Chenglong Fu

Assistant Professor, Department of Cybersecurity, UNC Charlotte
chenglong.fu@charlotte.edu | Google Scholar

Research Interests

My research focuses on IoT and cyber-physical systems security, AI security and privacy, and AI-assisted security analysis. I combine system analysis, formal methods, and experimental evaluation to study device behavior, adversarial risks, and verifiable automation. I also develop open-source infrastructure for auditable AI-assisted research and smart-home interoperability.

Education

Temple University Philadelphia, PA
Ph.D. in Computer and Information Sciences *Aug. 2016 – May. 2022*

- Supervised by Prof. Xiaojiang Du
- Dissertation Title: Semantics-aware Effective Security Solutions for Home Automation System

University of Science and Technology of China Hefei, China
Bachelor of Engineering in Information Security *Aug. 2011 – June. 2015*

Research & Work Experiences

Assistant Professor Aug 2022 – Present
University of North Carolina at Charlotte *Charlotte, NC*

Postdoc Research Fellow Jan. 2022 – Aug. 2022
University of South Carolina *Columbia, SC*

Research Assistant Sep. 2016 – December. 2021
Temple University *Philadelphia, PA*

Selected Peer-Reviewed Publications and Accepted Papers

[1] Jiahang Wang, **Chenglong Fu** (corresponding author), Xiaojiang Du, and Bo Luo. "Jailbreaking via Activation Dilution: Neuron-Guided Adaptive Decomposition of Language Models." Accepted to ACM Conference on Computer and Communications Security (CCS), 2026.

[2] ZhuoYi Shi, **Chenglong Fu**, Xiaojiang Du, and Rong Xu. "Effective Handling of Erroneous Executions of Automation Rules on Multiple Platform Smart Home IoT Systems." In International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2026. **Best Paper Award.**

[3] Liqun Shan, Yazhou Tu, Kaiying Han, Sheng Chen, **Chenglong Fu**, and Xiali Hei. "UDPU: Unlabeled Data Purification and Unlearning for Backdoor Defense." In International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2026.

[4] Huan Bui and **Chenglong Fu**. "PG-DSL: Physics-Grounded Admission Checking for MCP-Controlled CPS Tools." Accepted to Annual Computer Security Applications Conference (ACSAC), 2026.

[5] **Chenglong Fu**, Chi Zhang, and Mengtian Li. "Cross-Referencing Whitepaper Claims and Smart Contract Code for Automated ICO Auditing." In IEEE/IFIP International Conference on Dependable Systems and Networks, Industry Track (DSN Supplemental Volume), 2026, pp. 85–91.

[6] **Chenglong Fu**, Shirin Besati, and Miao Wang. "LLM-GridEval: Measuring the Evaluation Validity Gap in Smart Grid Security with Adaptive LLM Attackers." In ACM SIGEnergy Workshop on Cybersecurity and Privacy of Energy Systems (EnergySP), ACM Sustainability Week Companion, 2026, pp. 100–109.

[7] Zhelin Zheng, **Chenglong Fu**, Xiaojiang Du, and Yuede Ji. "L2R: Verification-Guided Repair of LLM-Generated Smart-Home Automation Rules." Accepted to International Conference on Information Security and Cryptology (Inscrypt), 2026.

[8] **Chenglong Fu**, Xuening Xu, and John Du. "Does Efficiency Leak? Auditing the Privacy of Compressed and Stale Updates in Federated Intrusion Detection for IoT." Accepted to International Conference on Information Security and Cryptology (Inscrypt), 2026. **Best Paper Award (Security Track).**

[9] Huan Bui and **Chenglong Fu**. "PROVSAFE: Provenance-Gated Enforcement for Tool-Using LLM Agents." Accepted to IEEE International Performance, Computing, and Communications Conference (IPCCC), 2026.

[10] Huan Bui and **Chenglong Fu**. "Effective Perturbation Budget: Auditing Preprocessing-Induced Amplification in ICS Anomaly Detector Robustness." Accepted to IEEE International Performance, Computing, and Communications Conference (IPCCC), 2026.

[11] Huan Bui, **Chenglong Fu**, and Fei Zuo. "TAPAssure: Safe Automation in Smart Homes with LLMs and Formal Verification." In *Security and Privacy in Cyber-Physical Systems and Smart Vehicles* (SmartSP 2025), pp. 41–61, Springer, 2026.

