CALL FOR PAPERS
for Special Section on

Security & Privacy for Cloud-Assisted Internet of Things (IoT) and Smart Grid Applications

Theme: Cloud computing has emerged as a new technological domain in the IT industry. Virtualization is one of the key technologies in the cloud environment which enables the creation of an intelligent abstraction layer, called Virtual Machine Monitor (VMM) or Hypervisor. Currently, several organizations working in various domains such as healthcare, finance, manufacturing, smart grid, Internet of Things (IoT) and IT etc. are increasingly integrating cloud computing with their traditional applications. The key idea behind the usage of cloud computing in IoT, is to increase the efficiency without compromising the data quality. When it comes to collecting data of thousands or millions of servers, cloud offers scalability and reduces the computational load on each sensor. The highly configured servers in cloud are very useful in processing and analyzing the sensors’ data. These days many cloud service vendors such as AWS, Google, and IBM etc. are offering the IoT–based services along with the data analytics services. These services can easily be incorporated along with the IoT-applications. In addition to IoT, cloud computing platform is also suitable for smart grid applications because of its elastic, scalable, dynamic and shared nature of services. The electric power utilities use smart grid (SG) to track and control the power usage of the consumers. The Smart Grid (SG) is used by electric power utilities to track and control power usage of consumers. The entire protection devices and power supply management systems are controlled by control servers to provide strong security to smart grid load balancing systems during communication. The communication process is facilitated through the cloud servers between power supply companies and substations. The strong security frameworks are essential during communication. As the smart grid software applications are also hosted on cloud servers, data privacy and security is a very strong concern. Many applications are hosted on each cloud servers. The security of such a shared infrastructure is a very crucial. In addition, the network traffic should also be secured at the same time along with securing the stored data of consumer and companies and SG applications in cloud servers. However, security is the major barriers in adoption to cloud based services, followed by issues regarding compliance, privacy, and legal matters.

The purpose of the special issue is to publish high-quality papers addressing state-of-the-art security & privacy issues for Cloud-Assisted Internet of Things (IoT) and Smart Grid (SG) applications. We are soliciting original contributions, of leading researchers and practitioners from academia as well as industry, which address a wide range of theoretical and application issues in this domain.

Topics include, but are not limited to, the following research topics and technologies:

Security & Privacy for Cloud-Assisted Internet of Things (IoT):
1. SP - Cloud-Assisted IoT privacy preserving frameworks to prevent non-authorized data acces
2. SP - Cloud-Assisted secure communications strategies to detect and mitigate IoT attacks
3. SP - Cloud-Assisted IoT security & privacy frameworks
4. SP - Cloud-Assisted IoT Malware Detection and Prevention Strategies
5. SP - Trust management in Cloud-Assisted IoT applications
6. SP - Cloud-Assisted IoT security Techniques/architectures
7. SP - IoT attacks analysis using Cloud Servers
8. SP - Cloud-Assisted Big data analytics for IoT security & Privacy
10. SP - Cloud-Assisted Block-chain based IoT security frameworks

Security & Privacy for Cloud-Assisted Smart Grid Applications:
1. SP - Cloud-Assisted security and privacy frameworks and models for Smart Grid
2. SP - Big Data security analysis in Cloud-Assisted Smart Grid
3. SP - Cloud-Assisted integrated secure frameworks for renewable energy resources in Smart Grids
4. SP - Cloud-Assisted secure energy management frameworks for Smart Grid
5. SP - Secure real time communication in Cloud-Assisted Smart Grids
6. SP - Machine learning for secure Cloud-Assisted Smart Grid frameworks
7. SP - Deep models for secure Cloud-Assisted smart grid frameworks
8. SP - Data security and privacy techniques/architectures in Cloud-Assisted Smart Grids
9. SP - Integrated simulation, testbed and case Studies for Smart Grid security and privacy
10. SP - Attack Detection, Mitigation and Attribution in the Cloud-Assisted Smart Grid
11. SP - Cloud-Assisted Block-chain based Smart Grid security frameworks

Manuscript Preparation and Submission
Follow the guidelines in “Information for Authors” in the IEEE-IES website: http://www.ieee-ies.org/pubs/transactions-on-industrial-informatics. Please submit your manuscript in electronic form through Manuscript Central website: https://mc.manuscriptcentral.com/tii. On the submitting page #1 in popup menu of manuscript type, select SS on

Security & Privacy for Cloud-Assisted Internet of Things (IoT) and Smart Grid Applications

Submissions to this Special Section must represent original material that has been neither submitted to, nor published in, any other journal. Regular manuscript length is 8 pages.

Note: The recommended papers for the section are subject to final approval by the Editor-in-Chief. Some papers may be published outside the special section, at the EIC discretion.

Timetable:
Deadline for manuscript submissions March 15, 2021
Expected publication date (tentative) August, 2021

Guest Editors:
Dr. Preeti Mishra, Graphic Era Deemed to be University, Dehradun, India scholar.preeti@gmail.com
Dr. Ankit Vidyarthi, Jaypee Institute of Information Technology Noida, India ankit.vidyarthi@jiit.ac.in
Dr. Pierluigi Siano, University of Salerno, Italy p.siano@unisa.it

Editor-in-Chief: Prof. Dr.-Ing. Ren C. Luo
tii@ira.ee.ntu.edu.tw
http://www.ieee-ies.org/pubs/transactions-on-industrial-informatics