Emily (Shuya) Feng

Email : shuya.feng@uconn.edu
Website : https://shuyafeng.github.io/

Research Interests

- **Security and Privacy**
  - Data Privacy, Privacy Modeling & Analysis, Privacy Attacks, Differential Privacy, Blockchain Security
- **Responsible AI**
  - ML Privacy & Security, LLM Privacy & Security

Education

University of Connecticut
Ph.D. Candidate in Computer Science and Engineering — Aug 2022 to July 2025
Advisor: Dr. Yuan Hong

Illinois Institute of Technology
Attended in the Dept. of Computer Science — Aug 2019 to May 2022
Advisor: Dr. Maggie Cheng

M.S. in Computer Science — Aug 2015 to May 2017

Harbin Institute of Technology
B.S. in Computer Science — Aug 2011 to July 2015

Professional Appointments

University of Alabama at Birmingham, Birmingham, AL — Aug 2025–Present
Assistant Professor

Amazon, NYC, NY — May 2024–Aug 2024
Research Intern

University of Connecticut, Storrs, CT — Aug 2022–July 2025
Research Assistant, Teaching Assistant

Illinois Institute of Technology, Chicago, IL — Aug 2019–Aug 2022
Research Assistant, Teaching Assistant

Major Trading Inc, Lombard, IL — Dec 2017–May 2019
Data Scientist

Teaching

CSE5173 Deep Learning, University of Cincinnati, Guest Lecture — Nov 2024
CSE4400 Computer Security, UConn, TA — Jan 2023–May 2023
CSE1010 Introduction to Computing for Engineers, UConn, TA — Aug 2022–Dec 2022
CS425 Database Organization, IIT, TA — Jan 2022–May 2022
CS528 Data Privacy and Security, IIT, TA — Aug 2021–Dec 2021

Refereed Publications

[1] **Shuya Feng**, Meisam Mohammady, Hanbin Hong, Shenao Yan, Binghui Wang, Ashish Kundu, and Yuan Hong. "Harmonizing Differential Privacy Mechanisms in Federated Learning: Ensuring Boosted Accuracy and Convergence." In Proceedings of the Fifteenth ACM Conference on Data and Application Security and Privacy (CODASPY '25).

[2] Xiaochen Li, Zhan Qin, Kui Ren, Chen Gong, **Shuya Feng**, Yuan Hong, and Tianhao Wang. "Delay-allowed Differentially Private Data Stream Release," In Proceedings of the Network and Distributed System Security Symposium (**NDSS**), San Diego, CA, USA, 2025.

[3] Can Jin, Hongwu Peng, Anxiang Zhang, Nuo Chen, Jiahui Zhao, Xi Xie, Kuangzheng Li, **Shuya Feng**, Kai Zhong, Caiwen Ding, and Dimitris N. Metaxas. 2025. RankFlow: A Multi-Role Collaborative Reranking Workflow Utilizing Large Language Models. In Companion Proceedings of the ACM on Web Conference 2025 (WWW '25).

[4] **Shuya Feng***, Meisam Mohammady*, Han Wang, Xiaochen Li, Zhan Qin, and Yuan Hong. "DPI: Ensuring Strict Differential Privacy for Infinite Data Streaming." In Proceedings of the 45th IEEE Symposium on Security and Privacy (**S&P**). [Acceptance Rate in Cycle 2: 83/558=14.9%, * Equal Contribution]

[5] Boyuan Feng, Yijiang Zheng, Ruting Cheng, Khashaya Vaziri, **Shuya Feng**, and James Hahn. "Enhanced body composition estimation from 3d body scans." In Proceedings of the 16th International Conference on Bioinformatics Models, Methods and Algorithms (BIOINFORMATICS). SCITEPRESS, 2024.

