March 2026

Insup Lee

AI & Security Researcher

islee94@korea.ac.kr | Homepage | LinkedIn | Google Scholar | ORCiD

Research Statement

My research focuses on the intersection of AI and cybersecurity. I have designed **security-specific generative models** (e.g., diffusion transformers and GANs) to address data insufficiency in physical and wireless security, including RF signal processing and side-channel analysis (SCA). I have also advanced **cyber threat intelligence (CTI)** using NLP and LLMs to analyze attack campaigns. While I maintain active collaborations in these areas, my primary focus now transitions toward **securing AI itself**. I will apply my structural understanding of generative models and security expertise to investigate vulnerabilities within **LLMs** and **agentic AI systems**, and to ensure their trustworthiness.

Education

Ph.D. Candidate in Cybersecurity, Korea University – Seoul, Republic of Korea — Sep 2019 – Present

- Title: Domain-Specific Generative Models for Data Augmentation in Multi-Layer Cybersecurity
- Advisors: Prof. Sangjin Lee and Prof. Seokhie Hong | Expected Graduation: Aug 2026

B.E. in Cyber Defense, Korea University – Seoul, Republic of Korea — Mar 2014 – Feb 2018

- Advisor: Prof. Jongin Lim

Employment History

Lecturer, Korea University – Seoul, Republic of Korea — Sep 2025 – Feb 2026

Research Intern, Indiana University Bloomington – Remote — Mar 2025 – Jun 2025

- Explored adversarial attacks on ML systems in autonomous vehicles (Advisor: Prof. Hyungsub Kim)

Research Engineer (Cyber Officer), Ministry of National Defense – Republic of Korea — Aug 2023 – May 2025

- Led international joint research on AI-based security with the UAE Ministry of Defense as PI
- Investigated AI-based RF signal analysis for drone security ([J6])

Researcher, Agency for Defense Development (ADD) – Seoul, Republic of Korea — Jul 2018 – Jul 2023

- Conducted AI-based security research and in-house software development (PI / Mentor: Prof. Changhee Choi)
- Analyzed nation-sponsored cyber attacks using NLP technologies ([J1]-[J3], [J5])
- Applied generative models for cybersecurity data augmentation ([C1], [C2])

Selected Publications

A representative selection of my work focusing on trustworthy AI, security-specific generative models, and system security

1. **[CAL 2026] I. Lee** *et al.*, "LeakDiT: Diffusion Transformers for Trace-Augmented Side-Channel Analysis"
2. **[SPL 2025] I. Lee** *et al.*, "Enhancing Modulation Classification via Diffusion Transformers for Drone Video Signal Processing"
3. **[TDSC 2024] I. Lee** *et al.*, "UniQGAN: Towards Improved Modulation Classification With Adversarial Robustness Using Scalable Generator Design"
4. **[TIFS 2025] I. Lee** *et al.*, "MuCamp: Generating Cyber Campaign Variants via TTP Synonym Replacement for Group Attribution"
5. **[DAC 2026]** D. Bae, S. Park, **I. Lee**, *et al.*, "Exploiting Per-Core Leakage: Electromagnetic Side-Channel Monitoring of Multicore Architectures"

Awards and Honors

- KU Graduate School Achievement Award — Feb 2026
  Korea University, Seoul, Republic of Korea
- Outstanding Paper Award — Nov 2025
  CISC-W'25, KIISC
- Certificate of Commendation (UAE-ROK Engagement Program) — Mar 2025
  United Arab Emirates Ministry of Defense
- Ambassador's Commendation — Mar 2025
  Embassy of the Republic of Korea to the United Arab Emirates
- Full Tuition Scholarship (Korea University) — Mar 2014 – Feb 2018
  Ministry of National Defense, Republic of Korea

