
**Call for papers**
**Special Issue on**

# Security and Trust in Ubiquitous Systems

## Lead Guest Editor

- **Prof. Samia Bouzefrane,** Conservatoire National des Arts et Métiers, France

## Guest Editors

- **Prof. Jenny Gabriela Torres Olmedo,** Escuela Politecnica Nacional, Ecuador
- **Prof. Gongxuan Zhang,** Nanjing University of Science and Technology (NJUST), China

## Topics of interest for this special issue include but are not limited to:

- Security/Cybersecurity in ubiquitous systems
- Data privacy in ubiquitous systems
- Intrusion detection and resiliency in ubiquitous systems
- Secure data analytics for ubiquitous systems
- Adaptive intelligence in security measures for ubiquitous systems
- Trust computing for ubiquitous systems
- Hardware trusted platforms, secure elements, trusted execution environment for ubiquitous systems
- Reputation-based recommendation systems for ubiquitous systems

5G will enable massive Internet of Things (IoT) applications and domains such as connected cars, smart cities, smart homes, wearables, health care devices, smart factories, smart farming, and other IoT devices. One of the IoT-applications requirements that 5G must meet is the security/cybersecurity. Security must be delivered from design to protect the networks, the applications and the services. By extending the vision to IoT devices that are resource-constrained, new types of security threats are introduced hence increasing the attack surface.
In addition to the traditional security properties that are required to secure networks, platforms, services and users, trust and reputation are the other concerns in ubiquitous environments either in business or in mission-critical applications. While trust can rely on hardware trusted platforms and secure elements, reputation is built upon recommendation systems which may use artificial-intelligence mechanisms.

Ubiquitous systems may refer to any pervasive system such as: IoT, Cyber physical systems, edge computing, mobile computing, cloud computing, etc. Designing secure and data-protected solutions for these systems require to meet key constraints such as scalability, maintainability and performance.

This special issue aims to collect and report on recent research and advanced knowledge related to security and trust in ubiquitous systems.

Papers must describe original research that advances state-of-the-art research and must not be simultaneously submitted to a journal or a conference with proceedings. Papers must be written in excellent English and should not exceed 10 pages. Previously published or accepted conference papers must contain at least 50% new material to be considered for the special issue. A covering letter to the Guest editors clearly describing the extensions made must accompany these types of submissions.
All submissions must be made using the instructions available at: http://annalsoftelecommunications.wp.mines-telecom.fr/how-to-publish/

The authors can directly submit their papers at: https://www.editorialmanager.com/ante/ and must select the item “CfP: Security and Trust in Ubiquitous Systems” when answering the submission questionnaire.

**Proposed schedule**

- **Manuscript submission** ~~December 15, 2019~~ Extended to January 31, 2020
- **Online with DOI** As soon as accepted
- **Printed issue** Early 2021

---

Springer **Published by Springer, *Annals of telecommunications* is indexed in ISI and Scopus Databases, 2018 Impact Factor: 1.55 2087 *Journal Citation Reports* ® Science Edition (Thomson Reuters, 2019)**

Institut Mines-Télécom