THE 20TH IEEE INTERNATIONAL CONFERENCE ON INDUSTRIAL TECHNOLOGY IEEE-ICIT 2019

13 - 15 FEBRUARY 2019, MELBOURNE CONVENTION AND EXHIBITION CENTRE, MELBOURNE, AUSTRALIA

Special Session on

"Security Hardening of Industrial IoT Systems"

Organized by

Chairman: Dr. Alireza Jolfaei, Federation University Australia, Victoria, Australia
a.jolfaei@federation.edu.au

Co-chair: Dr. Muhammad Usman, Quaid-I-Azam University, Islamabad, Pakistan
musman@qau.edu.pk

Co-chair: Dr. Pouya Ostovari, San Jose State University, California, USA
pouya.ostovari@sjsu.edu

Co-chair: Associate Professor Iqbal Gondal, Federation University Australia, Victoria, Australia
iqbal.gondal@federation.edu.au

Call for Papers

Internet of Things evolve continuously both in terms of physical aspects (for example, new devices added, old ones upgraded or retired), and the operational environment (for example, new or different vulnerabilities). As the Internet of Things continues to evolve with new technologies and applications, this incredible synthesis of networked humans and machines will generate constant streams of data that can introduce new surfaces for malicious attacks. This has been justified by recent major data breaches in the financial services, healthcare, and retail sectors. Whether it is a payment-processing device, a medical device, or another industrial device, the need for security hardening is paramount to ensure the integrity of operations and sensitive data. The aim of this special session is to provide a platform for researchers to share and showcase their original works on security hardening of Internet of Things. In addition, it will discuss the current open research challenges in IoT security, to stimulate new research approaches and directions in this field.

Topics of interest include, but are not limited to:

- Novel methods, protocols, and algorithms for IoT infrastructure security;
- Cyber and cyber-physical attacks identification and prevention systems in industrial IoT applications;
- Middleware for privacy, security, and trust in industrial IoT applications;
- Cross-domain security, privacy, and trust issues; and
- Future perspectives of security, privacy, and trust issues in industrial IoT applications.

Accepted papers will be published in an IEEE proceedings volume and will be also submitted for the International Publication in *IEEExplore*