Yooshin Kim

yooshin0303@dgist.ac.kr | Website | GitHub | Google Scholar | ORCID

Research Interests

Industrial Cybersecurity (Industrial Control Systems, Critical Infrastructure)

Anomaly Detection (Time-Series Modeling, Anomaly Diagnosis, Contextual Digital Twins)

Trustworthy AI (Explainability, Robustness, Privacy-Preserving Machine Learning)

Education

Daegu Gyeongbuk Institute of Science and Technology (DGIST) — Feb 2023 - present
Integrated M.S.-Ph.D. Program, Electrical Engineering and Computer Science — *Daegu, South Korea*

- Advisor: Prof. Donghoon Shin

DGIST — Feb 2018 - Feb 2023
B.S., School of Undergraduate Studies — *Daegu, South Korea*

University of California, Berkeley — Jun 2022 - Aug 2022
Exchange Student — *Berkeley, CA, USA*

Publications

⋆ Equal contribution. † Corresponding author. 4 additional manuscripts are under review.

Kim, Y., Shin, D.†. (2026). Drift-Aware Memory-Augmented Spatio-Temporal Graph Attention for Industrial Anomaly Detection. *ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)*

Heo, W.*, Youn, S.*, **Kim, Y.**, Chae, C., Shin, D.†. (2026). Tracing the Origins: Legacy Codec Identification in Neural Audio Transcoding. *Annual Conference of the International Speech Communication Association (INTERSPEECH)*

Kim, Y., Kwon, N., Shin, D.†. (2026). KDPrint: Passive Authentication using Keystroke Dynamics-to-Image Encoding via Standardization. *Computers & Security, 160, 104725*

Kim, Y.*, Heo, W.*, Woo, E., Shin, D.†. (2025). LCDTwin: Contextual Digital Twin for Actuator-Sensor Correlation in ICS. *5th International Conference on Robotics, Automation and Artificial Intelligence (RAAI)*

Jeong, D.*, **Kim, Y.***, Shin, D.†. (2025). Privacy-Preserving Anomaly Detection with Homomorphic Encryption for Industrial Control Systems in Critical Infrastructure. *IEEE Embedded Systems Letters, 17(4), 276-279*

Research Experience

Digital Twin-Based Fault Diagnosis and Prognosis for Power Plants — Apr 2025 - Dec 2026
Ministry of Science and ICT (MSIT) — *Daegu, South Korea*

- Led development of a drift-aware anomaly detector with dynamic spatio-temporal weighting.
- Built a contextual digital twin using sensor-actuator correlations for anomaly diagnosis.
- Designed a metric to evaluate the utility of time-series anomaly scores.

Cloud-Based Cybersecurity Training Environment for Critical Infrastructure — Mar 2023 - Oct 2024
National Security Research Institute (NSR) — *Daegu, South Korea*

- Led PLC and HMI virtualization using OpenPLC and AdvancedHMI.
- Developed a CODESYS-to-OpenPLC porting tool.
- Designed scenarios and deployed a cloud-based cyber training environment.

ICS Network Visualization System — Mar 2023 - Feb 2024
National Security Research Institute (NSR) — *Daegu, South Korea*

- Led the design and implementation of a Go-based framework for visualizing ICS networks.

Honors and Awards

Best Presentation Award, RAAI 2025 — *Dec 2025*

Best Paper Award, Korea Computer Congress — *Jul 2025*

Dean's List, DGIST — *Spring/Fall 2021, Fall 2022*