

Cyber Security and Privacy of IoT-enabled Infrastructures in Smart Grid, Smart vehicle, Smart cloud and Smart home (CSPIoT 2018)

The Internet of Things (IoT) is the inter-networking of various physical devices, objects, and people. The vital role of IoT is to collect and share the electronic information between the source and destination. In recent years, IoT is widely applied in many areas it includes a development of smart city and smart home, continuous patient monitoring system, and environmental monitoring. Nowadays, the data generation sources are enlarged noticeably, such as high-end streaming devices, wireless sensor networks, satellite, wearable IoT devices. IoT devices generate a massive volume of data (Big data) in a continuous manner. Big data refers to a collection of massive volume of data that cannot be processed by conventional data processing tools and technologies. The explosion of multimedia big data has created unprecedented opportunities and fundamental security challenges as they are not just big in volume, but also unstructured and multi-modal. The massive transmission of connected devices in the IoT has generated enormous demand for robust security in response to the growing demand of billions of connected devices worldwide. The number of threats is rising daily, and attacks have been on the increase in both number and complexity. Hence, the cyber security algorithms and architectures are required for IoT with data confidentiality, integrity, authenticity and authorization. Moreover, privacy protection must also be considered. Many IoT devices and critical infrastructures produce an enormous amount of personal and sensitive data which may be abused by unauthorized users and intruders.

The vital role of this special issue is to deliver a foremost global platform for an extensive range of professions including academicians, scholars, researchers, and individuals who works in industry to deliberate and present the most recent privacy and cyber security issues, challenges and advancements in multimedia big data in Smart Grid, Smart vehicle, Smart cloud and Smart home from an outlook of providing security awareness and its best practices for the everyday life.

The intention of this special issue is to focus the most recent advances in research topics that include but are not limited to:

- Smart grid security
- Urban transportation system security
- Access control of Big Data
- Privacy aware data fusion of Big Data
- Cryptographic protocols against attacks
- Big data forensics
- Security protocols in IoT
- Privacy protocols in IoT

- Cryptography and Big Data
- Multimedia big data
- Security and privacy of big data in IoT
- Intrusion detection systems in IoT
- Storage and system security for Big Data
- Wireless sensor network security and privacy
- Security and privacy of multimedia information

Notes for Prospective Authors

The special issue on “Cyber Security and Privacy of IoT-enabled Infrastructures in Smart Grid, Smart vehicle, Smart cloud and Smart home”; in Concurrency and Computation: Practice and Experience issue will carry revised and substantially extended versions of selected papers presented at the 5th EAI International Conference on Big data and Cloud Computing Challenges, March 8–9, 2018, Chennai, Tamilnadu, India, but we also strongly encourage researchers unable to participate in the conference to submit articles for this open call.

All papers are refereed through a peer review process. All papers must be submitted online. To submit a paper, please read our Submitting articles page. If you have any queries concerning this special issue, please email the Guest Editors:

Important Dates:

Manuscripts due by: *28 July, 2018*

Notification to authors: *30 Sep, 2018*

Final versions due by: *15 Nov, 2018*

Guest Editors:

Dr. Gunasekaran Manogaran, VIT University, Vellore, India gunavit@gmail.com

Dr. Naveen Chilamkurti, LaTrobe University, Melbourne, Australia,
n.chilamkurti@latrobe.edu.au

Dr. Ching-Hsien Hsu, Chung Hua University, Taiwan chh@chu.edu.tw

Dr. V. Vijayakumar VIT University, Chennai, India, vijayakumar.v@vit.ac.in