

Insup Lee

insuplee94@gmail.com | [LinkedIn](#) | [Homepage](#) | [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, adversarial machine learning, and secure communications.

Research Interests

- **AI + Security:** AI for cybersecurity, adversarial ML, NLP for threat intelligence, LLM for vulnerability detection
- **Generative Models:** diffusion models with transformers, GANs, robustness via data augmentation
- **Network and Wireless Security:** drones, robust communications, anomaly detection, network IDS, etc.

Education

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

- Completed all required coursework and passed Ph.D. qualifying examination
- Researched generative models to enhance robustness in communication systems

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

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

- Collaborated with international colleagues and led AI-based security projects in the UAE
- Executed cyber defense operations and developed automation tools at the Cyber Operations Command

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

- ADD is a South Korean government agency dedicated to defense R&D, including cybersecurity and AI
- Carried out three AI-driven cybersecurity projects, conducting research and in-house software development
 - (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 six international papers [C1, C2, J2, J3, J4, J6], four patents, and 12 domestic papers

Technical Skills

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

Research Projects

Diffusion Models for Enhanced Drone Communications Mar 2024 - Present

- Keywords: diffusion models, vision transformers, drone communications, adversarial robustness
- Frameworks/Tools: PyTorch
- Publications: two papers are under review

Detection of Nation-Sponsored Cyber Attacks Using NLP Technologies Apr 2021 - Jul 2023

- Keywords: cyber threat intelligence, NLP, data augmentation, embedding, SOAR, MITRE ATT&CK
- Frameworks/Tools: PyTorch, scikit-learn, FastAPI, Git, PostgreSQL
- Publications: [J2], [J3], [J4], [J6] & one paper is under review

Generative Adversarial Networks for Robust Modulation Classification May 2020 - Dec 2022

- Keywords: wireless communications, GANs, adversarial attacks, I/Q data augmentation, adversarial robustness
- Frameworks/Tools: PyTorch, IBM ART
- Publications: [J1], [J5]

Generative Models for Cybersecurity Data Augmentation Jun 2019 - Oct 2020

- Keywords: host IDS, sequence data, CycleGAN, SeqGAN, Seq2Seq, ADFA-LD
- Frameworks/Tools: TensorFlow, Node.js, Git
- Publications: [C1], [C2]

Network Intrusion Detection Systems Using Incremental Learning Sep 2019 - Apr 2020

- Keywords: network IDS, machine learning, encrypted traffic classification, incremental learning
- Frameworks/Tools: scikit-learn
- Publications: [C3]

IPADS: Integrated Proactive and Adaptive Defense Systems Aug 2018 - May 2019

- Keywords: anomaly detection, network IDS, in-vehicle network, MilCAN, CIC-IDS2017
- Frameworks/Tools: scikit-learn

Other Experience

AI Cyber Challenge (AICCC), 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

- 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

Publications

Under Review

- [Multi-Step LLM Pipeline for Enhancing TTP Extraction in Cyber Threat Intelligence](#)
Hyoungrok Kim, Donghyeon Lee, [Insup Lee](#), Soohan Lee, and Sangjin Lee
- [Enhancing Modulation Classification via Diffusion Transformers for UAV Video Signal Processing](#)
[Insup Lee](#), Khalifa Alteneiji, and Mohammed Alghfeli

Journal Articles

- 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 2023 I/F Top 9.03% 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 5.30% 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 23.29% 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 34.66% 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 34.66% 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 33.61% 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

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.

Domestic Journals and Conferences (Korean)

- 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.
- 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.
- 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.
- Insup Lee, Jingoek 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.

Mentoring Experience

- | | |
|---|---------------------|
| • Hyunjun Park (Navy Lieutenant at Ministry of National Defense)
DDoS detection via transfer learning (paper submitted to JICS) | Nov 2024 – Feb 2025 |
| • Kangmun Kim (First Lieutenant at Cyber Operations Command)
Web shell detection via user behavior embedding (paper published at JKIISC) | Jan 2024 – Sep 2024 |

Professional Service

Reviewer

- IEEE Transactions on Dependable and Secure Computing (TDSC), 2025
- IEEE International Conference on Computer Communications (INFOCOM), 2023-2024
- IEEE Communications Letters, 2022
- ICT Express, 2025