

Insup Lee

islee94@korea.ac.kr | [Homepage](#) | [LinkedIn](#) | [Google Scholar](#) | [ORCID](#)

Research Interests

- AI-based security, Secure communications, Network security, Side-channel analysis, and Generative models

Education

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

- Advisors: Prof. Sangjin Lee and Prof. Seokhie Hong

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

Employment History

Lecturer, Korea University – Seoul, Republic of Korea Sep 2025 – Present

Research Intern, Indiana University – Bloomington, Indiana, USA Mar 2025 – Jun 2025

Security Engineer, Ministry of National Defense – Republic of Korea Aug 2023 – May 2025

- Led AI-based security projects and taught cybersecurity courses in the UAE
- Published one international paper [J7] and 2 domestic papers [D2, D3]

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

- Conducted AI-based security research and in-house software development (Advisor: Prof. Changhee Choi)
 - (1) "Detection of Nation-Sponsored Cyber Attacks Using NLP Technologies" (Apr 2021 – Jul 2023)
 - (2) "Generative Models for Cybersecurity Data Augmentation" (Jun 2019 – Oct 2020)
 - (3) "IPADS: Integrated Proactive and Adaptive Defense Systems" (Aug 2018 – May 2019)
- Published seven international papers [C1, C2, J2, J3, J4, J6, J8], four patents, and 12 domestic papers

Publications

Under Review

- Sujin Park, Daehyeon Bae, Insup Lee, Jeonghyeok Kim, Haengrok Oh, Heeseok Kim, Seokhie Hong, "Multi-Domain Side-Channel Analysis for Anomaly Detection in Embedded System,"
- Jiwoo Baek, Gilsang Ahn, Sujin Park, Daehyeon Bae, Gysang Kim, Insup Lee, Heeseok Kim, Seokhie Hong, "-",
- Daehyeon Bae, Sujin Park, Insup Lee, Young-Giu Jung, Kyeongsik Lee, Heeseok Kim, Seokhie Hong, "-",

Journal Publications

- J9 Insup Lee, Daehyeon Bae, Seokhie Hong, and Sangjin Lee, "LeakDiT: Diffusion Transformers for Trace-Augmented Side-Channel Analysis," *IEEE Computer Architecture Letters (CAL)*, Vol. 25, No. 1, pp. 5-8, Jan./Jun. 2026.
- J8 Hyoungrok Kim, Donghyeon Lee, Insup Lee, Soohan Lee, and Sangjin Lee, "Multi-Step LLM Pipeline for Enhancing TTP Extraction in Cyber Threat Intelligence," *IEEE Access*, Vol. 13, pp. 179696-179710, Oct. 2025.
- J7 Insup Lee, Khalifa Alteneiji, and Mohammed Alghfeli, "Enhancing Modulation Classification via Diffusion Transformers for Drone Video Signal Processing," *IEEE Signal Processing Letters (SPL)*, Vol. 32, pp. 3325-3329, Aug. 2025.
- J6 Insup Lee and Changhee 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.
- J5 Insup Lee and Wonjun 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.

- J4 Insup Lee and Changhee Choi, "Camp2Vec: Embedding Cyber Campaign With ATT&CK Framework for Attack Group Analysis," *ICT Express*, Vol. 9, No. 6, pp. 1065-1070, Dec. 2023.
- J3 Chanhoo Shin, Insup Lee, and Changhee Choi, "Exploiting TTP Co-occurrence via GloVe-Based Embedding With ATT&CK Framework," *IEEE Access*, Vol. 11, pp. 100823-100831, Sep. 2023.
- J2 Youngjun Kim, Insup Lee, Hyuk Kwon, Gyeongsik Lee, and Jiwon Yoon, "BAN: Predicting APT Attack Based on Bayesian Network With MITRE ATT&CK Framework," *IEEE Access*, Vol. 11, pp. 91949-94968, Aug. 2023.
- J1 Insup Lee and Wonjun Lee, "UniQGAN: Unified Generative Adversarial Networks for Augmented Modulation Classification," *IEEE Communications Letters (CL)*, Vol. 26, No. 2, pp.355-358, Feb. 2022.

Conference Publications

- C3 Insup Lee, Heejun Roh, and Wonjun Lee, "Encrypted Malware Traffic Detection Using Incremental Learning," *IEEE INFOCOM - Poster Session*, Jul. 2020.
- C2 Sunguk Shin, Insup Lee, and Changhee Choi, "Anomaly Dataset Augmentation Using Sequence Generative Models," *IEEE International Conference on Machine Learning and Applications*, Dec. 2019.
- C1 Changhee Choi, Sunguk Shin, and Insup Lee, "Opcode Sequence Amplifier Using Sequence Generative Adversarial Networks," *International Conference on ICT Convergence (ICTC)*, Oct. 2019.

Domestic Journal Publications (Korean)

- D3 Hyunjun Park and Insup 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.
- D2 Kangmun Kim and Insup 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.
- D1 Yongbin Park, Sunguk Shin, and Insup Lee, "A Study on Evaluation Method of NIDS Datasets in Closed Military Network," *Journal of Internet Computing and Services (JICS)*, Vol. 21, No. 2, pp. 121-130, Apr. 2020.

Patents

- Changhee Choi and Insup Lee, "Method for Augmentating Cyber Attack Campaign Data to Identify Attack Group, and Security," Korea Patent Application Number. 10-2024-0176082, December 2, 2024.
- Changhee Choi, Insup Lee, Chanhoo Shin, and Sungho Lee, "Information Identification Method and Electronic Apparatus Thereof," Korea Patent Application Number. 10-2024-0006106, January 15, 2024.
- Changhee Choi, Chanhoo Shin, Sunguk Shin, Seongyeon Seo, and Insup 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.
- Changhee Choi, Sunguk Shin, and Insup Lee, "Appratus, 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.

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)

Awards and Honors

- Outstanding Paper Award, CISC-W'25, KIISC (Paper Title: EM-Based Anomaly Detection using a Dual-Domain Approach) Nov 2025

- Ambassador's Commendation for excellence in defense cooperation, Embassy of the Republic of Korea to the United Arab Emirates Mar 2025
- The 3rd Prize, Military Cybersecurity Experts Hackathon, Ministry of Science and ICT, Republic of Korea Dec 2023
- Full Tuition Scholarship, Ministry of National Defense, Republic of Korea Mar 2014 – Feb 2018

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

Teaching Experience

- Lecturer, Fall 2025: Computer Networks (SCS302), Korea University

Mentoring Experience

- **Sujin Park** (Ph.D. Student at Korea University) Jun 2025 – Present
Side-channel analysis for anomaly detection
- **Hyunjun Park** (Navy Lieutenant at Ministry of National Defense) Nov 2024 – Feb 2025
DDoS detection via transfer learning (paper published at JICS)
- **Kangmun Kim** (First Lieutenant at Cyber Operations Command) Jan 2024 – Sep 2024
Web shell detection via user behavior embedding (paper published at JKIISC)

Technical Skills

- AI & Deep Learning: Generative models (diffusion transformers, GANs), LLM pipelines, Adversarial robustness
- Cybersecurity: Side-channel analysis, CTI (TTP extraction, attribution), Cryptographic engineering (25k+ LoC)
- Languages & Tools: Python, C/C++ , CUDA, PyTorch, Linux, Git, Docker, Streamlit