UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Qualifying Exam

Wednesday October 19, 2022 at 1pm via Zoom

Abbas Yazdinejad

An Efficient and Auditable Privacy-Preserving Framework for Federated and Distributed Environments

Chair: Dr. Joe Sawada
Advisor: Dr. Ali Dehghantanha
Co-Advisor: Dr. Hadis Karimipour [SoE]
Non-Advisory 1: Dr. Hassan Khan
Non-Advisory 2: Dr. Fattane Zarrinkalam [SoE]

Abstract:

Machine learning (ML) models, at the core of Artificial intelligence (AI), are widely applied in our digital world. To build these models, huge amounts of data must be collected, and many assets must be protected under privacy law. Data privacy is a critical issue when training and testing ML models. For privacy concerns to be adequately addressed in today's ML systems, there needs to be considered privacy gaps in ML, as trained ML models can be vulnerable to adversarial attacks. In this regard, federated learning and distributed environments (based on blockchains) are the new paradigms that have emerged with the promise of privacy-preserving by design while utilizing ML models. The new paradigms have promising privacy-preserving potential; however, they neglect several fundamental privacy and security issues the fact that adversaries can exploit shared gradients and global parameters, the parameter server may drop gradients that have been mistakenly or deliberately updated, and also enough data is available to train models. The proposed research addresses privacy concerns in federated and distributed environments.

This proposal aims to establish a privacy-preserving framework that can be audited in federated and blockchain-based environments. Additionally, we would like to generalize our approaches to threat detection in these environments. In this stage, the proposal contains a review of appropriate background literature, a description of the proposed auditable privacy-preserving framework and its merits, as well as a schedule of the research plan.