IEEE Internet of Things Journal

Special Issue on Industrial Security for Smart Cities

More than half of the world's current population resides in urban areas to compare to with just 30% in the 1950s. The process of urbanization leads to exurban sprawl, the formation of slums, scattered workplaces, and aging infrastructure. These may cause huge inefficiencies in energy use, traffic, governance, waste management, and pollution, among others. To overcome these social, economic, and environmental challenges, public and private sectors invest heavily in smart city technologies. However, the risks of using smart technologies in critical sectors should be addressed.

Attackers would set their sights on smart cities for a number of reasons. Malicious individuals may consider smart cities as playgrounds they can test their hacking skills on. They may toy with available technologies for personal satisfaction. For cybercriminals, the interconnectedness of devices and systems in a smart city can be a means to steal money and data from citizens and local enterprises. State-sponsored actors can also abuse the pervasiveness of smart city technologies to launch their own espionage or hacktivist campaigns. In some very extreme cases, smart implementations may even be exploited for acts of terror. Therefore, researchers and engineers should provide actionable solutions and methods to help local governments and urban developers design more secure smart cities.

The aim of this special issue is to foster novel and multidisciplinary approaches that improve industrial security for smart cities by taking into consideration various challenges faced by industrial applications.

Scope of the Special Issue

- AI and machine learning for intrusion detection and intelligence
- Blockchain technologies in industrial security solutions
- Industrial security solutions and privacy in smart city
- Cloud computing integration and big data analysis in industrial security
- Communication protocols in industrial security
- Industrial security solutions for data visualization, augmented and virtual reality
- Security for smart transportation system planning, evaluation, and technologies
- Security solutions for sewage, water and electricity management
- Security for emergency management and infrastructures
- Security solutions for healthcare service monitoring
- Security for crime watching and alerting systems
- Security education, training and social services
- Security for smart home, smart building and social community networks/infrastructures
- Security solutions for networking, services and infrastructures and reliability
- Secure and smart environment modeling, monitoring, prediction and analysis
- Security solutions of big data, open data, and urban computing
- Security for smart utilities, consumption, sensing and Internet of Things
- Security for smart communities and neighborhoods

Submission Guidelines: Authors need to follow the manuscript format and an allowable number of pages described at http://ieeeiotj.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.

Important Dates

Submission Deadline: July 1, 2020 First Review Due: September 15, 2020

Revision Due: October 30, 2020 Sec. Reviews Due/Notification: November 30, 2020

Final Manuscript Due: December 15, 2020

Guest Editors

Huimin Lu, Kyushu Institute of Technology, Japan (dr.huimin.lu@ieee.org)

Pin-Han Ho, University of Waterloo, Canada (p4ho@uwaterloo.ca)

Mohsen Guizani, University of Idaho, USA (mguizani@gmail.com)