Mentoring Experience

- Sujin Park (Ph.D. Student at Korea University) — Jun 2025 – Present
  Mentored research on side-channel analysis for anomaly detection, resulting in two co-authored domestic conference papers and an Outstanding Paper Award
- Hyunjun Park (Navy Lieutenant at Ministry of National Defense) — Nov 2024 – Feb 2025
  Supervised research on DDoS detection via transfer learning, resulting in a domestic journal publication as the corresponding author
- Kangmun Kim (First Lieutenant at Cyber Operations Command) — Jan 2024 – Sep 2024
  Supervised research on web shell detection via user behavior embedding, resulting in a domestic journal publication as the corresponding author

Teaching Experience

- Lecturer, Computer Networks (SCS302, Fall 2025), Korea University — Sep 2025 - Dec 2025
- Instructor, Penetration Testing - Intermediate, UAE Ministry of Defense — Sep 2024
- Instructor, Penetration Testing - Basic, UAE Ministry of Defense — Jul 2024

Professional Service

Reviewer

- IEEE Transactions on Dependable and Secure Computing (TDSC), 2025
- IEEE Transactions on Information Forensics and Security (TIFS), 2026
- IEEE Transaction on Communications (TCOM), 2025, 2026
- IEEE Journal on Selected Areas in Communications (JSAC), 2025, 2026

Other Experience

AI Cyber Challenge (AIxCC), DARPA and ARPA-H, USA — Apr 2024 – Aug 2024

- Participated in the semifinal round as a member of Team KORIA, submitting our cyber reasoning system that leverages LLMs for automated detection and patching of software vulnerabilities

SW Outsourcing Development, KCMVP-Certified Cryptographic Module — Jun 2017 – May 2018

- Implemented a cryptographic module with 25,000 LoC in C - ARIA block cipher (modes: ECB, CBC, CTR), hash functions (SHA-256, SHA-512), and HMAC-based DRBG for Windows (.dll) and Linux (.so)

Full Publications

Under Review

- S. Park, D. Bae, **I. Lee**, J. Kim, H. Oh, H. Kim, and S. Hong, "Multi-Domain Side-Channel Analysis for Anomaly Detection in Embedded System," submitted to IEEE Embedded Systems Letters.
- J. Baek, G. Ahn, S. Park, D. Bae, G. Kim, **I. Lee**, H. Kim, and S. Hong, "-," submitted to ACM CCS 2026.

International Publications

(C: Conference, J: Journal)

C3 D. Bae, S. Park, **I. Lee**, Y. Jung, K. Lee, H. Kim, and S. Hong, "Exploiting Per-Core Leakage: Electromagnetic Side-Channel Monitoring of Multicore Architectures," ACM/IEEE Design Automation Conference (**DAC**), Jul. 2026.

J8 **I. Lee**, D. Bae, S. Hong, and S. Lee, "LeakDiT: Diffusion Transformers for Trace- Augmented Side-Channel Analysis," IEEE Computer Architecture Letters, Vol. 25, No. 1, pp. 5-8, Jan./Jun. 2026.

J7 H. Kim, D. Lee, **I. Lee**, S. Lee, and S. Lee, "Multi-Step LLM Pipeline for Enhancing TTP Extraction in Cyber Threat Intelligence," IEEE Access, Vol. 13, pp. 179696-179710, Oct. 2025.

J6 **I. Lee**, K. Alteneiji, and M. Alghfeli, "Enhancing Modulation Classification via Diffusion Transformers for Drone Video Signal Processing," IEEE Signal Processing Letters, Vol. 32, pp. 3325-3329, Aug. 2025.

J5 **I. Lee** and C. Choi, "MuCamp: Generating Cyber Campaign Variants via TTP Synonym Replacement for Group Attribution," IEEE Transactions on Information and Forensics Security (**TIFS**), Vol. 20, pp. 6162-6174, Jun. 2025.

J4 **I. Lee** and W. Lee, "UniQGAN: Towards Improved Modulation Classification With Adversarial Robustness Using Scalable Generator Design," IEEE Transactions on Dependable and Secure Computing (**TDSC**), Vol. 21, No. 2, pp. 732-745, Mar./Apr. 2024.

