

Insup Lee

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

Summary

I am an AI & Security Researcher based in Abu Dhabi, UAE, working on generative models for cybersecurity and drones. Previously, I spent five years as a researcher at the Agency for Defense Development (ADD), conducting research in AI-driven cybersecurity. I am also a Ph.D. candidate in Cybersecurity at Korea University, where I earned my B.E. in Cyber Defense. My research interests lie at the **intersection of AI and cybersecurity**, focusing on generative models, AI-driven security, network security, and secure communications.

Research Interests

- **AI for Cybersecurity:** threat intelligence using NLP/LLM, HW security (side-channel analysis), adversarial ML
- **Network and Wireless Security:** drones, robust communications, network IDS, anomaly detection
- **Generative Models:** diffusion transformers and GANs for data augmentation, LLM for vulnerability detection

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

- Studied computer science, cybersecurity, cryptography, and secure coding

Employment History

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

- Taught graduate-level course "Computer Networks (SCS 302)"

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

- Researched quantification methods for ML security in autonomous vehicle systems

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 ([UAE ambassador's commendation](#))
- Executed cyber defense operations and developed automation tools at the Cyber Operations Command
- 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

Technical Skills

- Frameworks/Tools: PyTorch, Keras, TensorFlow, scikit-learn, pandas, Git, Streamlit
- Programming Languages: Python, C, JavaScript, SQL

Publications

Under Review

- (Blind Review)
Daehyeon Bae, Sujin Park, Insup Lee, Young-Giu Jung, Kyeongsik Lee, Heeseok Kim, Seokhie Hong
- (Blind Review)
Sujin Park, Daehyeon Bae, Insup Lee, Jeonghyeok Kim, Haengrok Oh, Heeseok Kim and Seokhie Hong

Journal Articles

- J9 [LeakDiT: Diffusion Transformers for Trace-Augmented Side-Channel Analysis](#)
Insup Lee, Daehyeon Bae, Seokhie Hong, and Sangjin Lee
IEEE Computer Architecture Letters, 2025
(SCI 2024 I/F Top 79.2% in Computer Science, Hardware & Architecture)
- J8 [Multi-Step LLM Pipeline for Enhancing TTP Extraction in Cyber Threat Intelligence](#)
Hyoungrok Kim, Donghyeon Lee, Insup Lee, Soohan Lee, and Sangjin Lee
IEEE Access, 2025
(SCI 2024 I/F Top 34.8% in Engineering, Electrical & Electronic)
- J7 [Enhancing Modulation Classification via Diffusion Transformers for Drone Video Signal Processing](#)
Insup Lee, Khalifa Alteneiji, and Mohammed Alghfeli
IEEE Signal Processing Letters, 2025
(SCI 2024 I/F Top 31.6% in Engineering, Electrical & Electronic)
- J6 [MuCamp: Generating Cyber Campaign Variants via TTP Synonym Replacement for Group Attribution](#)
Insup Lee and Changhee Choi
IEEE Transactions on Information and Forensics Security (TIFS), 2025
(SCI 2024 I/F Top 7.8% in Computer Science, Theory & Methods)
- J5 [UniQGAN: Towards Improved Modulation Classification With Adversarial Robustness Using Scalable Generator Design](#)
Insup Lee and Wonjun Lee
IEEE Transactions on Dependable and Secure Computing (TDSC), 2024
(SCI 2023 I/F Top 4.9% in Computer Science, Software Engineering)
- J4 [Camp2Vec: Embedding Cyber Campaign With ATT&CK Framework for Attack Group Analysis](#)
Insup Lee and Changhee Choi
ICT Express, 2023
(SCI 2023 I/F Top 23.0% in Computer Science, Information Systems)
- J3 [Exploiting TTP Co-occurrence via GloVe-Based Embedding With ATT&CK Framework](#)
Chanho Shin, Insup Lee, and Changhee Choi
IEEE Access, 2023
(SCI 2023 I/F Top 34.4% in Engineering, Electrical & Electronic)
- J2 [BAN: Predicting APT Attack Based on Bayesian Network With MITRE ATT&CK Framework](#)
Youngjun Kim, Insup Lee, Hyuk Kwon, Gyeongsik Lee, and Jiwon Yoon
IEEE Access, 2023
(SCI 2023 I/F Top 34.4% in Engineering, Electrical & Electronic)
- J1 [UniQGAN: Unified Generative Adversarial Networks for Augmented Modulation Classification](#)
Insup Lee and Wonjun Lee
IEEE Communications Letters, 2022
(SCI 2023 I/F Top 33.2% in Telecommunications)

Conference Proceedings

- C3 [Encrypted Malware Traffic Detection Using Incremental Learning](#)
Insup Lee, Heejun Roh, and Wonjun Lee
IEEE International Conference on Computer Communications (INFOCOM) - Poster Session, 2020
- C2 [Anomaly Dataset Augmentation Using Sequence Generative Models](#)
Sunguk Shin, Insup Lee, and Changhee Choi
IEEE International Conference on Machine Learning and Applications (ICMLA), 2019

C1 [Opcode Sequence Amplifier Using Sequence Generative Adversarial Networks](#)

Changhee Choi, Sunguk Shin, and Insup Lee

International Conference on ICT Convergence (ICTC), 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.

