Keynote Talk 3: Security and Privacy Challenges in Learning-enabled IoT Systems

Mani Srivastava, *Fellow, ACM; Fellow, IEEE*
Professor
University of California, LA

Abstract:
Innovative edge devices, pervasive wireless connectivity, and powerful cloud computing are leading to a new generation of learning-enabled IoT systems. Unlike their precursors that primarily focused on collecting sensor data for off-line knowledge discovery and simple control, this new generation of IoT systems harness machine learning (ML) to make rich inferences about the state of natural, engineered, and human systems; to comprehend and project it to the future; and to decide on actions that influence and nudge that state in a desired and timely manner. While data-driven ML algorithms are helping equip these emerging IoT systems with intelligence and autonomy, they also introduce vulnerabilities to a variety of security and privacy problems. This talk will cover research in my group on (i) efficient black-box attacks on sensor data and machine learning models that cause these systems to make incorrect inferences and control actions, (ii) defense mechanisms that help detect and mitigate these attacks, and (iii) protecting against privacy loss arising from inference attacks on high-dimensional sensory data being shared by differentially-private synthetic sensor data generation.

Short Biography:
Mani Srivastava is on the faculty at UCLA where he is associated with the ECE Department with a joint appointment in the CS Department. His research is broadly in the area of networked human-cyber-physical systems, and spans problems across the entire spectrum of applications, architectures, algorithms, and technologies. His current interests include issues of energy efficiency, privacy and security, data quality, and variability in the context of systems and applications for mHealth and sustainable buildings. He is a Fellow of both the ACM and the IEEE. More information about his research is available at his lab's website: http://www.nesl.ucla.edu and his Google Scholar profile at https://scholar.google.com/citations?user=X2Qs7XYAAAAJ.