

ABOUT ME

I am a Ph.D. student in Artificial Intelligence at Sungkyunkwan University, working in the Software Laboratory under Prof. Moohong Min. My research centers on the security and trustworthiness of machine learning systems, including adversarial robustness, jailbreaking and red-teaming of large language models, multimodal threat detection, and forensic analysis of AI agent behavior.

EDUCATION

Sungkyunkwan University

Ph.D. in Artificial Intelligence

Suwon-si, Republic of Korea

2026–Current

Sungkyunkwan University

M.S. in Immersive Media Engineering

Seoul, Republic of Korea

2024–2026

Sungkyunkwan University

B.S. in Computer Education

Seoul, Republic of Korea

2020–2024

HONORS AND AWARDS

- Graduate School Scholarship Type 2 (half-tuition, $\approx$ \$11,500), SKKU, Korea Mar. 2026
- Best Student Paper Award, ISOFIC 2024, “Procedures for Developing Secure FPGA in Nuclear Power Plants”, Korea Dec. 2024
- ICT Innovation Human Resources Development Scholarship (full-tuition, $\approx$ \$23,000), Ministry of Science and ICT (MSIT) / IITP, Korea Mar. 2024
- Grand Award, Gyeonggi-do Metaverse Ideathon, Ministry of Science and ICT, Korea Nov. 2023
- Bronze Award, 2nd SKKU College of Education AI Education Hackathon, SKKU, Korea Sep. 2022
- Silver Award, College of Education AI Education Capstone Design Contest, SKKU, Korea Dec. 2021
- Encouragement Award, 2021 Capstone Design and Idea Hackathon Contest, Korea Internet & Security Agency, Korea Oct. 2021

CONFERENCE PUBLICATIONS

- [C1] **M. Hur**, J. Shin, D. Kim, and M. Min, “Cite Unseen: Measuring Citation-Channel Vulnerabilities in Retrieval-Augmented Generation”, in *CIKM*, 2026, to appear.
- [C2] **M. Hur**, J. Shin, and M. Min, “STAFT: Privacy-Preserving Semantic Trace Abstraction for Forensic Triage of Personal AI Agent Incidents”, in *DFRWS APAC*, 2026, to appear.
- [C3] **M. Hur**, J. Shin, and M. Min, “MD-SRA: Multimodal Detection of SEO-based Redirection Attacks”, in *SAC*, 2026, pp. 1107–1116.
- [C4] **M. Hur**, D. Kim, and M. Min, “SensitiveMamba: Selective State Space Modeling for Robust Time Series Anomaly Detection”, in *SAC*, 2026, pp. 1156–1163.
- [C5] D. Kim, **M. Hur**, J. Lee, and M. Min, “Jailbreaking LLMs Through Cross-Cultural Prompts”, in *CIKM*, 2025, pp. 4874–4878.

- [C6] J. Kim, **M. Hur**, and M. Min, “From RAG to QA-RAG: Integrating Generative AI for Pharmaceutical Regulatory Compliance Process”, in *SAC*, 2025, pp. 1293–1295.
- [C7] **M. Hur**, E. Lee, S. Seo, J. Hwang, D. Kim, M. Min, and A. Kim, “Development of an Attack Case Generation Model Based on the Characteristics of Digital Assets of Nuclear Power Plants”, in *CSA*, 2024.
- [C8] **M. Hur**, J. Shin, M. Min, and A. Kim, “Analysis of FPGA Development Processes and Associated Security Threats”, in *CSA*, 2024.
- [C9] **M. Hur**, J. Shin, M. Min, and A. Kim, “Procedures for Developing Secure FPGA in Nuclear Power Plants”, in *ISOFIC*, 2024. **(Best Student Paper Award)**

JOURNAL PUBLICATIONS

- [J1] **M. Hur**, S. Seo, J. Hwang, and M. Min, “Are Large Language Models Effective for Detecting Spam Messages?”, in *International Journal of Information Security* 25, no. 4, 2026, p. 127.
- [J2] Y. Lee, **M. Hur**, and M. Min, “Evidence Access Design for LLM-based Scientometrics: Graph-based Evidence Augmentation over Semantic Retrieval”, in *Scientometrics*, 2026, pp. 1–35.

