

Special Issue on
**Design of a Power Efficient, Intelligent, and Secure
System for the Internet of Things (IoT)**

CALL FOR PAPERS

Over the past ten years the term “Internet of Things” (IoT) has become widely recognized, and this technology is growing rapidly from media hype to reality. It is predicted that by 2020 there will be 50 billion things connected to internet. It is also predicted that 200 things per person could be connected to IoT which could potentially lead to several hundred billion devices. In the future, enormous number of sensors will be deployed to collect the data from the surrounding environment. It is often incredibly expensive to replace sensor battery once it is employed in the field; therefore energy efficiency is important to extend the battery life. This creates the demand for the design of energy efficient sensors that requires no battery replacement, as well as the development of communication protocols to save energy.

With the expansion of the IoT system, the demand for saving huge amounts of information in data-bases is increasing. To process these data in real time, one needs fast and energy efficient techniques, and hence big data analysis is one of the most challenging research fields in IoT that needs smart and efficient data bases. This big data comes from connected devices with different levels of processing capabilities in which they store, process, and retrieve the data. In smart devices, the amount of data processing is a tradeoff with the device power consumption, where more processing may lead to higher power consumption compared to the case that it transmits raw data to a central processing unit. However, optimization of the amount of on-the-node data processing is highly dependent on the application specifications. Moreover, not all the data are important or useful. Architecture-wise, it is natural for sensor data to be processed in a hierarchical and distributed fashion. If the system can recognize the importance of data in the beginning, then only relevant data is transferred to the server and considerable power can be saved.

The growth of IoT has drawn the attention to data security and privacy, which are major concerns. The smart, secure, and connected devices at the edge nodes of the IoT are critical for realizing robust and intelligent end-to-end cyber-physical systems. Conventional firewalls that provide network security by blocking malicious traffic can no longer work in the IoT because of its decentralized nature. If the lightweight devices are not properly secured, the data they produce cannot be fully trusted, as attackers may provide false information that alters the behaviors of the system. Designing low-cost and scalable crypto algorithms and hardware accelerators is crucial, and system-level security analytics and a self-adaptive security policy framework are also needed.

This special issue aims to publish high-quality technical papers describing the state of-the-art research on related topics.

Potential topics include but are not limited to the following:

- ▶ Power management in IoT based sensors
- ▶ Memory power management for resource constrained IoT devices
- ▶ Power system reliability and security for IoT
- ▶ IoT based energy/power management system
- ▶ Power efficient networking and communication technologies for IoT
- ▶ Power efficient circuits and systems for IoT
- ▶ Cryptography, security, and privacy
- ▶ IoT data analytics for intelligent power efficient systems
- ▶ System architecture and protocol design of IoT for power efficient systems

Authors can submit their manuscripts through the Manuscript Tracking System at <https://mts.hindawi.com/submit/journals/jece/power.systems/dpiss/>.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor

Ajay Kumar Singh, Multimedia University, Melaka, Malaysia
ajay.singh@mmu.edu.my

Guest Editors

Ahmed Abdelgawad, Central Michigan University, Mount Pleasant, USA
abdella@cmich.edu

Sotirios K. Goudos, Aristotle University of Thessaloniki, Thessaloniki, Greece
sgoudo@physics.auth.gr

Mehedi Masud, Taif University, Taif, Saudi Arabia
mmasud@tu.edu.sa

Rosdiadee Nordin, Universiti Kebangsaan Malaysia, Bangi, Malaysia
adee@ukm.edu.my

Submission Deadline

Friday, 3 May 2019

Publication Date

September 2019