COURSE DETAIL

DATA PRIVACY

Country
Korea, South

Host Institution
Yonsei University

Program(s)
Yonsei University

UCEAP Course Level
Upper Division

UCEAP Subject Area(s)
Computer Science

UCEAP Course Number
130

UCEAP Course Suffix

UCEAP Official Title
DATA PRIVACY

UCEAP Transcript Title
DATA PRIVACY

UCEAP Quarter Units
4.50

UCEAP Semester Units
3.00

Course Description

This course explores advanced mathematical problems and theoretical approaches in deep learning with a strong emphasis on privacy-related challenges. Key topics include: Differential privacy, with a focus on its application in federated learning and mechanisms to ensure robust privacy guarantees in distributed settings; Privacy in generative diffusion models, including the use of stochastic differential equations and innovative techniques to safeguard private data in generative processes; Privacy considerations in large language models (LLMs), examining methods for mitigating data leakage, adversarial attacks, and ensuring compliance with differential privacy principles in training and inference.

Language(s) of Instruction
English

Host Institution Course Number
CAS4108

Host Institution Course Title
DATA PRIVACY

Host Institution Campus

Host Institution Faculty

Host Institution Degree

Host Institution Department

Print