

***** CALL FOR PAPERS *****

SUBMISSION DUE DATE: 30-11-2018

SPECIAL SESSION ON PRIVACY, SECURITY AND MACHINE INTELLIGENCE IN IOT.

INTERNATIONAL CONFERENCE ON INNOVATIVE COMPUTING AND COMMUNICATION ICICC-2019

Guest Editor: Rashmi Arora, Guru Tegh Bahadur Institute of Technology, NewDelhi, India, icicc.spmiot@gmail.com

INTRODUCTION: The Internet of Things (IoT) refers to uniquely addressable objects and their virtual representations in an internet-like structure. The concepts of pervasive computing and ubiquitous computing are related to the internet of things, in the sense that all of these paradigms are enabled by large-scale embedded sensor devices. On the other hand, Machine Intelligence aims to design and develop robust automated decision making systems. Its objective is to minimize the manual interruptions and maximize the accuracy of the machine made 'thoughts' in a system. Since IoT can sense and communicate, they have become tools for understanding complexity, and may often enable autonomic responses to challenging scenarios without human intervention. There are many recent examples of attacks that exploit IoT devices to perform large-scale distributed denial of service attacks, to spy on people, and to hijack communication links, therefore delivering full control of anything that is remotely accessible to an attacker. The special session focuses on both the theoretical & practical aspects of the security, privacy, and trust of IoT networks, devices, applications, and services as well as novel ways of dealing with their vulnerabilities and mitigating sophisticated cyber-attacks. The large number of devices simultaneously producing data in an automated way will greatly dwarf the information which individuals can enter manually. Machine Intelligence provides us the framework and tools to go beyond trivial real-time decision and automation use cases for IoT. This is a quite challenging task as the real time accurate decisions are to be made in various circumstances over similar 'things' may be with some different features. This session aims to introduce the machine intelligence features to solve the challenges in IoT or to enhance its performance and to have interface among academicians and industry people over the problems and feasible solutions.

RECOMMENDED TOPICS:

Topics to be discussed in this special session include (but are not limited to) the following:

- Blockchain applications in IoT
- Cyber-threat intelligence
- Game-theoretic security for IoT

- Identity management and access control for IoT
- Artificial Intelligence for IoT
- Real-world applications based on IoT
- Malware detection and mitigation
- Network intrusion detection/mitigation
- Privacy and data protection in IoT
- State of the art reviews on topics related to IoT
- Internet of Things
- Feature Engineering with a focus on sensor data features
- Generating high-quality features from sensor data
- Application in various areas like e-health, smart city, intelligent transportation system
- Automated video surveillance and tracking

SUBMISSION PROCEDURE:

Researchers and practitioners are invited to submit papers for this special theme session on **[PRIVACY, SECURITY AND MACHINE INTELLIGENCE IN IOT.] *on or before [30TH Nov 2018]***. All submissions must be original and may not be under review by another publication. INTERESTED AUTHORS SHOULD CONSULT THE CONFERENCE'S GUIDELINES FOR MANUSCRIPT SUBMISSIONS at http://icicc-conf.com/paper_submission.html. All submitted papers will be reviewed on a double-blind, peer review basis.

NOTE: While submitting paper in this special session, please specify [**insert special session title: PRIVACY, SECURITY AND MACHINE INTELLIGENCE IN IOT**] at the top (above paper title) of the first page of your paper.

All inquiries should be should be directed to the attention of:

Rashmi Arora

PRIVACY, SECURITY AND MACHINE INTELLIGENCE IN IOT
E_mail: icicc.spmiot@gmail.com

* * * * *