DISTINGUISHED LECTURE SERIES 2022/23

TOWARDS PRODUCTION FEDERATED LEARNING SYSTEMS

5 JUN 2023 (MON)
10:00 – 11:00AM (HKT)

Cheung Ching Lan Diana Memorial Lecture Theatre
WLB204, Shaw Campus, HKBU /

Online via Zoom

PROF. BAOCHUN LI

Professor
Department of Electrical and Computer Engineering
University of Toronto

Abstract:

While there were thousands of papers in the literature in the recent years on federated learning, very few are concerned with its production use in practice. As the (perhaps only) practical paradigm that preserves data privacy when training a shared machine learning model, I expect that federated learning will be widely used in production. But are research results in the literature valid and practical in production federated learning systems? In this talk, I will share our recent experiences with claims in the existing literature along the lines of privacy leakage attacks, and show that their assumptions do not necessarily hold in production systems. I will also introduce more efficient ways to solve the "unlearning" problem, which is necessary due to regulatory constraints in production, such as the GDPR. Our experiments were conducted on Plato, a new open-source federated learning framework that I designed from scratch in the past two years to be as close to production systems as possible, while using a minimum amount of computing resources.

Enquiries: +852 3411 2385 / comp@comp.hkbu.edu.hk

香港浸會大學
HONG KONG BAPTIST UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE
計算機科學系

35 YEARS OF EXCELLENCE

Speaker's Biography

Event Registration