UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Seminar 1

Friday Dec 20, 2019 at 10 AM in Reynolds, Room 2224

A Federated AI-Based Framework to Automate Privacy Preservation in IoT

Mohammad Amiri-Zirandi

Advisor: Dr. Rozita Dara

Co-Advisor: Dr. Evan Fraser [Geography]

Advisory Committee: Dr. Xiaodong Lin

Advisory Committee: Dr. Hassan Khan

ABSTRACT:

Internet of things (IoT) is a technology that aims to connect everything from everywhere. This concept has affected our daily lives and has become an inseparable part of our everyday activities. Since IoT devices collect valuable and sensitive data in different applications, the services in this ecosystem must guarantee privacy preservation. Some of the concerns in IoT data privacy including but not limited to interoperability, regulations, processes and protocols, and the technical requirements. Recently, the use of Artificial Intelligence (AI) to help IoT data protection has gained a lot of attention. The large amount of data is accessible in IoT ecosystem provides an opportunity for AI to leverage this information and guide data protection operations automatically and improve their performance. These operations include authentication, access control, data aggregation, and regulatory compliance. AI can also limit contextual raw data sharing among different components of IoT to keep data more private and protected.

In this research, we aim to develop an AI-based framework to automate privacy protection operations in a distributed manner. The proposed framework leverages a software-defined approach to abstract privacy control from hardware and facilitates automated procedures for privacy protection. The AI engines that are distributed and work on the control layer, will gather data from IoT and assess privacy vulnerabilities of IoT devices and applications using privacy evaluation operations such as trust assessment, access control, and policy compliance.

As a preliminary step, we have developed a framework for trust management. A blockchain-based decentralized trust management system have been developed in the infrastructure and control layers of the proposed framework to asses the trust factors of IoT nodes. This system uses direct experience from previous transactions in addition to indirect feedback from other nodes in the network. Furthermore, to increase the security of the system against bad-mouthing and ballot stiffing attacks, the system uses entropy to weighting the effect of each node in indirect trust evaluation process. Our next step will be adding machine learning to the control layer of proposed network.