[12] Fei Zuo, Junghwan Rhee, Yung Ryn Choe, **Chenglong Fu**, Xianshan Qu. "Few-Shot Learning-Based Cyber Incident Detection with Augmented Context Intelligence". In IEEE Annual International Computer Software and Applications Conference (COMPSAC) 2025.

[13] Xuening Xu, **Chenglong Fu**, Xiaojiang Du, Bo Luo. "Discovering and Exploiting IoT Device Hidden Attributes: A New Vulnerability in Smart Homes", In ACM Conference on Computer and Communications Security (CCS) 2025.

[14] Md Rabbi Alam, Jinpeng Wei, Md Sajidul Islam Sajid, Qingyang Wang, and **Chenglong Fu**. "Moving from the Developer Machine to IoT Devices: An Empirical Study." In IEEE Secure Development Conference (SecDev), 2024, pp. 140–152.

[15] Huan Bui, Harper Lienerth, **Chenglong Fu**, and Meera Sridhar. "Poster: TAPChecker: Model Checking in Trigger-Action Rules Generation Using Large Language Models." Poster presented at the ACM Conference on Computer and Communications Security (CCS) 2024, Salt Lake City, Utah, October 2024.

[16] Haotian Chi, Qi Ma, Yuxuan Zhang, **Chenglong Fu**, Yuwei Wang, Haijun Geng, and Xiaojiang Du. "Audio-Assisted Smart Home Security Monitoring with Few Samples." In Proceedings of the 2024 IEEE Global Communications Conference: Communication & Information Systems Security (Globecom 2024 CISS), Cape Town, South Africa, 2024, pp. 2413–2418.

[17] Huan Bui and **Chenglong Fu**. "ShadowConn: Breaking the Entanglement of Cross-Platform IoT Delegation in Multi-user Environments." In *Security and Privacy in Cyber-Physical Systems and Smart Vehicles* (SmartSP 2024), pp. 158–184, Springer, 2025.

[18] Md Rabbi Alam, Jinpeng Wei, Md Sajidul Islam Sajid, Qingyang Wang and **Chenglong Fu**, "Attacking IoT Devices through the IoT Cloud Platforms: An Empirical Study", In ACM Conference on Data and Application Security and Privacy (CODASPY) 2024

[19] Trent Reichenbach, **Chenglong Fu**, Xiaojiang Du, Jia Di, Yuede Ji, "TrustEvent: Cross-Platform IoT Trigger Event Verification Using Edge Computing", In IEEE International Conference on Communications (ICC), June 2024.

[20] **Chenglong Fu**, Xiaojiang Du, Qiang Zeng, Zhenyu Zhao, Fei Zuo, Jia Di, "Seeing Is Believing: Extracting Semantic Information from Video for Verifying IoT Events", In 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), May 2024.

[21] Andrew D'Angelo, **Chenglong Fu**, Xiaojiang Du, E. Paul Ratazzi. "Discovering Complex Correlations among Multiple IoT Devices in Smart Environments", IEEE Global Communications Conference (Globecom), December 2023.

[22] Andrew F D'Angelo, **Chenglong Fu**, Xiaojiang Du, Paul Ratazzi, "Transformer-based Compound Correlation Miner for Smart Home Anomaly Detection", IEEE International Conference on Cloud Networking (CloudNet), November 2023.

[23] Yunping Fang, **Chenglong Fu**, Xiaojiang Du, "Virtual-Device-Based Policy Enforcement in Multi-Admin Smart Environments", IEEE International Conference on Cloud Networking (CloudNet), November 2023.

[24] Xuening Xu, **Chenglong Fu**, Xiaojiang Du. "MP-Mediator: Detecting and Handling the New Stealthy Delay Attacks on IoT Events and Commands", 26th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), October 2023.

[25] Xuening Xu, **Chenglong Fu**, Xiaojiang Du, and E. Paul Ratazzi. "VoiceGuard: An Effective and Practical Approach for Detecting and Blocking Unauthorized Voice Commands to Smart Speakers", IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June 2023.

[26] Chenxu Jiang, **Chenglong Fu**, Zhenyu Zhao, Xiaojiang Du,"Effective Anomaly Detection in Smart Home by Integrating Event Time Intervals", International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN), October 2022.

[27] **Chenglong Fu**, Qiang Zeng, Haotian Chi, Xiaojiang Du, and Siva Likitha Valluru. "IoT Phantom-Delay Attacks: Demystifying and Exploiting IoT Timeout Behaviors." In IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2022, pp. 428–440.

