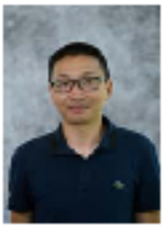
You're Invited to ECE's guest speaker Series

Tuesday, Oct. 3, 2023 | 10:00 AM EST | Held via Zoom

Rutgers Efficient AI (REFAI) Seminar

A New Paradigm of Efficiency, Security and Privacy by Design for Intelligent Data Processing



Prof. Wujie Wen
North Carolina State University

Abstract: The surge in sensing data and advances in machine learning are propelling intelligence from the cloud to the edge, reshaping Cyber-Physical Systems (CPS) and IoT applications. Yet, current intelligent data services, including cloud-based Machine Learning as a Service (MLaaS), confront significant challenges: ensuring low latency, trustworthy ML inference, and client data confidentiality. In this talk, I'll introduce a novel paradigm for designing efficient, secure, and private ML-enabled data processing. We'll begin with "DeepN-JPEG," an innovative data compression approach dedicated to machine vision, NOT "human vision", that reduces communication latency in edge-cloud collaborative inference. Then, I'll unveil "CryptoGCN," the first attempt to accelerate Homomorphic Encryption-based private graph convolutional neural network (GCN) inference. This approach substantially reduces memory and computation requirements for HE operations through optimizations in ciphertext encoding, sparse matrix operations, and model architecture. Lastly, I'll discuss "Neuropots," a pioneering cross-layer real-time proactive defense framework centered around the concept of "Honeypots." This framework offers highly cost-effective protection for ML inference on hardware, safeguarding against fault injection attacks. Our aim is that this talk will provide an alternative perspective on designing for efficiency, security, and privacy, tailored for smart systems.

Speaker Bio: Prof. Wujie Wen is an Associate Professor in Department of Computer Science at North Carolina State University. He earned Ph.D. degree from University of Pittsburgh. His current research efforts include efficient, reliable, secure, and privacy-preserving computing, particularly from the aspects of software-hardware co-design and electronic design automation, as well as their applications to embedded, IoTs, smart medical and intelligent cyber-physical systems. His research group has published extensively on CSRankings conference venues, including DAC, ICCAD, MICRO, HPCA, Oakland, USENIX Security, NeurIPS, ICML, CVPR, ICCV, ECCV, AAAI, etc. Dr. Wen received best paper nominations from all four major EDA conferences. He serves as an Associate Editor of Neurocomputing and IEEE Circuit and Systems Magazine. He is a recipient of the NSF Faculty Early Career Award.