Department of Computer Science
Colloquium Lecture

"Practices and Hazards in Reusing Pre-Trained Neural Networks: A Software Engineering Perspective

James Davis

Purdue University

February 12 • 4:30-5:30 pm

Rekhi 214 and Zoom

Talk Abstract: Deep neural networks are widely used in computing systems, from image recognition in autonomous vehicles to detecting anomalies in system logs. Creating and specializing neural networks is growing more difficult as state-of-the-art architectures grow more complex. Following the path of traditional software engineering, machine learning engineers have begun to exchange and reuse pre-trained neural networks (PTNNs). Understanding this software engineering process is the first step to optimizing and securing it, e.g. through model search engines for reuse, improved testing techniques for validation, and better definitions for PTNN packaging. However, the details of real-world PTNN reuse remain unknown. In this talk I present results from our empirical software engineering work to define the PTNN supply chain and evaluate aspects of trust in this context. I will discuss three projects: (1) Characterizations of the kinds of PTNN registries; (2) Interviews with software engineers describing their processes and challenges; and (3) Measurements of hazards along the PTNN research-to-practice pipeline.

Read more and find the Zoom link.

Computing [MTU]
Department of Computer Science

1885
Michigan Tech