

Han Wu

School of Electronics and Computer Science, University of Southampton, UK

h.wu@soton.ac.uk; whinhust@gmail.com



Research Interests

AI privacy and security, differential privacy, privacy auditing, federated learning, synthetic data

Academic Appointments

University of Southampton

Lecturer in Cyber Security, School of Electronics and Computer Science

- Differential privacy, machine unlearning, and large language model security.

University of Birmingham

Research Fellow, School of Computer Science

- Developed federated-learning-based systems for synthetic tabular data generation; worked with researchers in law, business, social sciences, arts, and culture on interdisciplinary research into complex online harms.

Newcastle University

Research Associate, School of Computing

- Developed federated learning systems tailored to financial tabular data; evaluated privacy risks in federated learning systems under different attack settings in collaboration with the Business School and Atom Bank.

Education

Freie Universitaet Berlin

PhD in Computer Science, with distinction

Tongji University

MSc in Software Engineering

Huazhong University of Science and Technology

BEng in Civil Engineering

Berlin, Germany

Sep 2016–Jan 2021

Shanghai, China

Sep 2013–Mar 2016

Wuhan, China

Sep 2009–Jun 2013

Research Projects

AGENCY: Safeguarding Citizen Agency in a World with Complex Online Harms

Location and period: University of Birmingham, Aug 2022–Mar 2024

Role: Research Fellow

- EPSRC project (£2,674,250) studying citizen agency, complex online harms, smart homes, digital identity, and online disinformation.

Machine Unlearning for Tabular Data: Exploring Public Perceptions of Privacy

Location and period: University of Birmingham, May 2023–Present

Role: Principal Investigator

- Paul and Yuanbi Ramsay Research Fund project (£2,970) on public perceptions of privacy and feature sensitivity in tabular data.

UnFed: Selective Forgetting in Federated Financial Applications

Location and period: University of Southampton, 2023–2024

Role: Co-PI

- EPSRC/UKFin+ pilot project (£20,000) on selective forgetting in privacy-preserving federated financial applications.

FinTrust: Trust Engineering for the Financial Industry

Location and period: Newcastle University, May 2021–Jul 2022

Role: Researcher

- EPSRC Digital Economy Theme project (£1,047,202) on trust, identity, privacy, and security in financial technology.

Collaborative and Privacy-Preserving Deep Learning Technologies in Financial Services

Location and period: Newcastle University, Jul 2022–Dec 2022

Role: Principal Investigator

- Alan Turing Institute project (£2,000) exploring privacy risks and privacy-preserving federated learning for financial services.