[6] Matta Varun, **Shuya Feng**, Han Wang, Shamik Sural, and Yuan Hong. "Towards Accurate and Stronger Local Differential Privacy for Federated Learning with Staircase Randomized Response." In Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy, 2024, pp. 307-318. [Acceptance Rate: 34/160=21.25%, Co-advised work]

[7] Han Wang*, Jayashree Sharma*, **Shuya Feng**, Kai Shu, and Yuan Hong. "A Model-Agnostic Approach to Differentially Private Topic Mining." In Proceedings of the 28th SIGKDD Conference on Knowledge Discovery and Data Mining (**KDD**), Washington D.C., August 14-18, 2022. [Acceptance Rate: 254/1695=14.99%, * Equal Contribution]

[8] **Shuya Feng**, Jia He, and Maggie Cheng."Security Analysis of Block Withholding Attacks in Blockchain," In Proceedings of IEEE International Conference on Communications (**ICC**), Montreal, QC, Canada, 2021, pp. 1-6, doi: 10.1109/ICC42927.2021.9500630.

Under Review or To Be Submitted

[1] Meisam Mohammady, Han Wang, **Shuya Feng**, Lingyu Wang, Mengyuan Zhang, Yosr Jarraya, Suryadipta Majumdar, Makan Pourzandi, Mourad Debbabi, and Yuan Hong. "DPOAD: Differentially Private Outsourcing of Anomaly Detection through Iterative Sensitivity Learning." Under Review.

[2] Hanbin Hong, Shenao Yan, **Shuya Feng**, and Yuan Hong. "Zero-shot Generative Active Learning via Controllable Text-to-image Generation." Under Review.

[3] "SoK: A Universal Platform for Integrating and Evaluating Jailbreak Attacks and Defenses on Large Language Models". To be submitted.

[4] "Density-Aware Privacy Preservation in High-Dimensional Embedding Spaces". To be submitted.

[5] "Double Poisoning: Breaking Both Privacy and Robustness in Locally Private Graph Neural Networks". To be submitted.

[6] "Utility-Optimized Differentially Private Mechanism for Adder Network". To be submitted.

Honors and Distinctions

Conference Participation Award by The Graduate School UConn	July 2024
The Marion and Frederick Buckman Engineering Fellowship	May 2024
Travel Conferenceship by IEEE S&P	Apr 2024
Synchrony Fellowship by UConn CSE	Aug 2023

Grant Activity

- Assisted in writing the proposal "PDaSP: Track 1: Towards Sustainable, Equitable, and Auditable Privacy Protection for Clinical Risk Prediction in Distributed Healthcare Systems", submitted to the NSF Privacy-Preserving Data Sharing in Practice (PDaSP) Program. [Pending, Total Amount: $1,000,000].
- Assisted in writing the proposal "PDaSP: Track 2: A Holistic Privacy Preserving Collaborative Data Sharing System for Intelligent Transportation", submitted to the NSF Privacy-Preserving Data Sharing in Practice (PDaSP) Program. [Pending, Total Amount: $1,500,000].

Professional Contributions

External Reviewer

2025	USENIX Security, NDSS
2024	USENIX Security, ACM TOPS, IEEE TIFS, IEEE TDSC, IEEE INFOCOM
2023	ACM CCS, USENIX Security Symposium, WWW, RAID, ACM AsiaCCS
2022	AAMAS, PETs, IEEE TPS, DBSEC, ESORICS
2021	IEEE/ACM CCGrid

Volunteer Experience

Student Volunteer, IEEE S&P 2024
Conference Coordinator, ICPP 2021

Invited Talks

- "Strict privacy in streaming data" at UCONN Security Seminar, Dec 2024.
- "Privacy and security in deep learning" at the University of Cincinnati(online), Nov 2024.
- "Preserving strict privacy in streaming data" at Yale Univerisity, Spring 2025.

Open-Source Development

- DPI: https://github.com/ShuyaFeng/DPI
- UDP-FL: https://github.com/ShuyaFeng/UDP-FL
- TopicDP: https://github.com/hwangcsiit/Differentilaly-private-topic-mining
- SRR-FL: https://github.com/matta-varun/SRR-FL