THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

Research Centre on Data Science & Artificial Intelligence
人工智能與數據科學研究中心

IEEE Computational Intelligence Society

Distinguished Seminar Series on Data Science & Artificial Intelligence

Is Federated Learning Ready for Real-World Deployment?

Prof. Baochun LI

Professor
Department of Electrical and Computer Engineering
University of Toronto
Canada

6 July 2023 (Thu)

16:00 - 17:00 (HKT, UTC+8)

Online via Zoom / HJ305

English

Please register at https://polyu.hk/sbTrh or scan the QR code

All are welcome!

Abstract

While there were thousands of papers in the literature in recent years on federated learning, very few are concerned with whether it is ready for production deployment in practice. As the (perhaps) only practical paradigm that preserves data privacy when training a shared machine learning model, Prof. LI personally expects that federated learning should be widely adopted and deployed in the real world. But are we moving towards real-world deployment, or is it just wishful thinking? Is federated learning just an academic pursuit, or does it have real-world production value?

In this talk, Prof. Li will share a few of their recent experiences that attempted to answer these questions. He first shows that privacy may be quite well protected in federated learning, and claims in the existing literature along the lines of privacy leakage attacks may not necessarily be valid. He will then introduce more efficient ways to solve the "unlearning" problem, which is necessary due to regulatory constraints in production, such as the GDPR. Next, he will show some hurdles in real-world deployment on consumer computing devices, especially with recent trends of larger models. He will conclude the talk with a brief introduction to Plato, a new open-source federated learning framework that I designed from scratch in the past two years to be as close to real-world systems as possible, while still using a minimum amount of computing resources.

This talk will be jointly presented by Ningxin SU and Fei WANG, Prof. Li's PhD students.

About the Speaker

Prof. Baochun LI received his B.Engr. degree from the Department of Computer Science and Technology, Tsinghua University, China, in 1995 and his M.S. and Ph.D. degrees from the Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, in 1997 and 2000. Since 2000, he has been with the Department of Electrical and Computer Engineering at the University of Toronto, where he is currently a Professor. He holds the Bell Canada Endowed Chair in Computer Engineering since August 2005. His current research interests include cloud computing, security and privacy, distributed machine learning, federated learning, and networking.

Prof. Li has co-authored more than 440 research papers, with a total of over 24000 citations, an H-index of 86 and an i10-index of 314, according to Google Scholar Citations. He was the recipient of the IEEE Communications Society Leonard G. Abraham Award in the Field of Communications Systems in 2000. In 2009, he was a recipient of the Multimedia Communications Best Paper Award from the IEEE Communications Society, and a recipient of the University of Toronto McLean Award. He is a member of ACM and a Fellow of IEEE.

Co-speakers - Prof. Li's PhD students

Ningxin SU

Ningxin SU is a third-year Ph.D. student in the Department of Electrical and Computer Engineering, University of Toronto, under the supervision of Prof. Baochun Li. She received her M.E. and B.E. degrees from the University of Sheffield and Beijing University of Posts and Telecommunications in 2020 and 2019, respectively. Her research area includes distributed machine learning, federated learning and networking. Her website is located at ningxinsu.github.io.

Fei WANG

Fei WANG is a second-year Ph.D. student at the Edward S. Rogers Sr. Department of Electrical & Computer Engineering, University of Toronto, Canada, under the supervision of Prof. Baochun Li. She received her B.E. degree with honours from Hongyi Honor College, Wuhan University, China. Her research interests lie at the intersections of networking and communication and machine learning, especially deep reinforcement learning and federated learning. Her personal website is located at silviafeiwang.github.io.