宋颖

出生年月：2004-3-15 · **政治面貌：中共预备党员**
手机：18081214369 · **邮箱：**songying_@stu.scu.edu.cn

教育背景

四川大学 - 网络空间安全专业 - 本科 2022.09 - 2026.06

- GPA：3.70/4.0　　排名：35/161（22%）
- 英文能力：599（CET6）
- 主修课程：应用密码学（93）、数据结构与算法（91）、离散数学（91）、线性代数（91）等

科研经历

Secure Federated Learning via Knowledge Distillation and Secret Sharing: A Dual-Server Collaborative Framework

第一作者

- 研究提出了一种融合知识蒸馏与秘密分享的安全高效联邦学习框架，构建双服务器半诚实信任模型，支持在模型异构与数据异构场景下的隐私保护本地训练与安全聚合，采用布尔秘密分享、相关不经意传输（COT）与高效比特组合机制实现全局模型更新。在 MNIST、EMNIST、CIFAR-10 与 CIFAR-100 数据集上的实验结果表明，该框架在准确性、隐私保护和通信效率方面具有显著优势，适用于实际的边缘计算场景。
- 独立开展相关领域文献调研，系统分析现有联邦学习方法的性能瓶颈与隐私风险，主导核心框架设计与实现，统筹论文撰写与项目推进；组织并参与多轮实验设计与参数调优，与成员协作完成多数据集实验验证与论文初稿撰写。

项目经历

大学生创新创业项目

信息物理系统中恶意软件传播的动力学行为及其混合控制策略研究 2023.10 - 2024.08

- 项目针对现有 CPS 恶意软件传播模型忽略感染率动态增强的缺陷，深入研究其传播动力学行为并提出创新性 SIZORS 模型（双感染率）及参数扰动与记忆反馈结合的混合控制策略，经仿真验证可有效抑制系统混沌、确保关键平衡点稳定性；成果为设计高安全 CPS 提供理论支撑，可应用于网络安全（威胁快速处置）及智能工业（风险预防）。
- 项目主要成员，负责项目文书撰写与校验，确保项目文档规范、准确、美观；与团队密切配合，积极参与团队学术研讨与方案评审，推动模型优化与策略改进。

实训项目

智能主机威胁监测与响应平台 2025.06 - 2025.06

- 项目开发了一套企业级主机威胁感知系统，采用平台端与客户端协同架构，构建全方位的主机安全防护体系。基于 Spring Boot 搭建高可用平台，集成 Redis、RabbitMQ、MyBatisX 及 PageHelper 优化性能，支撑主机数据高效处理。核心功能涵盖四大模块，融合 AI 技术智能评估风险，实现资产动态监控、风险主动预警、日志异常识别及基线合规自动化检测。
- 负责风险探测、日志审计等模块的后端开发，提供展示支持以清晰呈现探测信息，并接入 AI 辅助分析系统；参与基线检测后端及规则库接口开发，助力构建完善体系。

校园经历

网络空间安全学院团委学生会，权益部干事 2022.10 - 2023.6

- 在职期间参与策划并执行学院内外的多项权益活动，包括网络安全宣传周、学生权益讲座等。作为团队成员，与学生会其他部门紧密合作，协调资源，锻炼了跨部门沟通和团队合作能力。

奖励荣誉

- 大学生创新创业大赛国家级优秀结题 2024
- 四川大学单项一等奖学金 2023、2024
- 四川大学“优秀学生” 2024