Publications

- **[ICML '26]** Zou, S., Wang, S., Zhu, Z., Li, J., Dong, C., Sassone, V., & **Wu, H.***. SlaClip: Gradient Norm Slacks can be Indicator for Adaptive Clipping in DP-SGD. In *Proceedings of the 43rd International Conference on Machine Learning*. <CoreRank: A*, Spotlight, Top 2.2%>.
- **[T-Rel '26]** **Wu, H.**, Shang, Z., Wu, H., & Wolter, K. An Adaptive Mini-Batching Strategy for Reliable Streaming Data Delivery in Real-Time. *IEEE Transactions on Reliability*, 75, 1782–1796. <JCR: Q1>.
- **[EuroMLSys '26]** Wang, J., Zhao, Z., Aniello, L., & **Wu, H.*** Peeling the Layers of Privacy-Utility Onion on Tabular Data. In *Proceedings of the Sixth European Workshop on Machine Learning and Systems*, 139–146. ACM.
- **[USENIX '25]** Wang, S., Dong, C., Song, X., Li, J., Zhou, Z., Wang, D., & **Wu, H.** Beyond Statistical Estimation: Differentially Private Individual Computation via Shuffling. *USENIX Security Symposium*. <CoreRank: A*, Honorable Mention Award>.
- **[DSN '25]** Zhao, Z., **Wu, H.***, van Moorsel, A., & Chen, L. Y. GTV: Generating Tabular Data via Vertical Federated Learning. In *2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 33–46. IEEE. <CoreRank: A>.
- **[TCSI '25]** Yuan, X., Yao, Y., **Wu, H.**, & Feng, M. Impacts of Physical-Layer Information on Epidemic Spreading in Cyber-Physical Networked Systems. *IEEE Transactions on Circuits and Systems I: Regular Papers*. <JCR: Q1>.
- **[TCSS '24]** Kolomeets, M., **Wu, H.**, Shi, L., & van Moorsel, A. The Face of Deception: The Impact of AI-Generated Photos on Malicious Social Bots. *IEEE Transactions on Computational Social Systems*. <JCR: Q1>.
- **[FGCS '23]** Olabode, S., Owens, R., Zhang, V. N., Copilah-Ali, J., Kolomeets, M., **Wu, H.**, Malviya, S., Markeviciute, K., Spiliotopoulos, T., Neesham, C., & Shi, L. Complex Online Harms and the Smart Home: A Scoping Review. *Future Generation Computer Systems*. <JCR: Q1>.
- **[ISSRE '22]** **Wu, H.**, Zhao, Z., Chen, L. Y., & van Moorsel, A. Federated Learning for Tabular Data: Exploring Potential Risk to Privacy. In *2022 IEEE International Symposium on Software Reliability Engineering*, 193–204. IEEE. <CoreRank: A>.
- **[ECML '22]** **Wu, H.**, Qian, H., Wu, H., & van Moorsel, A. LDRNet: Enabling Real-Time Document Localization on Mobile Devices. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*, 618–629. Springer. <CoreRank: A>.
- **[ICBC '22]** Ma, X., **Wu, H.**, Xu, D., & Wolter, K. CBlockSim: A Modular High-Performance Blockchain Simulator. In *2022 IEEE International Conference on Blockchain and Cryptocurrency*, 1–5. IEEE.
- **[IoTJ '21]** Peng, G., Wu, H., **Wu, H.**, & Wolter, K. Constrained Multiobjective Optimization for IoT-Enabled Computation Offloading in Collaborative Edge and Cloud Computing. *IEEE Internet of Things Journal*, 8(17), 13723–13736. <JCR: Q1>.
- **[ISSRE '20]** **Wu, H.**, Shang, Z., Peng, G., & Wolter, K. A Reactive Batching Strategy of Apache Kafka for Reliable Stream Processing in Real-Time. In *2020 IEEE International Symposium on Software Reliability Engineering*, 207–217. IEEE. <CoreRank: A>. Acceptance rate: 25.7%.
- **[DSN '20]** **Wu, H.**, Shang, Z., & Wolter, K. Learning to Reliably Deliver Streaming Data with Apache Kafka. In *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 564–571. IEEE. <CoreRank: A>. Acceptance rate: 16.5%.
- **[ISSREW '19]** **Wu, H.** Research Proposal: Reliability Evaluation of the Apache Kafka Streaming System. In *2019 IEEE International Symposium on Software Reliability Engineering Workshops*, 112–113. IEEE.
- **[ISSREW '19]** **Wu, H.**, Shang, Z., & Wolter, K. TRAK: A Testing Tool for Studying the Reliability of Data Delivery in Apache Kafka. In *2019 IEEE International Symposium on Software Reliability Engineering Workshops*, 394–397. IEEE.
- **[HPCC '19]** **Wu, H.**, Shang, Z., & Wolter, K. Performance Prediction for the Apache Kafka Messaging System. In *2019 IEEE 21st International Conference on High Performance Computing and Communications*, 154–161. IEEE.

Academic Service

- Gold Reviewer, ICML 2026.
- Program Committee Member, IEEE/IFIP DSN 2026.
- Reviewer, IEEE Transactions on Information Forensics and Security.
- Reviewer, IEEE Transactions on Parallel and Distributed Systems.
- Reviewer, IEEE Transactions on Dependable and Secure Computing.
- Program Committee Member, ACM/SPEC International Conference on Performance Engineering (ICPE) 2023.
- Shadow Program Committee Member, EuroSys 2022.
- Reviewer, SRDS 2018.