Domestic Conference Publications (Korean)

- Sujin Park, Daehyeon Bae, Insup Lee, Heeseok Kim, and Seokhie 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)
- Jebin Kim, Insup Lee, Chanho Jeon, Suhri Kim, Seokhie Hong, and Sangjin Lee, "Reinforcement Learning for Parameter Optimization in CADO-NFS Polynomial Selection," in *Proc. of the KIISC Winter Conference (CISC-W)*, Nov. 2025.
- Sujin Park, Daehyeon Bae, Insup Lee, Heeseok Kim, and Seokhie Hong, "A Statistical Time-Domain Approach to Anomaly Detection for Robotic-Arm MCU," in *Proc. of the KIMST Fall Conference*, Nov. 2025.
- Insup Lee, Chanho Shin, and Changhee Choi, "Mutating Cyber Camapaign With TTP Word Replacement," in *Proc. of the KIMST Annual Conference*, Jun. 2023.
- Chanho Shin, Insup Lee, and Changhee Choi, "Towards GloVe-Based TTP Embedding With ATT&CK Framework," in *Proc. of the KIMST Annual Conference*, Jun. 2023.
- Changhee Choi, Insup Lee, Chanho Shin, and Sungho Lee, "Cyber Threat Campaign Analysis Based on PEGASUS and RoBERTa Model," in *Proc. of the KIMST Annual Conference*, Jun. 2023.
- Insup Lee, Chanho Shin, Sunguk Shin, Seongyeon Seo, and Changhee Choi, "Analyzing Cyberattack Campaign Similarity via TTP Sequence Embedding," in *Proc. of the KIMST Annual Conference*, Jun. 2022.
- Sunguk Shin, Insup Lee, Chanho Shin, Seongyeon Seo, and Changhee Choi, "Cyber Campaign Analysis With TTP Embedding Using TF-IDF," in *Proc. of the KIMST Annual Conference*, Jun. 2022.
- Chanho Shin, Sunguk Shin, Insup Lee, Seongyeon Seo, and Changhee Choi, "Classifying TTP Based on CIA Labeling," in *Proc. of the KIMST Annual Conference*, Jun. 2022.
- Changhee Choi, Chanho Shin, Sunguk Shin, Seongyeon Seo, and Insup Lee, "Cyber Attack Group Classification Using Siamese LSTM," in *Proc. of the KIMST Annual Conference*, Jun. 2022.
- Chanho Shin, Sunguk Shin, Seongyeon Seo, Insup Lee, and Changhee Choi, "Embedding and Training RNN to Estimating the Goal of Cyber Attack," in *Proc. of the KIMST Fall Conference*, Nov. 2021.
- Sunguk Shin, Chanho Shin, Seongyeon Seo, Insup Lee, and Changhee Choi, "The Proposed Approach for Country Prediction With TTP-based Cyber Data Using GCN," in *Proc. of the KIMST Fall Conference*, Nov. 2021.
- Changhee Choi, Chanho Shin, Sunguk Shin, Seongyeon Seo, and Insup Lee, "Deep Learning for Estimating Next Action of Cyber Attack," in *Proc. of the KIMST Fall Conference*, Nov. 2021.
- Insup Lee, Jinguok Kim, and Jeongchan Park, "Analysis of Weight Setting in Incremental Learning to Improve Real-Time Intrusion Detection," in *Proc. of the KIMST Annual Conference*, Jun. 2019.

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, Chanho Shin, and Sungho Lee, "Information Identification Method and Electronic Apparatus Thereof," Korea Patent Application Number. 10-2024-0006106, January 15, 2024.
- Changhee Choi, Chanho 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 while following secure coding conventions
- Covered the ARIA block cipher (modes: ECB, CBC, CTR), hash functions (SHA-256, SHA-512), and HMAC-based DRBG for Windows (.dll) and Linux (.so), respectively

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

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)

Professional Service

Reviewer

- IEEE Transactions on Dependable and Secure Computing (TDSC), 2025
- IEEE Transaction on Communications (TCOM), 2025
- IEEE Journal on Selected Areas in Communications (JSAC), 2025
- IEEE International Conference on Computer Communications (INFOCOM), 2023-2024
- IEEE Communications Letters, 2022

Teaching Experience

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