Editorial

P. Karrupusamy*

Department of Electrical and Electronics Engineering,
Surya Engineering College,
Mettukadai, Erode 638107, India
Email: pkarrupusamyphd@gmail.com
*Corresponding author

Joy Iong-Zong Chen

Department of Electrical Engineering,
Da-Yeh University,
No. 168, University Road, Dacun, Changhua, 51591, Taiwan
Email: jchen@mail.dye.edu.tw

Biographical notes: P. Karrupusamy is working as a Professor and Head in the Department of Electrical and Electronics Engineering at the Surya Engineering College, Erode. He completed his Doctorate degree from the Anna University, Chennai, in 2017 and Postgraduate in Power Electronics and Drives from the Government College of Technology, Coimbatore, India, in 2007. He has more than ten years of teaching experience. He has published more than 40 papers in national and international journals and conferences. He has acted as the Conference Chair in IEEE international conferences and guest editor in reputed journals. His research area includes modelling of PV arrays, adaptive neuro-fuzzy model for grid connected photovoltaic system with multilevel inverter.

Joy Iong-Zong Chen is currently a Full Professor from the Department of Electrical Engineering, Dayeh University, Changhua Taiwan. Prior to joining Dayeh University, he worked at the Control Data Company (Taiwan) as a Technical Manager since September 1985 to September 1996. His research interests include wireless communications, spread spectrum technical, OFDM systems, and wireless sensor networks. He has published a large number of SCI journal papers in the issues addressed physical layer for wireless communication systems. Moreover, he also majors in developing some applications of the internet of things (IoT) techniques and owned some patents authorised by the Taiwan Intellectual Property Office (TIPO).

Due to the rapid growth of mobile technologies, smart devices and mobile internet, it has become the most popular scenario and faces challenges like threatening attacks and unsecure communication between the users. The security challenges involved in the internet of things (IoT) are data encryption, data authentication, firewall, data integrity and routing control. That has been resolved by the designing of secure internet architecture with the quality attributes like integrity, confidentiality, accountability and availability. Most trending technologies like block chain, cyber security and cyber resiliency helps to improve the security strength in IoT communication.

This special issue addressed the consequences of IoT adoption with the supporting skills like hardware authentication, user-behaviour analytics, data loss prevention, cloud computing and deep learning. IoT helps to improve performance in the way of sensing, visualisation, accessibility and data analytics. It offers tremendous opportunities for innovative technologies and provides better solutions for cyber-attacks and weighted against the growing risks. Advanced security mechanisms realises the security mesh in IoT, in which maintain the essential trust for future internet.