Title: Towards Secure, Interpretable, and Scalable Machine Learning Applications in Cyber-Physical Systems

Speaker: Dr Shailja Thakur

Date: 16 Feb, 2024

Time: 2:30 - 3:30 PM

Venue: RM 101, Dept of CSE.

Abstract:

In a world increasingly reliant on Cyber-Physical Systems (CPS), there are critical challenges associated with the integration of complex software and hardware. The enormous and diverse nature of data, alongside pressing security and privacy concerns, demands innovative solutions. My work aims to enhance the intelligence of CPS through AI, aiming for systems that are not only self-aware but also capable of adapting in real-time to changing environments. To that end, my work has spanned the automotive, energy, and hardware sectors, delivering practical solutions engineered alongside industry partners. I have made significant strides in enhancing security in automotive systems and have pioneered tools for deciphering the decision-making processes of machine learning models. In the realm of hardware design, I am exploring the potentials of Large Language Models (LLMs) to automate and optimize the process, reducing human error and increasing efficiency. In the future, I want to expand upon the challenges and scope of applying generative AI in CPS for developing time-efficient, scalable, safe and transparent real-world applications.

Bio:

Shailja Thakur is a postdoctoral fellow currently at New York University in the Tandon School of Engineering within the Department of Electrical and Computer Engineering and the Center of CyberSecurity with Professors Ramesh Karri and Professor Siddharth Garg. Her research interests span the field of cybersecurity, with a particular focus on the application of language modelling in embedded systems, LLM attributions, safety, and privacy. Shailja received her Ph.D from the University of Waterloo and a masters in Computer Science and Engineering from IIIT Delhi.