The University of Queensland - IIT Delhi Academy of Research Joint PhD Project

Project title	**Context-aware Security for the Internet of Things**
Project code	**UQIDAR 00197**
Project description	A modern paradigm in the design of IoT systems is the use of reusable components. For example, if a person has a sensor in her coffee cup to measure the temperature of coffee, she can seamlessly take the sensor out and use it to measure her own body temperature. A noteworthy point here is that in the latter scenario requirements for security and privacy are comparatively much more, and thus there is a need to make devices context aware such that they can tailor their privacy and security requirements accordingly. Given that ensuring security and privacy comes at a cost --energy and time -- we would like to have a secure layer that is aware of the context and is aware of the user's requirements and can then tailor his behavior accordingly. This would require a complex mix of IoT middleware, algorithms and techniques to sense the context, some degree of machine learning, and exhaustive experimentation to measure the different trade-offs that are involved. Such context-aware IoT networks can be designed, implemented and deployed in various environments. A set of security and privacy requirements will be set in terms of CIA triads and other attributes. The system's configuration and security information for a deployed IoT network will be collected and processed. The processed network and security information will be used to assess the security risk of the IoT network via a formal graphical security model, and well-known security/privacy metrics. The graphical security models and metrics will be used to check whether the security and privacy requirements for the IoT network are met. If the requirements are satisfactorily met, the IoT network will not change its security configurations, whereas if it is not the case, the security level will be adjusted to meet the security and privacy requirements.
Project outcomes	1. An algorithm to specify and detect the context of an IoT device. 2. A formal model to specify security properties in a given context. 3. Methods to adjust security and privacy settings online.
Advisory team	**UQ Principal Supervisor** **Associate Professor Dan Kim** Information Technology and Electrical Engineering dan.kim@uq.edu.au https://researchers.uq.edu.au/researcher/23703 **IITD PrincipalSupervisor** **Associate Professor Smruti Sarangi** Computer Science & Engineering srsarangi@cse.iitd.ac.in http://www.cse.iitd.ac.in/~srsarangi/
Type of student	Applications are open to: I or q students who meet eligibility criteria.
Discipline background of student	Ideally, this project requires students with a background in: Bachelors or Masters in Electronics or Computer Engineering
Ideal candidate	**Essential Capabilities:** Bachelors or Masters in Electronic or Computing Engineering

Application process	Apply online by the due date: https://www.uqidar.org/students/how-to-apply/