Younghan Lee

Email: 201younghanlee@gmail.com
Phone: + 82)10-9103-5353
Portfolio: 201younghanlee.github.io

EDUCATION

2017 – 2024 **Seoul National University**, Seoul, *Republic of Korea*
Ph.D. in Electrical and Computer Engineering
Thesis: Solving Contemporary Security Problems in Deep Learning
Advisor: Yunheung Paek

2013 – 2016 **Imperial College London**, *London, United Kingdom*
BEng in Electrical and Electronic Engineering

EMPLOYMENT HISTORY

2024 – Present **Seoul National University**, Seoul, *Republic of Korea*
Postdoctoral Researcher
Advisor: Yunheung Paek

2024 – Present **Soongsil University**, Seoul, *Republic of Korea*
Lecturer
Department of AI·Techno Convergence

2024 – Present **Sungshin Women's University**, Seoul, *Republic of Korea*
Lecturer
Department of Convergence Security Engineering

RESEARCH INTEREST

Security and Privacy in AI, Adversarial Example Attacks, Model Extraction Attacks, Federated Learning, Differential Privacy, Multimodal Learning, Robotics

PUBLICATIONS

2023 **FLGuard: Byzantine-Robust Federated Learning via Ensemble of Contrastive Models**
Younghan Lee, Yungi Cho, Woorim Han, Ho Bae, Yunheung Paek. *European Symposium on Research in Computer Security (ESORICS)*

2023 **Exploring Clustered Federated Learning's Vulnerability against Property Inference Attack**
Hyunjun Kim*, Yungi Cho*, **Younghan Lee**, Ho Bae, Yunheung Paek, *Equal Contribution. *International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*

2022 **Precise Extraction of Deep Learning Models via Side-Channel Attacks on Edge/Endpoint Devices**
Younghan Lee, Sohee Jun, Yungi Cho, Woorim Han, Hyungon Moon, Yunheung Paek. *European Symposium on Research in Computer Security (ESORICS)*

2022 **A pilot study of machine-learning-based algorithms to assist integrated care for older community-dwelling adults**

So Im Ryu, **Younghan Lee**, Sohee Jun, Yunheung Paek, Hongsoo Kim, BeLong Cho, Yeon-Hwan Park. *Computers, Informatics, Nursing (CIN)*

2021 **Learn2Evade: Learning-based Generative Model for Evading PDF Malware Classifiers**
Ho Bae*, **Younghan Lee***, Yohan Kim, Uiwon Hwang, Sungroh Yoon, Yunheung Paek, *Equal Contribution. *IEEE Transactions on Artificial Intelligence (IEEE TAI)*

2020 **Hawkware: Network Intrusion Detection based on Behavior Analysis with ANNs on an IoT Device**
Sunwoo Ahn, Hayoon Yi, **Younghan Lee**, Whoi Ree Ha, Giyeol Kim, Yunheung Paek. *Design Automation Conference (DAC)*

2019 **Riskim: Toward complete kernel protection with hardware supportq**
Dongil Hwang, Myonghoon Yang, Seongil Jeon, **Younghan Lee**, Donghyun Kwon, Yunheung Paek. *Design, Automation & Test in Europe Conference & Exhibition (DATE)*

2018 **Mimicry resilient program behavior modeling with LSTM based branch models**
Hayoon Yi, Gyuwan Kimy, Jangho Leey, Sunwoo Ahn, **Younghan Lee**, Sungroh Yoon, Yunheung Paek. *Deep Learning and Security Workshop*

PORJECTS

2023 – Present **Motion Tracking System for the Analysis of the Activity and Emotional Patterns of Pets with Deep Learning**, *Seoul National University (SNU)*

2023 – Present **Development of Artificial Intelligence-based Phishing Attack Prevention and Performance Verification Technology**, *Seoul Business Agency (SBA)*

2022 – Present **Deriving Differential Privacy Concepts Applicable to National Statistical Data and Addressing Issues to Ensure the Usefulness of Statistical Analysis**, *Statistics Korea (KOSTAT)*

2022 – Present **Research on Applying Artificial Intelligence on Medical Data**, *Ewha Womans University Medical Center (EUMC)*

2023 – 2023 **Protecting Images from Cyber Phishing Attacks using De-identification**, *Cubig*.ai

2023 – 2023 **Developing Differential Privacy based Image Generation Artificial Intelligence**, *Cubig.ai*

2020 – 2021 **Research on Applying Machine Learning on Health and Nursing Data**, *Seoul National University Hospital (SNUH)*

2019 – 2020 **Development of Intelligent Security Threat Countermeasure Solution based on Aritificial Intelligence**, *Seoul Business Agency (SBA)*

2017 – 2020 **Development of Programmable IPs and Unified SDK to Enable Building Security-Integrated Computer Systems**, *Ministry of Science and ICT*

2017 – 2019 **Development of Cloud-based Intelligent Security Technology for Providing Customized Security Services**, *Ministry of Science and ICT*

2016 – 2017 **Development of Network Anomaly Detection**, *SK Infosec*

TEACHING

2024 AI Programming (5048923201)
Department of AI Techno-Convergence, Soongsil University

2024 Machine Learning-based Communication Networks Security (1000717-001)
Department of Convergence Security Engineering, Sungshin Women's University

SEMINARS & TEACHING ASSISTANT

2023 Seminars on Security and Privacy in Deep Learning
Department of Convergence Security Engineering, Sungshin Women's University

2023 Seminars on Security and Privacy in Deep Learning
College of AI Convergence, Chonnam National University

2022 Seminars on Theory of Information Security
ELTEC College of Engineering, Cyber Security, Ewha Womans University

2019 Teaching Assistant in Cyber Security and Blockchain
Department of Engineering, Seoul National University

PROGRAMMING & LANGUAGE SKILLS

- Python, Pytorch, C, MATLAB
- English, Korean