

曹思聪 (Sicong Cao)

151-9597-1698 sicongcao1996@gmail.com



个人简介

曹思聪, 男, 江苏泰州人, 中共党员, 扬州大学信息工程学院(人工智能学院)博士, 师从扬州大学信息工程学院(人工智能学院)院长、博士生导师**孙小兵教授**, 主要研究方向为人工智能、软件工程(AI4SE)与网络安全(AI4Sec)的交叉领域, 重点关注基于深度学习的软件漏洞检测相关技术(DL4Vul), 目前共发表**CCF推荐期刊/会议14篇**, 其中以第一/通讯作者身份发表**CCF-A/中科院1区Top期刊论文5篇**, **CCF-A会议论文6篇**, 包括软件工程顶级会议**ICSEx3, ASEx2**与信息安全顶级会议**S&P**, 获得**BlockSys 2023最佳论文奖**, 授权发明专利**4件**, 谷歌学术累计引用**547次**(单篇被引超过**200次**), 2023年受中国国家留学基金委(CSC)资助在新加坡管理大学进行博士联合培养, 合作导师为**IEEE/ACM/ASE Fellow, David Lo**(谷歌学术累计引用39519次, h-index 104).

教育经历

新加坡管理大学(Singapore Management University)	2023.10 – 2024.09
软件工程 联合培养(导师David Lo) School of Computing and Information Systems	新加坡
扬州大学	2019.09 – 2025.06
软件工程 博士(硕博连读) 信息工程学院(人工智能学院)	江苏 扬州
南京工程学院	2015.09 – 2019.06
软件工程 本科 计算机科学与技术学院	江苏 南京

实习经历

蚂蚁集团(安全非攻实验室)-高级安全工程师	2022.04 – 2022.06
研究课题: JAVA开放式动态反序列化Gadget Chains自动化挖掘	

获奖情况

• 扬州大学学业先锋	2024.11
• 中国软件大会-软件缺陷自动修复挑战赛竞赛二等奖	2024.11
• 第六届“华为杯”中国研究生人工智能创新大赛全国二等奖	2024.09
• ACM SIGSOFT CAPS, ASE'24	2024.09
• 第九届中国高校计算机大赛(C4)-网络技术挑战赛全国 特等奖	2024.09
• ACM SIGSOFT CAPS, ICSE'24	2024.02
• 扬州大学十佳研究生学术创新之星	2024.01
• 扬州大学博士研究生学术新人奖	2023.12
• 扬州大学校长特别奖学金(x2)	2023, 2024
• 研究生国家奖学金(x2)	2023, 2024
• CCF-蚂蚁科研基金优秀应用项目	2023.10
• 第八届中国高校计算机大赛(C4)-网络技术挑战赛全国 一等奖	2023.09
• 第五届“华为杯”中国研究生人工智能创新大赛全国三等奖	2023.09
• BlockSys'23-最佳论文奖	2023.08
• 扬州大学无锡“芯享”奖学金	2022.11
• 中国软件大会-软件研究成果原型系统竞赛(命题型)二等奖	2020.11

代表性工作(*通讯作者)

- 曹思聪, 孙小兵, 薄莉莉, 吴潇雪, 李斌, 陈厅, 罗夏朴, 张涛, 刘维. “基于结构感知图神经网络的多类别漏洞检测方法.” 软件学报, 2025. (**CCF推荐计算领域高质量科技期刊T1类**)
- Xin Zhou, Sicong Cao*, Xiaobing Sun, and David Lo. “Large Language Model for Vulnerability Detection and Repair: Literature Review and the Road Ahead.” *ACM Transactions on Software Engineering and*

Methodology (TOSEM), 2025. (CCF-A, 软件工程顶级期刊)

- Sicong Cao, Xiaobing Sun, Xiaoxue Wu, David Lo, Lili Bo, Bin Li, Xiaolei Liu, Xingwei Lin, and Wei Liu. “Snopy: Bridging Sample Denoising with Causal Graph Learning for Effective Vulnerability Detection.” in *Proceedings of the 39th ACM/IEEE International Conference on Automated Software Engineering (ASE)*, 2024. (CCF-A, 软件工程顶级会议)
- Xiaobing Sun, Xingan Gao, Sicong Cao*, Lili Bo, Xiaoxue Wu, and Kaifeng Huang. “1+1>2: Integrating Deep Code Behaviors with Metadata Features for Malicious PyPI Package Detection.” in *Proceedings of the 39th ACM/IEEE International Conference on Automated Software Engineering (ASE)*, 2024. (CCF-A, 软件工程顶级会议)
- Sicong Cao, Xiaobing Sun, Xiaoxue Wu, David Lo, Lili Bo, Bin Li, and Wei Liu. “Coca: Improving and Explaining Graph Neural Network-Based Vulnerability Detection Systems.” in *Proceedings of the 46th IEEE/ACM International Conference on Software Engineering (ICSE)*, 2024. (CCF-A, 软件工程顶级会议)
- Sicong Cao, Biao He, Xiaobing Sun, Yu Ouyang, Chao Zhang, Xiaoxue Wu, Ting Su, Lili Bo, Bin Li, Chuanlei Ma, Jiajia Li, and Tao Wei. “ODDFuzz: Discovering Java Deserialization Vulnerabilities via Structure-Aware Directed Greybox Fuzzing.” in *Proceedings of the 44th IEEE Symposium on Security and Privacy (IEEE S&P)*, 2023. (CCF-A, 网络与信息安全顶级会议)
- Sicong Cao, Xiaobing Sun, Xiaoxue Wu, Lili Bo, Bin Li, Rongxin Wu, Wei Liu, Biao He, Yu Ouyang, and Jiajia Li. “Improving Java Deserialization Gadget Chain Mining via Overriding-Guided Object Generation.” in *Proceedings of the 45th IEEE/ACM International Conference on Software Engineering (ICSE)*, 2023. (CCF-A, 软件工程顶级会议)
- Sicong Cao, Xiaobing Sun, Lili Bo, Rongxin Wu, Bin Li, Xiaoxue Wu, Chuanqi Tao, Tao Zhang, and Wei Liu. “Learning to Detect Memory-Related Vulnerabilities.” *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 2023. (CCF-A, 软件工程顶级期刊)
- Sicong Cao, Xiaobing Sun, Lili Bo, Rongxin Wu, Bin Li, and Chuanqi Tao. “MVD: Memory-related Vulnerability Detection Based on Flow-Sensitive Graph Neural Networks.” in *Proceedings of the 44th IEEE/ACM International Conference on Software Engineering (ICSE)*, 2022. (CCF-A, 软件工程顶级会议)

