Annals of Telecommunications

Call for papers
Special Issue on

Security and Privacy for IoT and Smart Cities: Recent Advances and Challenges

---

Guest Editors

Dr. Weizhi Meng (Technical University of Denmark, Denmark)
Prof. Steven Furnell (University of Nottingham, UK)
Prof. Guo Song (The Hong Kong Polytechnic University, Hong Kong)
Prof. Jun Shao Zhejiang (Gongshang University, China)

A smart city is a newly developed concept, referring to an urban area using different kinds of electronic sensors to collect data and supply information, including data collected from citizens, devices, and assets. It integrates information and communication technology (ICT), various physical devices, and citizen services. To establish a smart city, Internet of Things (IoT) is an important basis, where connected devices in a smart city are not limited to static sensors anymore, but also include any personal wearable devices such as mobile phones, smart watch, smart glasses, etc. It was expected to reach 53.63 million connections in EU by 2025. However, IoT may also bring notable vulnerabilities to smart cities. For example, in late 2021, a group of hackers took down a power grid in a region of western Ukraine to cause the first blackout from a cyber attack. For privacy, around 10,000 households can generate 150 million discrete data points every day. This creates more entry points for hackers and leaves sensitive information vulnerable. Due to these security and privacy issues to IoT-based smart cities, there is a strong need to develop appropriate mechanisms to protect the security and privacy for IoT networks and smart city infrastructures.

This special issue intends to gather cutting-edge results on addressing security and privacy issues for IoT-enabled smart cities. The aim is to promote research and learn recent advances in the domain of IoT and smart cities.

In particular, the topic of interest includes but is not limited to

- Post-quantum security for IoT-enabled smart cities
- Secure design for IoT and smart cities
- Side-channel analysis for the security and privacy of IoT-enabled smart cities
- Security and risk analysis for IoT-enabled smart cities
- Privacy and anonymization techniques for IoT-enabled smart cities

- Trust management architectures for IoT-enabled smart cities
- Lightweight security solutions for IoT-enabled smart cities
- Sustainability solutions for IoT and smart cities
- Authentication and access control for IoT-enabled smart cities
- Innovative security techniques for smart city infrastructure
- Internet of Things devices and protocols security
- Cloud computing-based security solutions for IoT-enabled smart cities
- Critical infrastructures privacy and security for IoT-enabled smart cities
- Biometric modalities for IoT-enabled smart cities
- Cyber-attacks detection and prevention systems for IoT-enabled smart cities
- Interoperable security for smart city planning and applications
- Blockchain technologies for smart city security and privacy
- Edge computing for smart city security and privacy

Submission Guidelines:

All submissions have to be prepared according to the Guide for Authors as published in the Journal website at:

https://www.springer.com/journal/12243/submissionguidelines

Authors should submit online at:

https://www.editorialmanager.com/ante/

by selecting "SI: Security and Privacy for IoT and Smart Cities: Recent Advances and Challenges" from the " Special Issues" pull-down menu during the submission process.

All contributions must not have been previously published or be under consideration for publication elsewhere. A submission based on conference paper version should add at least 40% new material. Authors are required to attach to the submitted paper their relevant, previously published articles and a summary document explaining the enhancements made in the journal version.

All papers will be peer-reviewed by at least two independent reviewers.

Requests for additional information should be addressed to the leading guest editor (Dr. Weizhi Meng, weme@dtu.dk).

Proposed Schedule

Submission deadline: December 31, 2022
Initial notification: February 28, 2023
Final Acceptance/rejection notification: May 31, 2023
Online with DOI: as soon as accepted
Printed issue: second half of 2023

Editor Biography:

Weizhi Meng is currently an Associate Professor in the Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Denmark. He obtained his Ph.D. degree in Computer Science from the City University of Hong Kong (CityU), Hong Kong. Prior to joining DTU, he worked as a research scientist at the Institute for Infocomm Research, A*STAR, Singapore. His primary research interests are cyber security and intelligent technology in security including intrusion detection, smartphone security, biometric authentication, HCI security, cloud security, trust management, malware detection, blockchain in security, cyber-physical system security and IoT security. He is currently directing the SPTAGE Lab at DTU Compute, DTU, and received the IEEE MGA Young Professionals Achievement Award in 2020 for his contributions to leading activities in Denmark and Region 8. He is the associate editor / editorial board member for many journals such as IEEE TDSC, IJIS, JISA, SCN, WCMC, etc. He was also guest editor for IEEE TII, JSS, FGCS, SCN, WCMC, NCAA, CAEE, CCPE, etc.

Steven Furnell is a professor of cyber security at the University of Nottingham in the United Kingdom. He is also an Adjunct Professor with Edith Cowan University in Western Australia and an Honorary Professor with Nelson Mandela University in South Africa. His research interests include usability of security and privacy, security management and culture, and technologies for user authentication and intrusion detection. He has authored over 350 papers in refereed international journals and conference proceedings, as well as various books, book chapters and industry reports. Prof. Furnell is the UK representative to Technical Committee 11 (security and privacy) within the International Federation for Information Processing, as well as the editor-in-chief of Information and Computer Security, and a Fellow and board member of the Chartered Institute of Information Security.

Song Guo is a Full Professor at Department of Computing, The Hong Kong Polytechnic University. He also holds a Changjiang Chair Professorship awarded by the Ministry of Education of China. Prof. Guo is a Fellow of the Canadian Academy of Engineering and a Fellow of the IEEE (Computer Society). His research interests are mainly in edge AI, machine learning, mobile computing, and distributed systems. He published many papers in top venues with wide impact in these areas and was recognized as a Highly Cited Researcher (Clarivate Web of Science). He is the recipient of over a dozen Best Paper Awards from IEEE/ACM conferences, journals, and technical committees. Prof. Guo is the Editor-in-Chief of IEEE Open Journal of the Computer Society and the Chair of IEEE Communications Society (ComSoc) Space and Satellite Communications Technical Committee. He was an IEEE ComSoc Distinguished Lecturer and a member of IEEE ComSoc Board of Governors. He has served for IEEE Computer Society on Fellow Evaluation Committee, and been named on editorial board of a number of prestigious international journals like IEEE TPDS, IEEE TCC, IEEE TETC, etc. He has also served as chairs of organizing and technical committees of many international conferences.

Jun Shao received the Ph.D. degree from the Department of Computer Science and Engineering at Shanghai Jiao Tong University, Shanghai, China in 2008. He

was a postdoc in the School of Information Sciences and Technology at Pennsylvania State University, USA from May 2008 to April 2010. He was also a visiting professor in the Faculty of Computer Science, University of New Brunswick, Canada from October 2017 to March 2018. He is currently a professor of the School of Computer and Information Engineering at Zhejiang Gongshang University, Hangzhou, China. His research interests include applied cryptography, network security, and AI security

Published by Springer, *Annals of telecommunications*
is indexed in ISI and Scopus Databases, 2021 Impact Factor: 1.901