Jian Cui

cuijian0819.github.io
(last update: July 10, 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

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

PUBLICATION

- **Malla: Demystifying Real-world Large Language Model Integrated Malicious Services**
  *Zilong Lin, **Jian Cui**, Xiaofeng Wang, Xiaojing Liao*
  The 33rd USENIX Security Symposium **(USENIX Security 2024)**
- **Ignore Me But Don't Replace Me: Utilizing Non-Linguistic Elements for Pretraining on the Cybersecurity Domain**
  *Eugene Jang, **Jian Cui**, Youngjin Jin, Dayeon Yim, Jinwoo Chung, Yongjae Lee, Seungwon Shin*
  Annual Conference of the North American Chapter of the Association for Computational Linguistics **(NAACL 2024 Findings)**,
- **DRAINCLoG: Detecting Rogue Accounts with Illegally-obtained NFTs using Classifiers Learned on Graphs**
  *Hanna Kim, **Jian Cui**, Eugene Jang, Chanhee Lee, Yongjae Lee, Jinwoo Chung, Seungwon Shin*
  The Network and Distributed System Security Symposium **(NDSS 2024)**
- **DarkBERT: A Language Model for the Dark Side of the Internet**
  *Youngjin Jin, Eugene Jang, **Jian Cui**, Jinwoo Chung, Yongjae Lee, Seungwon Shin*
  The 61st Annual Meeting of the Association for Computational Linguistics **(ACL 2023)**
- **Meta-Path-based Fake News Detection Leveraging Multi-level Social Context Information**
  ***Jian Cui**, Kwanwoo Kim, Seung Ho Na, and Seungwon Shin*
  31st ACM International Conference on Information and Knowledge Management **(CIKM 2022)**
- **MECaNIC: SmartNIC to Assist URLLC Processing in Multi-Access Edge Computing Platforms**
  *Taejune Park, Myoungsung You, **Jian Cui**, Youngjin Jin, and Seungwon Shin*
  The 30th IEEE International Conference on Network Protocols **(ICNP 2022)**
- **Discovering Message Templates on Large-scale Bitcoin Abuse Reports using a Two-fold NLP-based Clustering Method**
  *Jinho Choi, Taehwa Lee, Kwanwoo Kim, Minjae Seo, **Jian Cui**, and Seungwon Shin*
  Institute of Electronics, Information and Communication Engineers **(IEICE letter)**

- ***Tweezers*: A Graph-based Security Event Detection Framework on Twitter.**
  Jian Cui, *Hanna Kim, Eugene Jang, Dayeon Yim, Kicheol Kim, Jinwoo Chung, Yongjae Lee, Seungwon Shin, Xiaojing Liao*
  (under review)
- **Exploring the Familiar Taste of Toxicity: A Causal Influence Analysis of Toxic Comments on Internet Forums**
  Kwanwoo Kim, ***Jian Cui****, Minkyoo Song, Seungwon Shin*
  (under review)

PROFESSIONAL EXPERIENCE

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

- **LLM Security**: Conducting research on security concerns in retrieval-augmented generation (RAG) for code generation models.

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

- **Privacy Compliance of Generative AI**: Conducting research on privacy implications in generative AI tools, focusing on investigating and analyzing real-world applications' privacy compliance, and ultimately aiming to develop strategies to ensure adherence to privacy regulations.

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

- **Security Language Model Pre-training**: Pre-train the Darkweb language model and the security language model, 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**: Propose a novel contrastive learning-based security event detection framework that can generate information-rich representation for better identifying the security-related events.

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.

Undergraduate Individual Research Intern
KAIST, South Korea *June. 2019 - Dec. 2019*

- Studied Software-defined Network (SDN) and implemented hardware-based networking scheduler in the NetFPGA using Verilog.

PROFESSIONAL ACTIVITIES

Program Committee

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

Reviewer

- IEEE Transactions on Information Forensics and Security (TIFS), 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
- IEEE European Symposium on Security and Privacy (EuroS&P), 2024

HONORS AND AWARDS

Indiana University Luddy Doctoral Summer Fellowship *Aug. 2023*

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

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

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

The 2020 Korea Cyber Security Paper Award *Sept. 2020*
Title: *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