🏢 发明专利

• 数据驱动的内存泄漏智能化检测方法及系统	ZL202110569646.1
• 可解释性的软件漏洞检测与推荐方法及系统	ZL202011131831.4
• 基于图神经网络的漏洞识别与预测方法、系统、计算机设备和存储介质	ZL202010053062.4
• 基于强化学习的Java反序列化漏洞检测系统及方法	ZL202111629096.4

🔧 科研项目

• 国家留学基金委-博士联合培养项目(202308320436)	2023.09 – 2024.08
基于深度学习的漏洞检测技术及其可解释性研究	主持人
• 扬州大学研究生院-博士研究生参加国际学术会议资助基金	2023.05
45th IEEE/ACM International Conference on Software Engineering (ICSE), 墨尔本	主持人
• 江苏省教育厅-江苏省研究生科研创新计划(KYCX22_3502)	2022.04 – 2024.04
基于深度学习的软件漏洞检测可解释性关键技术研究	主持人
• 国家自然科学基金委员会-青年科学基金项目(62202414)	2023.01 – 2025.12
基于多模态知识图谱的软件漏洞检测关键技术研究	主要参与人
• 国家自然科学基金委员会-面上项目(61972335)	2020.01 – 2023.12
知识驱动的软件缺陷分析与理解关键技术研究	主要参与人
• 国家自然科学基金委员会-面上项目(61872312)	2019.01 – 2022.12
基于知识探索的软件缺陷智能化修复关键技术研究	主要参与人
• CCF-蚂蚁科研基金(CCF-AFSGRF20210022)	2021.11 – 2022.10

学术报告

- Snopy: Bridging Sample Denoising with Causal Graph Learning for Effective Vulnerability Detection, 39th IEEE/ACM International Conference on Automated Software Engineering (ASE), 美国 萨克拉门托(线上), 口头报告, 2025.10
- Coca: Improving and Explaining Graph Neural Network-Based Vulnerability Detection Systems, TruX Open Online Seminars (TOOS), 卢森堡 卢森堡大学(线上), 口头报告, 2024.07
- Coca: Improving and Explaining Graph Neural Network-Based Vulnerability Detection Systems, 46th IEEE/ACM International Conference on Software Engineering (ICSE), 葡萄牙 里斯本(线上), 口头报告, 2024.04
- Coca: Improving and Explaining Graph Neural Network-Based Vulnerability Detection Systems, CCF软件工程专委会-ICSE 2024论文预讲会, 中国 线上, 口头报告, 2024.02
- ODDFuzz: Discovering Java Deserialization Vulnerabilities via Structure-Aware Directed Greybox Fuzzing, 44th IEEE Symposium on Security and Privacy (IEEE S&P), 美国 旧金山(线上), 口头报告, 2023.05
- Improving Java Deserialization Gadget Chain Mining via Overriding-Guided Object Generation, 45th IEEE/ACM International Conference on Software Engineering (ICSE), 澳大利亚 墨尔本, 口头报告, 2023.05
- Improving Java Deserialization Gadget Chain Mining via Overriding-Guided Object Generation, 2023年扬州大学“智能软件与安全”研究生国际学术创新论坛, 中国 扬州, 口头报告, 2023.03
- 数据驱动的软件漏洞检测, 2022 CCF 中国软件大会(ChinaSoft)-优秀博士生论坛, 中国 上海(线上), 口头报告, 2022.11
- MVD: Memory-related Vulnerability Detection Based on Flow-Sensitive Graph Neural Network, 44th IEEE/ACM International Conference on Software Engineering (ICSE), 美国 匹兹堡(线上), 口头报告, 2022.05

学术服务

- | | |
|--|---------|
| • EuroS&P 2025 PC Member | CCF-C会议 |
| • FSE 2025 外部审稿人 | CCF-A会议 |
| • MSR 2025 PC Member | CCF-C会议 |
| • ASE 2024 PC Member | CCF-A会议 |
| • CCS 2024 外部审稿人 | CCF-A会议 |
| • FSE 2024 注册主席、外部审稿人 | CCF-A会议 |
| • ICSE 2025 PC Member | CCF-A会议 |
| • IEEE Transactions on Software Engineering (TSE) 审稿人 | CCF-A期刊 |
| • ACM Transactions on Software Engineering and Methodology (TOSEM) 审稿人 | CCF-A期刊 |
| • IEEE Transactions on Dependable and Secure Computing (TDSC) 审稿人 | CCF-A期刊 |
| • IEEE Transactions on Information Forensics and Security (TIFS) 审稿人 | CCF-A期刊 |