Guest Editorial Preface

Security, Privacy, and Trust in IoT:
Special Issue of International Journal of Wireless Networks and Broadband Technologies

Muralidhar Kurni, Department of CSE, Anantha Lakshmi Institute of Technology & Sciences, Ananthapuramu, Andhra Pradesh, India

Saritha K, Sri Venkateswara Degree College, Ananthapuramu, Andhra Pradesh, India

Recently, in the area of wireless communications and networking, a new paradigm named the Internet of Things (IoT) has appeared. By embedding short-range mobile transceivers into a wide array of additional gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves, IoT adds a new dimension to the world of information and communication and IoT applications are changing the way people work and live by saving time and resources and opening new opportunities for growth, innovation and knowledge creation. Therefore, IoT has attracted considerable attention from both academia and industry.

However, many challenging issues still need to be addressed. One such challenge is security and privacy technologies for IoT. Two major issues in IoT are the privacy of the humans and the confidentiality of the business processes. For ensuring confidentiality, a large number of standard encryption technologies exist for use. However, the main challenge is to make encryption algorithms faster and less energy consuming. Moreover, an efficient key distribution scheme should be in place for using an encryption scheme. For privacy, the situation is more serious; one of the reasons is the ignorance (regarding privacy) of the general public. Moreover, the heterogeneity and mobility of 'things' in the IoT will add complexity to the situation. A similar argument can be made for authentication of devices and establishing trust.

This leads us to develop a special issue seeking a high quality of papers demonstrating real proofs-of-concept and solutions to enforce the importance of security, privacy and trust in IoT.

The four papers in this special issue present the main research challenges and the existing solutions in the field of IoT security, identifying open issues, and suggesting some hints for future research. Each of these papers has undergone full double-blind peer review, before being selected for this special issue.

In the paper "IoT Big Data Security, Privacy and Challenges Related To Smart Grid," security challenges and concerns of IoT big data associated with the smart grid are discussed along with the new security enhancements for identification and authentications of things in IoT big data environments.

The paper "Energy Efficient Clustering using MMHC (Modified Multi-Hop Clustering)," proposed an energy-efficient methodology named as MMHC (Modified Multi-Hop Clustering), for WSNs which not only helps in enhancing the network lifetime but also reduces the energy consumption since nowadays, monitoring agriculture environment has become one of the essential fields and IoT has been one of the eminent technology in recent years and WSN model has played the parallel role into it.

In the paper "Security Issues on IoT environment In Wireless Network Communications," security prerequisites of IoT in wireless network communications such as privacy, honesty, and validation, and so forth are discussed. In this study, twelve distinct kinds of assaults are sorted as low-level assaults, medium-level assaults, abnormal state assaults, and amazingly abnormal state assaults alongside their temperament/conduct just as recommended answers for the experience these assaults are discussed.

In the paper "IoT: A Review on Wireless Communication Protocol and Security Privacy," the use of wireless protocols that bridges the gap with the Security and Privacy Issues in the Internet of Things has been drastically discussed.

As the special issue of the International Journal of Wireless Networks and Broadband Technologies (IJWNBT) we feel proud to bring you this special issue. We hope that reading these high-quality papers will inspire you to make your submissions to future journals and conferences. We hope that this paper will help suggest the research road ahead, to allow a massive deployment of secure IoT systems in the real world.

We express our gratitude to the authors for their excellent contributions to this Special Issue. Great thanks to all reviewers for their efforts in reviewing these papers, and valuable comments that help greatly to improve the quality of the papers. We also appreciate the great efforts and support from the Editor-in-Chief, the Editorial Board, the administrative staff and especially Alexis Miller, Assistant Development Editor and Colleen Moore, Editorial Assistant to the Managing Director, without which this special issue would not have been possible. We hope this Special Issue will serve as a good reference for researchers, scientists, engineers, and academicians in the field of security, privacy, and trust in IoT.

Muralidhar Kurni
Saritha K
Guest Editors
IJWNBT