UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Seminar 2

Tuesday January 24, 2023 at 2pm via Zoom

Abbas Yazdinejad

Secure and Private ML-based Framework for Industrial Internet of Thing (IIoT)

Advisor: Dr. Ali Dehghantanha
Co-Advisor: Dr. Hadis Karimipour [SoE]
Advisory: Dr. Guatam Srivastava [Brandon University]
Advisory: Dr. Reza Parizi [Kennesaw State University]

Abstract:

The Industrial Internet of Things (IIoT) involves the integration of internet-connected devices in industrial settings, leading to increased efficiency and automation. However, these connected devices also introduce new security and privacy threats, such as hacking, data breaches, and unauthorized access to sensitive information. It is crucial to implement security and privacy tools to protect IIoT systems and the sensitive data they handle. Additionally, it includes integration with new technologies like blockchain technology that provide more security challenges of decentralized IIoT networks and ensures secure and transparent data management. In this work, we proposed a secure and private-enabled ML-based cybersecurity framework for the IIoT.

The proposed framework includes three major contributions: 1) an auditable privacy-preserving federated learning (FL) mechanism for IIoT, 2) a threat-hunting approach for detecting anomalies and identifying potential cyber threats in IIoT networks, and 3) an extension of the threat-hunting approach to incorporate the specific challenges and security considerations of blockchain-based IIoT. The proposed framework aims to address the growing concerns of data privacy in the IIoT while applying federated setup and provide an effective means of protecting these systems from cyber attacks via the benefits of federated learning. Our results prove the efficiency of the proposed framework in performance metrics such as accuracy, precision, F1-score, and Recall.