模态大模型的安全保护及风险管理。

项目职责：

1. 系统开发：负责”大模型安全检测平台“原型系统设计与实现、多模态深度伪造内容检测；
2. 项目管理：负责”大模型安全检测平台“整体进度监管、人员分工安排；
3. 项目配置：负责”大模型安全检测平台“详细页面设计、服务器配置、数据库配置等。

科研成果

论文：

”Deepfake detection model combining texture differences and frequency domain information”投稿期刊“ACM Transactions on Privacy and Security”（**CCF 网络与信息安全 B 类**）（录用）

“Deepfake video detection based on multi identity internal aggregation”投稿期刊“IEEE Transactions on Dependable and Secure Computing”（**CCF 网络与信息安全 TOP A 类**）（修回）

专利：

①一种基于注意力金字塔卷积神经网络的渗漏油识别方法（公开号：CN118411506A）。
②一种基于思维链的大语言模型迁移对抗攻击方法及系统（公开号：CN118796981A）。
③一种融合空域纹理差异和频域信息的深度伪造检测方法（公开号：CN118411506A）。
④一种多身份内部聚合的深度伪造视频检测方法。（公开号：CN120125978A）

省级课题：

2023.06—2024.3　　深度伪造图像检测系统设计与实现

一套深度伪造图像检测系统，通过植入至社交平台，对用户发布图像内容进行检测，如果涉及深度伪造，通知后台管理员进行相应操作。

2024.01—2024.07　　视觉表象弱变化下变压器早期渗漏油检测方法研究（河南省科技攻关项目）

一项针对变压器早期渗漏油检测的河南省科技攻关项目，通过设计相应算法模型，识别工业场景下变压器早期的渗漏油，并产生相应科研成果（专利、论文）。

2024.01—至今　　多模态大模型安全检测与对抗防御关键技术研发及示范化应用（河南省重点研发专项项目）

一项针对多模态大模型安全的河南省重点研发专项项目，通过多家单位联合（河南科技大学、新华三、河南师范大学），对多模态大模型的多种安全问题及对抗防御关键技术进行研究，并产出相应科研成果（专利、论文）。

2024.04—至今　　深度伪造图像检测系统设计与实现

针对深度伪造视频的检测系统，通过植入至社交平台，对用户发布视频内容进行检测，如果涉及深度伪造，通知后台管理员进行相应操作。

竞赛成果

2024 年 10 月 作为团队负责人参加“众智-2024”（信息发布方：国防科技创新快速响应办公室）获得国家级奖项
2024 年 7 月 作为团队负责人参加中国国际大学生创新创业大赛进入推荐省赛
2023 年 11 月 参加"华为杯"第二届中国研究生网络安全创新大赛创意作品赛获得国家级奖项
2023 年 6 月 作为团队负责人参加第十届"挑战杯"获得河南科技大学校级奖项

奖项荣誉

2025 年 6 月 河南科技大学校优秀硕士论文
2024 年 9 月 河南科技大学研究生一等奖学金
2023 年 12 月 河南科技大学优秀班干部
2023 年 9 月 河南科技大学研究生一等奖学金
2022 年 12 月 河南科技大学优秀班干部
2022 年 9 月 河南科技大学研究生一等奖学金
2022 年 6 月 鲁东大学优秀应届毕业生

专业技能

专业知识：掌握大模型工作原理，熟悉机器学习、深度学习基础知识，了解数据结构基础知识。
开发知识：精通 python 语言、pytorch 开发框架，掌握 Ollama+RAGFlow 本地模型、知识库部署方式；熟悉 LangChain 框架、LCEL 表达式构建链式工作流，具备多 Agent 系统应用经验。了解 LangChain+向量数据库（FAISS）集成实现 RAG 方案，能独立开发基于 LangChain 的简易 AI 应用原型；熟悉 Java 语言、C#后端开发语言、MySQL 数据库等。
网安知识：理解网络安全原理、网络攻防技术、信息安全管理等基础知识，熟悉常见的网络攻击手段与防御策略，了解网络安全工具的使用，熟悉大模型安全威胁及防御策略。
外语能力：英语四级

自我评价

- 逻辑思维能力强，能够快速分析和归纳复杂问题并提出有效解决方案。
- 具备较强的规划和统筹能力，有较强的执行能力，能够高效安排工作并确保任务按时完成。
- 对技术有浓厚兴趣，喜欢追踪行业最新动态，积极学习新技能并应用实践。
- 性格坚韧、执行力强，勇于面对一切挑战，确保目标达成。