UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

MSc Seminar

Wednesday August 16, 2023 at 2pm via Zoom [Remote]

Keerthana Madhavan

A Holistic Framework for Assessing Cybersecurity Risks in AI Systems

Advisor: Dr. Ali Dehghantanha
Co-Advisory: Dr. Fattane Zarrinkalam [SoE]
Advisory: Walter Cooke [CISM, CISSP, Co-operators Insurance]
Advisory: Dr. Eman Hammad [Texas A&M University]

Abstract:

Artificial Intelligence (AI) systems are crucial in various sectors, enhancing innovation and efficiency, but their rapid expansion has raised significant security and privacy concerns. This research proposal aims to address these challenges by conducting a systematic line-by-line audit of AI compliance standards and investigating the complementary security measures organizations employ to enhance their security. The research focuses on three widely adopted AI compliance standards: the National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework Playbook 1.0, the AI and Data Protection Risk Toolkit developed by the Information Commissioner's Office (ICO), and the Assessment List for Trustworthy AI (ALTAI) published by the European Commission. By identifying potential security risks within these standards and evaluating organizations' supplementary security measures, the research aims to develop a tailored risk assessment framework for AI systems. This holistic framework will offer a practical approach for assessing cybersecurity risks in AI, ensuring more secure and trustworthy applications. The study holds substantial implications for stakeholders, including auditors, security professionals, and policymakers, by offering a viable framework for enhancing AI security across industries.