School of Data Science
香港城市大學
City University of Hong Kong

Hong Kong Institute for Data Science
香港城市大學
City University of Hong Kong

ONLINE SEMINAR

Scalable, Heterogeneity-Aware and Privacy-Enhancing Federated Learning

Date: 24 November 2021 (Wednesday)

Time: 10:00am - 11:00am

Seminar link: https://cityu.zoom.us/j/99550325231

ABSTRACT

Federated learning has become a popular distributed machine learning paradigm for developing on-device AI applications. However, the data residing across devices is intrinsically statistically heterogeneous (i.e., following non-IID data distribution) and mobile devices usually have limited communication bandwidth to transfer local updates. Such statistical heterogeneity and communication limitation are two major bottlenecks that hinder the application of federated learning. In addition, recent works have demonstrated that sharing model updates makes federated learning vulnerable to inference attacks. In this talk, we will present our recent works on the federated learning frameworks to address the scalability and heterogeneity issues simultaneously. In addition, we will also reveal the essential reason of privacy leakage in federated learning and provide a privacy-enhancing defense mechanism accordingly.

Prof Yiran CHEN

GUEST SPEAKER'S PROFILE

Prof Yiran Chen received B.S (1998) and M.S. (2001) from Tsinghua University and Ph.D. (2005) from Purdue University. After five years in industry, he joined University of Pittsburgh in 2010 as Assistant Professor and then was promoted to Associate Professor with tenure in 2014, holding Bicentennial Alumni Faculty Fellow. He is now the Professor of the Department of Electrical and Computer Engineering at Duke University and serving as the director of the NSF AI Institute for Edge Computing Leveraging the Next-generation Networks (Athena) and the NSF Industry–University Cooperative Research Center (IUCRC) for Alternative Sustainable and Intelligent Computing (ASIC), and the co-director of Duke Center for Computational Evolutionary Intelligence (CEI). His group focuses on the research of new memory and storage systems, machine learning and neuromorphic computing, and mobile computing systems. Prof Chen has published 1 book and about 500 technical publications and has been granted 96 US patents. He has served as the associate editor of a dozen international academic transactions/ journals and served on the technical and organization committees of more than 60 international conferences. He is now serving as the Editor-in-Chief of the IEEE Circuits and Systems Magazine. He received seven best paper awards, one best poster award, and fifteen best paper nominations from international conferences and workshops. He received many professional awards and is the distinguished lecturer of IEEE CEDA (2018-2021). He is a Fellow of the ACM and IEEE and now serves as the chair of ACM SIGDA.

Enquiries: hkids@cityu.edu.hk

All are welcome