J3 **I. Lee** and C. Choi, "Camp2Vec: Embedding Cyber Campaign With ATT&CK Framework for Attack Group Analysis," ICT Express, Vol. 9, No. 6, pp. 1065-1070, Dec. 2023.

J2 C. Shin, **I. Lee**, and C. Choi, "Exploiting TTP Co-occurence via GloVe-Based Embedding With ATT&CK Framework," IEEE Access, Vol. 11, pp. 100823-100831, Sep. 2023.

J1 Y. Kim, **I. Lee**, H. Kwon, G. Lee, and J. Yoon, "BAN: Predicting APT Attack Based on Bayesian Network With MITRE ATT&CK Framework," IEEE Access, Vol. 11, pp. 91949-94968, Aug. 2023.

C2 S. Shin, **I. Lee**, and C. Choi, "Anomaly Dataset Augmentation Using Sequence Generative Models," IEEE International Conference on Machine Learning and Applications, Dec. 2019.

C1 C. Choi, S. Shin, and **I. Lee**, "Opcode Sequence Amplifier Using Sequence Generative Adversarial Networks," International Conference on ICT Convergence (ICTC), Oct. 2019.

Domestic Publications (Korean)

(†: Corresponding Author)

- S. Park, D. Bae, **I. Lee**, H. Kim, and S. Hong, “EM-Based Anomaly Detection using a Dual-Domain Approach,” in Proc. of the KIISC Winter Conference (CISC-W), Nov. 2025. (Selected as an Outstanding Paper Award)
- S. Park, D. Bae, **I. Lee**, H. Kim, and S. Hong, “A Statistical Time-Domain Approach to Anomaly Detection for Robotic-Arm MCU,” in Proc. of the KIMST Fall Conference, Nov. 2025.
- H. Park and **I. Lee**†, “Enhanced DDoS Detection via Traffic Volume-Based Labeling and Transfer Learning,” Journal of Internet Computing and Services (JICS), Vol. 26, No. 4, pp. 1-8, Aug. 2025.
- K. Kim and **I. Lee**†, “User Behavior Embedding via TF-IDF-BVC for Web Shell Detection,” Journal of The Korea Institute of Information Security & Cryptology (JKIISC), Vol. 34, No. 6, pp. 1231-1238, Dec. 2024.

Patents

- C. Choi and **I. Lee**, "Method for Augmentating Cyber Attack Campaign Data to Identify Attack Group, and Security," Korea Patent Application Number. 10-2024-0176082, December 2, 2024.
- C. Choi, **I. Lee**, C. Shin, and S. Lee, "Information Identification Method and Electronic Apparatus Thereof," Korea Patent Application Number. 10-2024-0006106, January 15, 2024.
- C. Choi, C. Shin, S. Shin, S. Seo, and **I. Lee**, "Method for Training Attack Prediction Model and Device Therefor," U.S. Patent Application Number. 18/126,005; U.S. Patent Number. US20230308462A1, September 28, 2023.
- C. Choi, S. Shin, and **I. Lee**, “Apparatus, Method, Computer-readable Storage Medium and Computer Program for Generating Operation Code,” Korea Patent Application Number. 10-2019-0141865, November 07, 2019; Korea Patent Number. 10-2246797, April 30, 2021.

March 2026

Reference

Sangjin Lee
Professor, School of Cybersecurity, Korea University
Relationship: Ph.D. Advisor
Email: sangjin@korea.ac.kr

Seokhie Hong
Professor, School of Cybersecurity, Korea University
Relationship: Ph.D. Advisor
Email: shhong@korea.ac.kr

Changhee Choi
Associate Professor, Department of Cyber Defense, Sejong University
Relationship: Research Mentor (Former PI at ADD)
Email: choich@sejong.ac.kr

Jongin Lim
Professor Emeritus, School of Cybersecurity, Korea University
Former Special Presidential Advisor for Cybersecurity, Republic of Korea
Relationship: Undergraduate Advisor
Email: jilim76@gmail.com