Department of Electrical Engineering
香港城市大學
City University of Hong Kong

香 港 大 學
THE UNIVERSITY OF HONG KONG

CityU Architecture Lab for Arithmetic and Security (CALAS) Seminar Series

Towards Robust and Heterogeneous Federated Learning

Prof. Edith C.H. Ngai, Associate Professor
Department of Electrical and Electronic Engineering, HKU

Abstract:

Edge Computing is the concept of capturing, storing, processing, and analyzing data closer to the location. Edge Intelligence is a combination of AI and edge computing, which enables the deployment of machine learning algorithms to the edge device where the data is generated. In this talk, I will give a brief introduction on federated learning and its benefits, major challenges, applications. Then, I will focus on system heterogeneity and robustness in federated learning. System heterogeneity aims to support edge devices with heterogeneous computation capabilities to collaborate in federated learning. It facilitates heterogeneous devices to perform federated learning with different local model architectures. After that, I will present our work on robust federated learning, which can improve the resilience of federated learning against data poisoning, model poisoning, and other kinds of security attacks.

Biography:

Edith C.H. Ngai is currently an Associate Professor in the Department of Electrical and Electronic Engineering, The University of Hong Kong. Before joining HKU in 2020, she was an Associate Professor in the Department of Information Technology, Uppsala University, Sweden. Her research interests include Internet-of-Things, edge intelligence, smart cities, and smart health. She was a VINNMER Fellow (2009) awarded by Swedish Governmental Research Funding Agency VINNOVA. Her co-authored papers received a Best Paper Award in QShine 2023 and Best Paper Runner-Up Awards in ACM/IEEE IPSN 2013 and IEEE IWQoS 2010. She was an Area Editor of IEEE Internet of Things Journal from 2020 to 2022. She is currently an Associate Editor in IEEE Transactions of Mobile Computing, IEEE Network Magazine, IEEE Transactions of Industrial Informatics, Ad Hoc Networks, and Computer Networks. She served as a program chair in ACM womENcourage 2015 and a TPC co-chair in IEEE SmartCity 2015, IEEE ISSNIP 2015, IEEE GreenCom 2022, and IEEE/ACM IWQoS 2024. She was a project leader of the “Green IoT” in Sweden, which was named on IVA's 100-list by the Royal Swedish Academy of Engineering Sciences in 2020. She received a Meta Policy Research Award in Asia Pacific in 2022. She was selected as one of the N²Women Stars in Computer Networking and Communications in 2022. She is a Distinguished Lecturer in IEEE Communication Society in 2023-2024.

4 October 2024 (Fri); 10:00am - 12:00nn HKT; G6302; https://cityu.zoom.us/j/96742093029