RESEARCH EXPERIENCE

University of Michigan

Ann Arbor, MI, USA

Summer Visiting Researcher, Kresge Hearing Research Institute

Summer 2026

- Analyzed auditory-nerve time-series data with machine learning and deep learning methods in Prof. Jun Hee Kim’s laboratory

Sungkyunkwan University

Suwon-si, Republic of Korea

Graduate Researcher, Software Laboratory

2024–Current

- Conducted government- and industry-funded research on AI security, illicit content detection, and cyber threat intelligence (see below)

RESEARCH PROJECTS

AI-based Diagnosis of Floor Impact Sound Reduction Performance in Apartment Buildings

Jun. 2026–Present

Funded by the Korea Agency for Infrastructure Technology Advancement (KAIA), in industry collaboration with MetaInnotech

- Advancing the AI analysis engine for AIoT-measured floor impact sound data for automatic measurement quality assessment, and an MLOps pipeline for continuous retraining and performance monitoring

Development of an Integrated Narcotics Investigation System Linked to Dark Web and Virtual Asset Transaction Tracing

Jan. 2026–Present

Funded by the Korean National Police Agency (KNPA) and the Ministry of Science and ICT (MSIT), managed by the Korea Institute of Police Technology (KIPoT)

- Developing deep learning techniques for detecting and identifying illicit drug advertisements on social media, dark web, and Telegram, covering drug slang database construction, multimodal advertisement classification, and adaptive handling of evolving slang and obfuscation patterns

Attack Scenario Analysis and Hybrid RAG Knowledge Base Construction Jan. 2026–Present
Based on MITRE ATT&CK and D3FEND

Part of the *Development of an AI White-Hacker-based Zero-Hacking System* program led by the Korea Institute of Science and Technology Information (KISTI), in collaboration with KAIST

- Designing and building the ATT&CK/D3FEND-grounded knowledge database that enables an LLM-based attack profiler to reason over multi-stage intrusion scenarios

Development of Cyber Security Regulation Technologies for Programmable Mar.–Dec. 2025
Logic Devices in the Development Phase of New Nuclear Reactors

Funded by the Korea Foundation of Nuclear Safety (KoFONS)

- Analyzed the FPGA development lifecycle, existing nuclear safety regulatory requirements, and known security vulnerabilities to derive development-phase cybersecurity requirements

Analysis of Security Evaluation Techniques for Boundary Protection to Jul.–Dec. 2024
Support Defense-in-Depth Strategies in Nuclear Facilities

Funded by the Korea Institute of Nuclear Nonproliferation and Control (KINAC)

- Surveyed boundary protection technologies applied to essential digital assets in nuclear facilities, developed security inspection procedures, and proposed regulatory application measures supporting the revision of the KINAC/RS-015 inspection and audit guideline

TEACHING EXPERIENCE

- **Machine Learning**, Teaching Assistant, Sungkyunkwan University Fall 2026
- **Derivatives**, Teaching Assistant, Sungkyunkwan University Fall 2026
- **Introduction to Data Analysis and AI**, Teaching Assistant, Sungkyunkwan University Spring 2026
- **AI Basics & Uses**, Teaching Assistant, Sungkyunkwan University Spring 2024–Fall 2025
Six semesters, from 2024 Spring through 2025 Fall
- **R&E (Research and Education) Program**, Seoul Science High School Mar.–Dec. 2024
Designed and led the R&E program organized by Seoul Science High School, mentoring the student project *Developing a Spam Detection Model Specifically Designed for Adolescents*
- **Problem Solving and Algorithm**, Teaching Assistant, Sungkyunkwan University Fall 2023
- **Teaching Practicum Student**, Sunae High School Apr. 2023

REVIEWING EXPERIENCE

- Conferences: CIKM '26, SAC '26

SKILLS

- Languages: Python, C/C++, SQL, Bash, L^AT_EX
- Software Tools: PyTorch, Transformers, Scikit-Learn, NumPy, Pandas, Git, Docker, Neo4j
- Spoken Languages: Korean (native), English (professional)