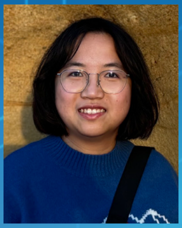
THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

50th Anniversary
Department of Computing
電子計算學系

RESEARCH SEMINAR

Privacy Vulnerabilities and Privacy-Preserving Algorithms in Federated Learning



Dr Ruihan WU
Postdoctoral Researcher
University of California
USA

Date : 26 Jun 2024 (Wed)
Time : 3:00 pm - 4:00 pm
Venue : PQ306

Abstract

Federated Learning (FL) is a popular framework for joint model training when the full dataset is distributed at multiple data owners and, due to privacy concerns, the data cannot be shared with other owners. According to how the data is distributed, there are two categories of FL: horizontal FL and vertical FL. In the horizontal FL, different owners have disjoint sets of data subjects. In the vertical FL, different stakeholders own disjoint sets of attributes belonging to the same group of data subjects. In this talk, I will first show the privacy vulnerability in a classic horizontal FL algorithm, even if some promising empirical defenses are provided. Then, I will introduce privacy-preserving algorithms for data release in the vertical FL setting. With the data released by our algorithm, one can study linear regression without the ability to infer private attributes of individuals.

About the Speaker

Dr Ruihan Wu is a postdoctoral researcher at the University of California. Her research interests mainly lie in machine learning, with a recent focus on privacy-preserving machine learning, machine learning safety, and practical applications of online and bandit algorithms. She received her Ph.D. from Cornell University in 2023 and her B.E. from Tsinghua University in 2018. She received the LinkedIn PhD Fellowship in 2022.

WE DRIVE INNOVATION THROUGH
SMART COMPUTING

Background Image: Technology Vectors by Vecteezy