2025 2학기 컴퓨터소프트웨어학부

CSE융합세미나

장소 ITBT관 911호

날짜 / 시간 2025.11.12 16:00~18:00

Upcoming Talk

박진성

Research Fellow / KIAS

딥러닝의 데이터 프라이버시 연구
(Data privacy in deep learning)

Deep learning models are known to pose a risk of privacy leakage from training data samples. To safeguard against potential data exposure, various methods, such as anonymization and encryption, have been proposed. Among them, differential privacy (DP) offers a mathematical guarantee against adversaries with practical implementations in training neural networks through gradient modifications. Recently, unlearning techniques have been investigated to delete personal information to fulfill the legal principle "right to be forgotten" in the European Union. In this talk, we will review recent advancements in privacy-preserving deep learning models, particularly focusing on the recent evolution of generative models. We will end with a discussion on promising future directions in the field.

한양대학교 HANYANG UNIVERSITY