UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Defence

Wednesday October 12, 2022 at 9am via Zoom

A Privacy-Preserving Trust Management Framework for IoT

Mohammad Amiri-Zarandi

Chair: Dr. Joe Sawada
Advisor: Dr. Rozita Dara
Advisory: Dr. Xiaodong Lin
Non-Advisory: Dr. Lei Lei [School of Engineering]
External Examiner: Dr. Ralph Deters [University of Saskatchewan]

ABSTRACT:

In the Internet of Things (IoT), numerous devices are connected to perform tasks and services in different applications. Although providing a seamless and remote connection among devices is an excellent feature for IoT, it also raises some concerns regarding security and privacy. The IoT devices are numerous and have complex interactions. Being ubiquitous, these systems are also vulnerable to sensitive data leakage in different stages of the data lifecycle. Trust management systems are mechanisms to automatically evaluate the access requests in the system and handle the permissions based on the trust between IoT nodes. Trust management helps IoT devices to overcome perceptions of uncertainty and risk and prevent adversaries from accessing the services and applications in the network. Trust management and privacy preservation mechanisms work together to reduce the risks related to data leakage and unapproved access in a system from two different perspectives. On the one hand, a trust management system can monitor communications and limit high-risk data access by different entities and, in turn, advance privacy protection. On the other hand, because trust management systems use sensitive data to operate, they need to be developed in a privacy-preserving manner.

In this study, working on both aspects, we aim to provide an enhanced trust management system that leverages AI and different available data sources in the trust evaluation mechanism. Moreover, the proposed system will be designed in a privacy-preserving manner that protects the sensitive data that is used in the developing phase of the system production. The novelty of the present research lies in utilizing data from diverse sources in a decentralized AI-based framework to extract knowledge and enhance the trust management process. The framework includes three different components for Social IoT data analysis, network data analysis, and user behavior data analysis. Moreover, the proposed framework provides privacy-preserving mechanisms for data analysis in all these components. Finally, the presented framework aggregates the outputs of different data analysis components to be utilized for trust management and access control in IoT. The obtained results show that the presented framework outperforms similar solutions in terms of accuracy and privacy.