[28] Haotian Chi, **Chenglong Fu** (Co-first author), Qiang Zeng, Xiaojiang Du. "Delay Wreaks Havoc on Your Smart Home", In IEEE Symposium on Security and Privacy (IEEE S&P), May 2022.

[29] Xuanyu Liu, Qiang Zeng, Xiaojiang Du, Siva Likitha Valluru, **Chenglong Fu**, Xiao Fu, Bin Luo "SniffMislead: Non-Intrusive Privacy Protection Against Wireless Packet Sniffers in Smart Homes." In the International Symposium on Research in Attacks, Intrusions and Defenses (RAID), October 2021.

[30] **Chenglong Fu**, Qiang Zeng, Xiaojiang Du. "HAWatcher: Semantics-Aware Anomaly Detection for Appified Smart Homes. " In the proceeding of 30th USENIX Security Symposium (USENIX Security), August 2021.

[31] Michael Wang, **Chenglong Fu**, Xiaojiang Du. "Decision-Tree Based Root Cause Localization for Anomalies in Smart IoT Systems." In the IEEE International Conference on Communications (ICC), June 2021

[32] Heena Rathore, **Chenglong Fu**, Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, Mohsen Guizani, and Zhengtao Yu. "Multi-layer security scheme for implantable medical devices." Neural Computing and Applications 32, no. 9 (2020): 4347-4360.

[33] Xuening Xu, **Chenglong Fu**, Xiaojiang Du, and E. Paul Ratazzi. "Effective UAV and Ground Sensor Authentication." In IEEE Global Communications Conference (GLOBECOM), December 2019.

[34] **Chenglong Fu**, Xiaojiang Du, Longfei Wu, Qiang Zeng, Amr Mohamed, and Mohsen Guizani."POKs-based secure and energy-efficient access control for implantable medical devices." In International Conference on Security and Privacy in Communication Systems (SecureComm), October 2019.

[35] Qiang Zeng, Jianhai Su, **Chenglong Fu**, Golam Kayas, Lannan Luo, Xiaojiang Du, Chiu C. Tan, and Jie Wu. "A multiversion programming inspired approach to detecting audio adversarial examples." In 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June 2019.

[36] **Chenglong Fu**, Tassadit Kezmane, Xiaojiang Du, Yat Fu, and Colin Morrisseau."An location-aware authentication scheme for cross-domain internet of thing systems." In International Conference on Computing, Networking and Communications (ICNC), March 2018.

Preprints

[P1] **Chenglong Fu**. "Research Should Outlive the Agent: RKA as Researcher-controlled Project Memory for Agentic Research." *SSRN preprint*, 2026. doi:10.2139/ssrn.7396118.

[P2] Peiran Shi, Jian Xiang, Xiang Zhang, and **Chenglong Fu**. "Where Does Detection Fail? A Residual-Evidence Diagnostic Workflow for Industrial Control Systems." *arXiv preprint*, arXiv:2608.02821v2, 2026.

[P3] Danial Abshari, Peiran Shi, **Chenglong Fu** (corresponding author), Meera Sridhar, Xiaojiang Du. "INVARLLM: LLM-assisted Physical Invariant Extraction for Cyber-Physical Systems Anomaly Detection", *arXiv preprint*, arXiv:2411.10918, 2024.

[P4] **Chenglong Fu**, Qiang Zeng, and Xiaojiang Du. "Towards Efficient Integration of Blockchain for IoT Security: The Case Study of IoT Remote Access." arXiv preprint, 2019.

Other Manuscripts

[M1] Rong Xu, **Chenglong Fu**, Xiaojiang Du, ZhuoYi Shi, Hao Wang, Nicholas Bielanos. "EdgeFuzzer: Context-guided Fuzzing for IoT Applications on Smart Home Hubs". Manuscript

[M2] Andrew D'Angelo, **Chenglong Fu** (corresponding author), Xiaojiang Du. "Phantom Buster: Defense against the Stealthy IoT Delay Attack in Smart Homes". Manuscript.

[M3] Xuening Xu, **Chenglong Fu**, Xiaojiang Du, Bo Luo. "EdgeDevil: The Dormant Menace in Your Smart Home", Manuscript.

[M4] Xuening Xu, **Chenglong Fu**, Xiaojiang Du, Bo Luo. "IoTtracer: Detecting Malicious Local Attacks on IoT Devices by Utilizing IoT System-level Traffic Patterns", Manuscript.

