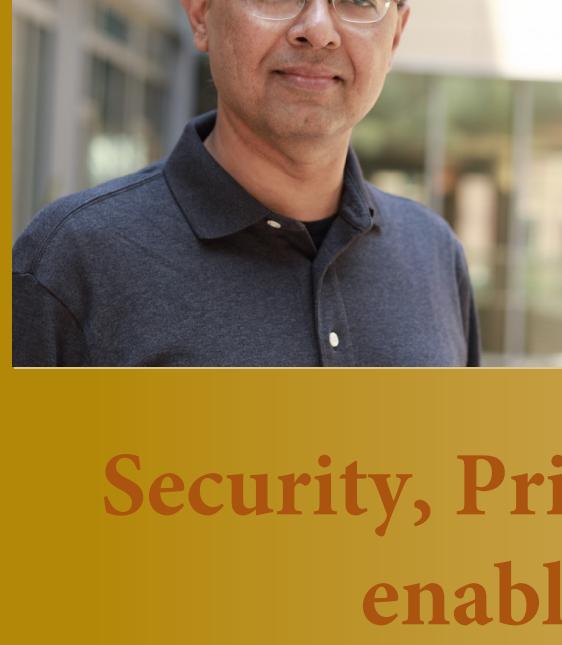# Distinguished Lectures
Fall 2022

Dr. Mani Srivastava

**Distinguished Professor, Electrical & Computer Engineering
with a joint appointment in Computer Science
University of California, Los Angeles
Amazon Scholar, Amazon**

Security, Privacy, and Trust Challenges in AI-enabled Cyber-Physical Systems

**Monday, October 24, 2022
Reception with refreshments: 10:30 a.m.
Lecture: 11:00 a.m.-12:00 noon
Lory Student Center Ballroom-350A**

Neuro-symbolic Architectures for Complex Event Processing in the Internet of Things

**Monday, October 24, 2022
Lecture: 2:00-3:00 p.m.
Lory Student Center 300**

**Sponsored by
Colorado State University's Information Science
and Technology Center (ISTeC)**

In conjunction with the Department of Computer Science and
Department of Electrical and Computer Engineering Seminar Series

Abstracts

Security, Privacy, and Trust Challenges in AI-enabled Cyber-Physical Systems

The emerging nexus of Artificial Intelligence (AI) and Cyber-Physical Systems (CPS) is critical to interfacing our digitized society with the analog world it is embedded via sophisticated perception-cognition-communication-action loops. Essential to this vision is the ability to computationally extract rich inferences about the complex events and activities taking place around us; devise actions and interventions that beneficially affect the physical world and nudge human behaviors; and, to do so in a manner that is performant, efficient, and trusted by various stakeholders. Drawing upon experience with the applications of AI-enabled CPS in mobile health, smart environments, and other use domains, the talk will discuss the unique challenges relating to trust, privacy, and security that arise in these systems; describe emerging approaches that address the challenges; and, highlight the importance of considering the socio-technical contexts of these systems.

Neuro-symbolic Architectures for Complex Event Processing in the Internet of Things

The combination of deep neural networks (DNNs) with the Internet of Things (IoT) allows sensing and actuation to be performed in our personal, social, and physical spaces in previously unimagined ways. Deep learning methods deployed across the edge-cloud continuum enable IoT systems to make accurate predictions and decisions from high-dimensional and unstructured real-world sensory data while benefiting from the high-performance tensor operations in hardware accelerators. As a result, in many settings, DNNs have entirely replaced symbolic and mechanistic approaches based on algorithms, scientific models, and human knowledge. However, the benefits come with considerably reduced abilities to generalize to new situations, to assure trustworthiness, and to reason about complex spatiotemporal events that require connecting the dots across large spans of time and space. We will present emerging neuro-symbolic approaches that seek to overcome this tension by integrating neural representations with symbolic reasoning. The former allows efficient processing of multimodal sensory inputs to create precepts that assist reasoning and the latter provides interpretability, enforces constraints, allows for human knowledge injection, and acts as regularizers that guide the learning of neural components. The talk will describe the unique capabilities that neuro-symbolic architectures bring to the IoT domain, the research challenges they present, and initial work on neuro-symbolic architectures in practice.

Speaker Biography

Mani Srivastava <mbs@ucla.edu> is on the faculty at UCLA where he is a Distinguished Professor in the ECE Department with a joint appointment in the CS Department, and is affiliated with Amazon as an Amazon Scholar. His research is broadly in the area of multimodal sensor information processing, and Human-Cyber-Physical and IoT systems that are learning-enabled, energy-efficient, and secure & trustworthy. His work spans problems across the entire spectrum of architectures, algorithms, and technologies while focusing on applications in mobile health, smart built environments, and military. He is a Fellow of 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 (https://scholar.google.com/citations?user=X2Qs7XYAAAAJ).

To arrange a meeting with the speaker, please contact Prof. Anura Jayasumana: anura.jayasumana@colostate.edu.