Anna Yoo Jeong Ha

Ph.D. Candidate, Computer Science — University of Chicago
annaha.net • GoogleScholar • annaha@uchicago.edu • LinkedIn

Research Interests

My research strengthens the security and integrity of AI systems. I study how adversaries exploit models and build practical defenses that detect manipulation, verify authenticity, and protect user data—ensuring AI remains trustworthy and resilient in real-world use.

Education

University of Chicago, Chicago, USA

Ph.D. Computer Science
Advisor: Prof. Ben Y. Zhao and Prof. Heather Zheng
GPA: 4.0 / 4.0

Korea University, Seoul, Republic of Korea Mar. 2021 – Feb. 2023

Master of Electrical and Computer Engineering

Korea University, Seoul, Republic of Korea Mar. 2017 - Feb. 2021

Bachelor of Mechanical Engineering

Awards & Patents

Distinguished Paper Award, CCS 2024 Oct. 2024

Video Processing System and Video Processing Method Using Split Learning US-11915477-B2

Publications

Anna Yoo Jeong Ha, Ronik Bhaskar, Haitao Zheng, Ben Y. Zhao. Mitigating Private Data Leakage in LLMs with Whiteout. *In Submission*. 2026.

Anna Yoo Jeong Ha, Wenxin Ding, Stanley Wu, Shawn Shan, Haitao Zheng, Ben Y. Zhao. Identifying Provenance of Generative Text-to-Image Models. *In 35th USENIX Security Symposium (USENIX Security)*. 2026.

Stanley Wu, Ronik Bhaskar, **Anna Yoo Jeong Ha**, Shawn Shan, Haitao Zheng, Ben Y. Zhao. On the Feasibility of Poisoning Text-to-Image AI Models via Adversarial Mislabeling. *Conference on Computer and Communications Security (CCS)*. 2025.

Anna Yoo Jeong Ha, Josephine Passananti, Ronik Bhaskar, Shawn Shan, Reid Southen, Haitao Zheng, Ben Y. Zhao. Organic or Diffused: Can We Distinguish Human Art from AI-generated Images?. *Conference on Computer and Communications Security (CCS)*. 2024. *Distinguished Paper Award*

Yoo Jeong Ha, Gusang Lee, Minjae Yoo, Soyi Jung, Seehwan Yoo, and Joongheon Kim. Feasibility Study of Multi-Site Split Learning for Privacy-Preserving Medical Systems under Data Imbalance Constraints in COVID-19, X-Ray, and Cholesterol Dataset. *Nature Scientific Reports*. 2022.

Yoo Jeong Ha, Minjae Yoo, Gusang Lee, Soyi Jung, Sae Won Choi, Joongheon Kim, and Seehwan Yoo. Spatio-Temporal Split Learning for Privacy-Preserving Medical Platforms: Case Studies with COVID-19 CT, X-Ray, and Cholesterol Data. *IEEE Access*. 2021.

Won Joon Yun, **Yoo Jeong Ha**, Soyi Jung, and Joongheon Kim. Autonomous Aerial Mobility Learning for Drone-Taxi Flight Control. *IEEE ICTC*. 2021.

Gusang Lee, Won Joon Yun, **Yoo Jeong Ha**, Soyi Jung, Jiyeon Kim, Sunghoon Hong, Joongheon Kim, and Youn Kyu Lee. Measurement Study of Real-Time Virtual Reality Contents Streaming over IEEE 802.11 ac Wireless Link. *MDPI Electronics*. 2021.

Yoo Jeong Ha, Minjae Yoo, Soohyun Park, Soyi Jung, and Joongheon Kim. Secure Aerial Surveillance using Split Learning. *IEEE ICUFN*. 2021.

Minjae Yoo, **Yoo Jeong Ha**, Soyi Jung, and Joongheon Kim. CNN-based Hand Gesture Recognition Using mmWave Radar. *ITC-CSCC*. 2021.

Serivces

Teaching

TA, CS35800 Advanced Adversarial Machine Learning, UChicago CS — Winter 2026
TA, CS25800 Adversarial Machine Learning, UChicago CS — Spring 2025
TA, Intro to CS, Korea University CS — Fall 2021

Leadership

PSDSC, Board Member of UChicago PSDSC — Spring 2023

Research Experience

Graduate Computer Science Researcher — SandLab 2023 – Present
Advisor: Prof. Ben Y. Zhao and Prof. Heather Zheng (University of Chicago)
Research on the security and privacy of AI systems from an adversarial perspective to enhance model robustness and ensure safety for users.
Develop technical solutions to protect against unethical AI practices and mitigate security vulnerabilities.

Quantum Hyper-Driving: Quantum-Inspired Hyper-Connected and Hyper-Sensing Autonomous Mobility Technologies – NRF Mar. 2022 – Dec. 2022
Research Assistant; Advisor: Prof. Joongheon Kim (Korea University)
Research on ultra-dense vehicle network environment using quantum computing and build an autonomous driving system.
Understanding network and security optimization for multimodal sensing based on quantum computing and quantum-based optimization algorithms to efficiently use large amounts of data.

Autonomous Intelligent COA Search Methods for Cyber-Attacks Dec. 2021 - Nov.2022
Research Assistant; Advisor: Prof. Joongheon Kim (Korea University)
Research on autonomous intelligent cyber threat COA detection technology (DRL, hierarchical attack representation model) in a large-scale distributed military network environment.

Development of Privacy-reinforcing Distributed Transfer-Iterative Learning Algorithm - MHW Jul. 2019 - Nov.2022
Research Assistant; Advisor: Prof. Joongheon Kim (Korea University)
Research on DisTIL, a distributed deep learning federated learning algorithm with enhanced personal information protection by utilizing three institutions' Common Data Model (CDM).

Technical Skills

Programming Languages: Python, C++, JavaScript, SQL
ML/AI Frameworks: PyTorch, TensorFlow, Scikit-learn, Pandas, NumPy
ML Specializations: LLMs, Text-to-Image Diffusion Models, Supervised/Unsupervised Learning, Reinforcement Learning
Statistics & Analysis: A/B Testing, Hypothesis Testing Languages
Native in English and Korean