Jian Cui

cuijian0819.github.io

(last update: August 22, 2025)

EDUCATION

University of Illinois Urbana–Champaign (UIUC) *Aug. 2025 – Present*
Ph.D. Student in Computer Science

Indiana University Bloomington (IUB) *Aug. 2023 – Aug. 2025*
Ph.D. Student in Computer Science

Korea Advanced Institute of Science and Technology (KAIST) *Mar. 2015 – Feb. 2022*
B.S. & M.S. in Electrical Engineering

RESEARCH INTEREST

Security & Privacy of Agentic AI, Data-driven Security, AI for Security

PUBLICATION

1. **Jian Cui***, Mingming Zha*, Xiaofeng Wang, Xiaojing Liao
   The Odyssey of `robots.txt` Governance: Measuring Compliance Implications of Web Crawling Bots in Large Language Model Services *(to appear)*
   The ACM Conference on Computer and Communications Security (CCS'25)

2. **Jian Cui**, Hanna Kim, Eugene Jang, Dayeon Yim, Kicheol Kim, Jinwoo Chung, Yongjae Lee, Seungwon Shin, Xiaojing Liao
   Tweezers: A Framework for Security Event Detection via Event Attribution-centric Tweet Embedding
   The Network and Distributed System Security Symposium (NDSS'25)

3. Zilong Lin, **Jian Cui**, Xiaofeng Wang, Xiaojing Liao
   Malla: Demystifying Real-world Large Language Model Integrated Malicious Services
   The 33rd USENIX Security Symposium (USENIX Sec'24)
   *Top15 finalist in the CSAW Best Applied Research Paper Competition, 2024

4. Eugene Jang, **Jian Cui**, Youngjin Jin, Dayeon Yim, Jinwoo Chung, Yongjae Lee, Seungwon Shin
   Ignore Me But Don't Replace Me: Utilizing Non-Linguistic Elements for Pretraining on the Cybersecurity Domain
   Annual Conference of the North American Chapter of the Association for Computational Linguistics (NAACL'24 Findings)

5. Hanna Kim, **Jian Cui**, Eugene Jang, Chanhee Lee, Yongjae Lee, Jinwoo Chung, Seungwon Shin
   DRAINCLoG: Detecting Rogue Accounts with Illegally-obtained NFTs using Classifiers Learned on Graphs
   ISOC Network and Distributed System Security Symposium (NDSS'24)

6. Youngjin Jin, Eugene Jang, **Jian Cui**, Jinwoo Chung, Yongjae Lee, Seungwon Shin
   DarkBERT: A Language Model for the Dark Side of the Internet
   The 61st Annual Meeting of the Association for Computational Linguistics (ACL'23)

7. **Jian Cui**, Kwanwoo Kim, Seung Ho Na, and Seungwon Shin
   Meta-Path-based Fake News Detection Leveraging Multi-level Social Context Information
   31st ACM International Conference on Information and Knowledge Management (CIKM'22)

8. Taejune Park, Myoungsung You, **Jian Cui**, Youngjin Jin, and Seungwon Shin
   MECaNIC: SmartNIC to Assist URLLC Processing in Multi-Access Edge Computing Platforms
   The 30th IEEE International Conference on Network Protocols (ICNP'22)

9. Zichuan Li*, **Jian Cui***, Xiaojing Liao, Luyi Xing
   Les Dissonances: Cross-Tool Harvesting and Polluting in Multi-Tool Empowered LLM Agents
   (under review)

10. **Jian Cui**, Zichuan Li, Luyi Xing, Xiaojing Liao
    Safeguard-by-Development: A Privacy-Enhanced Development Paradigm for Multi-Agent Collaboration Systems
    (under review)

PROFESSIONAL EXPERIENCE

Applied Scientist Intern (*Host: Pranav Garg, Shweta Garg***)**
AWS AI, United States *May. 2024 - Aug. 2024*

Research Intern
S2W Inc., South Korea *Feb. 2022 - June. 2023*

INVITED TALK

Towards Trustworthy Agent Development Framework: From Attacks to Defenses
Palo Alto Networks, United States *Aug. 2025*

ACADEMIC ACTIVITIES & SERVICES

Program Committee, NDSS Workshop on AI System with Confidential Computing (AISCC'24)

Reviewer, IEEE Transactions on Information Forensics and Security (TIFS'24)

Reviewer, Computers & Security (2024)

Artifact Evaluation Committee, USENIX Security Symposium (Security'24, Security'25)

Artifact Evaluation Committee, ACM Conference on Computer and Communications Security (CCS'24)

External Reviewer, ACM Conference on Computer and Communications Security (CCS'24, CCS'25)

External Reviewer, The Web Conference (TheWebConf'24)

External Reviewer, IEEE Symposium on Security and Privacy (IEEE S&P'24, S&P'25)

External Reviewer, IEEE European Symposium on Security and Privacy (EuroS&P'24, EuroS&P'25)

External Reviewer, USENIX Workshop on Automotive and Autonomous Vehicle Security (VehicleSec'25)

Volunteer, ACM Conference on Computer and Communications Security (CCS'25)

HONORS AND AWARDS

1st Place – Safety Track, UC Berkeley RDI AgentX Competition *Aug. 2025*

The Internet Society NDSS Symposium Fellowship *Feb. 2025*

2nd Place – Safety Track, Berkeley RDI LLM Agents Hackathon *Feb. 2025*

Indiana University Luddy Doctoral Summer Fellowship *Aug. 2023*

The 2023 Korea Financial Security Institute Paper Award *Oct. 2023*

The 2023 Korea Cyber Security Paper Award *Sept. 2023*

The 27th Samsung Humantech Paper Award *Feb. 2021*

TEACHING

Teaching Assistant
KAIST TS251: Data Science Overview *Spring 2020, Spring 2021*

LANGUAGE SKILLS

Chinese (Mandarin), Korean: Native

English: Professional