Jian Cui

cuijian0819.github.io

(last update: November 22, 2024)

Email: leesoo200823@gmail.com

Mobile: +1-812-360-8671

EDUCATION

Indiana University Bloomington — *Aug. 2023 - Now*
Ph.D. Program in Computer Science
- Advisor: *Xiaojing Liao*

Korea Advanced Institute of Science and Technology — *Mar. 2020 - Feb. 2022*
M.S. in Electrical Engineering
- Advisor: *Seungwon Shin*

Korea Advanced Institute of Science and Technology — *Aug. 2015 - Feb. 2020*
B.S. in Electrical Engineering

RESEARCH INTEREST

LLM Security & Privacy, AI for Security, Data-driven Security

PUBLICATION

1. **Jian Cui**, Hanna Kim, Eugene Jang, Dayeon Yim, Kicheol Kim, Jinwoo Chung, Yongjae Lee, Seungwon Shin, Xiaojing Liao
   Tweezers: A Graph-based Security Event Detection Framework on Twitter
   The Network and Distributed System Security Symposium (NDSS'25)

2. 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

3. 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)

4. 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)

5. 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)

6. **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)

7. 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)

8. Jinho Choi, Taehwa Lee, Kwanwoo Kim, Minjae Seo, **Jian Cui**, and Seungwon Shin
Discovering Message Templates on Large-scale Bitcoin Abuse Reports using a Two-fold NLP-based Clustering Method
Institute of Electronics, Information and Communication Engineers (IEICE letter)

9. **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
(under review)

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

PROFESSIONAL EXPERIENCE

Research Assistant
Indiana University Bloomington, United States *Aug. 2023 - Now*

- *LLM Agent Security*: Conducting research on security and privacy issues in LLM agents, with an emphasis on the security implications of tool integration and usage.
- *Privacy Compliance of LLM*: Conducting research on privacy compliance in LLM, focusing on the proper use of web data in LLM training.

Applied Scientist Intern
AWS AI, United States *May. 2024 - Aug. 2024*

- *Security of LLM for Code Generation*: Investigating security vulnerabilities in AI-powered coding assistants leveraging the Retrieval-Augmented Generation (RAG) mechanism, with a focus on Denial-of-Response (DoR) attacks that cause LLMs to reject legitimate user queries.

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

- *Security Language Model Pre-training*: Pre-train the Darkweb- and the security-oriented language models, and apply them to many practical use cases, such as noteworthy forum thread detection, security-related Named Entity Recognition (NER), etc.
- *NFT Scam Detection*: Developed a Graph Neural Network (GNN)-based framework to detect scams by capturing complex NFT transaction patterns and user relationships.
- *Security Event Detection in Twitter*: Developed a novel graph-based framework for robust and effective security event detection, using contrastive learning based approach.

Research Assistant
KAIST, South Korea *May. 2020 - Dec. 2021*

- *Fake News Detection*: Proposed an advanced framework integrating multi-level social context and temporal user engagement data for enhanced end-to-end fake news detection.
- *FPGA-based Network Schedular*: Studied Software-defined Network (SDN) and implemented hardware-based networking scheduler in the NetFPGA using Verilog.

ACADEMIC ACTIVITIES & SERVICES

Program Committee

- NDSS Workshop on AI System with Confidential Computing (AISCC), 2024

Reviewer

- IEEE Transactions on Information Forensics and Security (TIFS), 2024
- Computer & Security, 2024

Artifact Evaluation Committee

- USENIX Security Symposium, 2024
- ACM Conference on Computer and Communications Security (CCS), 2024

External Reviewer

- ACM Conference on Computer and Communications Security (CCS), 2024
- The Web Conference (TheWebConf), 2024
- IEEE Symposium on Security and Privacy (IEEE S&P), 2024, 2025
- IEEE European Symposium on Security and Privacy (EuroS&P), 2024, 2025

Volunteer

- ACM Conference on Computer and Communications Security (CCS), 2024

HONORS AND AWARDS

Indiana University Luddy Doctoral Summer Fellowship *Aug. 2023*

The 2023 Korea Financial Security Institute Paper Award *Oct. 2023*
"DRAINCLoG: Detecting Rogue Accounts with Illegally-obtained NFTs using Classifiers Learned on Graphs"

The 2023 Korea Cyber Security Paper Award *Sept. 2023*
"A Graph-based Clustering Framework for Multi-Label Security Event Detection on Twitter"

The 27th Samsung Humantech Paper Award *Feb. 2021*
"MECaNIC: SmartNIC to Assist URLLC Processing in Multi-Access Edge Computing Platforms"

The 2020 Korea Cyber Security Paper Award *Sept. 2020*
"CENSor: Detecting Illicit Bitcoin Operation via GCN-based Hyperedge Classification"

TEACHING

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

LANGUAGE SKILLS

Chinese (Mandarin), Korean: Native

English: Professional