Selected Open-Source Projects

RKA – Research Knowledge Agent

- An open-source knowledge system for long-running, AI-assisted research. Connects notes, experiments, decisions, and claims with supporting evidence to preserve research continuity and researcher control.
- github.com/rka-project/rka-core

EdgeLoom

- An open-source toolchain for smart-home edge drivers, including hidden-capability exposure, cross-platform translation, artifact validation, and reviewable audit records.
- github.com/edgeloom-oss/edgeloom

Funding and Grants

CCI Summer Education Project Award Summer 2026

- "Entry-Level Cybersecurity Course for All UNC Charlotte Majors." Awarded by the CCI Office of the Dean, UNC Charlotte; $7,000 in project support.

Lead PI - UNC Charlotte Core Facilities Program Sep 2024

- "Building Customizable Large Language Model Services for Education and Research", Granted by University of North Carolina at Charlotte, $250K. 2024-2026

CoPI - NC Research Opportunities Initiative June 2023

- "North Carolina Research Capacity Building for a Secure & Reliable Power Grid 2050", Granted by University of North Carolina System, $1.5M total project funding. 2023-2026

PI - UNCC Faculty Research Grants Program Jan 2024

- "Automated Auditing of Initial Coin Offerings", Granted by the University of North Carolina at Charlotte, $8K. 2024-2025

Teaching Experiences

ITIS 3200: Introduction to Security and Privacy Jan 2025 – May 2025

ITIS 4221/5221: Penetration Testing & Secure Programming Jan 2023 – Present

- Spring 2025 instructor evaluation: 4.0/5

ITSC 3146: Operating Systems & Computer Networks Jan 2023 – May 2023

- Instructor evaluation: 4.1/5

Professional Services

Program committees

- IEEE Symposium on Security and Privacy, 2027
- USENIX Security Symposium, 2027
- IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Research Track, 2026
- ACM Conference on Computer and Communications Security (CCS), 2025

University service

- University Research Council, UNC Charlotte, 2026–2028 term
- Research and Infrastructure Committee, Department of Cybersecurity, UNC Charlotte, Member, 2026
- Graduate Committee, Department of Cybersecurity, UNC Charlotte, Member, 2026–2027

Talks and panels

- RSTCON 2026, October 24, 2026: presented "The Center for Energy Security and Reliability at UNC Charlotte" and participated in the subsequent panel discussion.

Conference organization

- IEEE/IFIP International Conference on Dependable Systems and Networks 2026, Poster Chair
- IEEE/ACM International Symposium on Quality of Service 2023, Publicity Chair
- IEEE International Conference on Cloud Networking 2023, Publicity Chair
- IEEE International Conference on Intelligence and Security Informatics 2023, Finance Chair

Research funding review

- Hong Kong Research Grants Council, Research Fellow Scheme, External Reviewer, 2026/27

Journal and conference reviewing

- IEEE Transactions on Information Forensics and Security, Reviewer
- IEEE Transactions on Pattern Analysis and Machine Intelligence, Reviewer
- IEEE Transactions on Mobile Computing, Reviewer
- IEEE Internet of Things Journal, Reviewer
- IEEE Transactions on Consumer Electronics, Reviewer
- ACM Transactions on Computing Education, Reviewer
- Future Generation Computer Systems, Reviewer
- Computer Standards & Interfaces, Reviewer
- Information Fusion, Reviewer
- Journal of Systems Architecture, Reviewer
- The Journal of Supercomputing, Reviewer
- IEEE International Conference on Computer Communications 2021-2023, Reviewer

Awards and Honors

Best Paper Award, RAID 2026 *2026*

- "Effective Handling of Erroneous Executions of Automation Rules on Multiple Platform Smart Home IoT Systems," with ZhuoYi Shi, Xiaojiang Du, and Rong Xu.

Best Paper Award (Security Track), Inscrypt 2026 *2026*

- "Does Efficiency Leak? Auditing the Privacy of Compressed and Stale Updates in Federated Intrusion Detection for IoT," with Xuening Xu and John Du.

CCI Summer Education Project Award *2026*

- Support for developing an entry-level cybersecurity course for students across all UNC Charlotte majors.

Scott Hibbs Future of Computing Award *April 2021*

- Each year, only one student is selected from all the graduate and undergraduate students (over 1,000 students) in the CIS Department at Temple University

Outstanding Undergraduate Scholarship *Sep 2014*

- 10% among all undergraduates, granted by University of Science & Technology of China

Seagate Scholarship *2013*

- 5% among all undergraduates, Granted by Seagate Technology co., LTD

Outstanding College graduates in Provincial Scale *June 2015*

- 1 among all undergraduates in the department of Information Security, Granted by Department of Education of Anhui Province