# IEEE Internet of Things Journal Special Issue on
# "Secure Data Analytics for Emerging Internet of Things"

The recent rapid proliferation in hardware, software, and communication technologies have facilitated the spread of interconnected sensors, actuators and heterogeneous devices such as single board computers, which collect and exchange a large amount of data to offer a new class of advanced services characterized by being available anywhere, at any time and for anyone. This ecosystem is widely referred to as the Internet of Things (IoT). IoT networks collect, store, and exchange a large volume of heterogeneous data. It has already shown promising outcomes in the provisioning of potentially critical services (e.g., safety applications, healthcare, manufacturing) raise numerous issues related to the security, data analysis and energy awareness of the performed operations and provided services. Accordingly, research on the data analysis and security of IoT is attracting increasing attention from both industry and academia. In line with these efforts, the central theme of this Special Issue is to report novel methodologies, theories, technologies, techniques, and solutions for security and data analytics techniques and energy aware solutions for IoT.

This Special Issue aims at addressing these topics across multiple abstraction levels, ranging from architectural models, the provisioning of services, protocols and interfaces to specific implementation approaches. Furthermore, additional focus will be given to areas related to the role of data mining and machine learning in modeling and deploying secure and trustworthy sensor and wireless networks for IoT systems. It aims to present the most important and relevant advances to overcome the challenges related to security, data analytics, and energy aware solutions in Internet of Things.

**Topics of interest include, but are not limited to:**

- Novel security architectures, protocols, or applications for IoT
- Privacy preservation in IoT
- Vulnerability analysis in the IoT
- Threat modelling and Risk assessment in IoT
- Intrusion detection for IoT
- Context aware machine-learning-based data analytics in IoT
- Federated Learning and IoT Security
- 5G &B enabled Programming models for IoT.
- Interpretable Machine learning and IoT
- Security testbeds and experimental results for IoT
- Lightweight and Homomorphic security protocols for IoT
- Privacy enhancing and anonymization techniques in sensor networks and the IoT
- Trust and identity management in IoT
- Access control for shared data in IoT devices
- Game theory-based security framework for IoT

## Important Dates:

Submission Deadline: January 1, 2021
First Review Due: March 15, 2021
Revision Due: May 1, 2021
Sec. Reviews Due/Notification: June 1, 2021
Final Manuscript Due: June 15, 2021
Publication Date: 2021

## Submission Guidelines:

Authors need to follow the manuscript format and an allowable number of pages described at https://ieee-iotj.org/guidelines-for-authors/. To submit a manuscript for consideration for the special issue, please visit the journal submission website at https://mc.manuscriptcentral.com/iot.

## Guest Editors

Sachin S Shetty, Old Dominion University, USA, sshetty@odu.edu
Uttam Ghosh, Vanderbilt University, USA, uttam.ghosh@vanderbilt.edu
Schahram Dustdar, TU Wien, Austria, dustdar@dsg.tuwien.ac.at
Jhing-fa Wang, National Cheng Kung University, Taiwan, jameswangjf@gmail.com