Temple University
College of Engineering

Fall Seminar Series
Department of Electrical and Computer Engineering

Wednesday, October 25, 2023
Noon – 1:00 PM EST
Zoom https://temple.zoom.us/j/93071593846

Embracing Trustworthy Machine Learning Towards Edge Intelligence

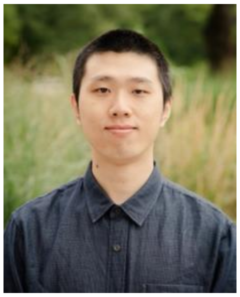
Professor: Xiaoyong (Brian) Yuan

College of Computing, Michigan Technological University

Abstract:

Edge Machine Learning (Edge ML) empowers the deployment of machine learning models on edge platforms, offering tangible benefits such as reduced latency, high availability, and decreased bandwidth consumption. Nevertheless, recent research has uncovered significant security and privacy threats to machine learning models. Concurrently, edge platforms have recently emerged as primary targets for adversaries. When edge computing meets machine learning, edge ML is more likely to introduce new attack vectors, whose impact remains unveiled. In this talk, I will present our recent efforts to identify, analyze, and mitigate critical threats in edge ML. First, I will explore inference-phase privacy threats, with a specific focus on neural network pruning. Pruning has been an essential technique in edge ML, compressing large-scale neural networks to accommodate resource-constrained edge platforms. Our work identified aggravated privacy risks associated with pruning and mitigated these risks through an innovative pruning-oriented defense mechanism. Next, I will present our recent work on training-phase privacy preservation, achieved through the federation of distributed edge platforms. We have developed a lightweight and distributed pruning framework that facilitates the generation of specialized tiny neural networks within the federated learning paradigm. Further, I will briefly introduce our research on safe and robust autonomous driving. Finally, this talk will conclude by discussing potential research directions for advancing trustworthy edge intelligence.

Biography:



Dr. Xiaoyong (Brian) Yuan is an assistant professor at the College of Computing, Michigan Technological University. He received his Ph.D. degree in computer science from the University of Florida in 2020, his master's degree in software engineering from Peking University in 2015, and his BS degree in mathematics from Fudan University in 2012. His research spans the fields of machine learning, security & privacy, and edge & cloud computing. Dr. Yuan has published papers in prestigious journals and conferences, e.g., IEEE TDSC, IEEE TNNLS, AAAI, USENIX Security, and IEEE ICDCS. He is the recipient of the ORAU Ralph E. Powe Junior Faculty Enhancement Award 2022 and the Michigan Tech ICC achievement award 2022. He is currently serving as an associate editor for IEEE Transactions on Neural Networks and Learning Systems (TNNLS).