Wireless Communications and Mobile Computing

WILEY | Hindawi

Special Issue on

On Context-Aware Security in Cloud Computing and Internet of Things

CALL FOR PAPERS

Cloud Computing and Internet of Things are emerging industry directions. One brings great scalability potential with the ability to reflect customer demands, optimizing resource usage. The other brings us the ability to interconnect a large number of heterogeneous devices, cars, buildings, sensors, and other things together. However, these technologies must deal with multiple challenges and in many cases rather novel technology approaches. One has the ability to process a lot of data, while the other has the ability to produce a lot of data.

Can we, however, trust our users, the data origin, or content, or do we need to involve multifactor authentication? Could the context-awareness provide an alternative approach, determine the security enforcement, or even simplify interaction in these environments? Both Cloud Computing and Internet of Things must deal with various challenges with regard to their security, privacy, or isolation. Can context-awareness bring better security measures? Context-awareness tracking location of users or devices, the environment metadata, and other elements can be utilized when system performs security-based decisions. How can context-awareness influence security and personalization and how can we employ it to improve usability? How can we assure that compromised device does not take the advantage from context-fabrication? Can we determine based on the context that user is really who claim to be?

Potential topics include but are not limited to the following:

- Context-aware security
- Context collection in IoT
- Context-awareness for secure device-free interaction
- Context-aware cloud-based solutions
- System monitoring and quality of service utilizing context
- Contextual M2M transmission
- Context-aware security as an alternative to multifactor authentication
- Strategies to prevent system vulnerability involving context-awareness
- Formal models and metrics for secure contextual systems
- Save context manipulation on mobile devices
- Detecting system malfunction through neighboring network of devices
- Strategies to identify intruder or malfunction in distributed environments
- Fair scheduling for heterogeneous workloads based on context
- Vulnerability system evaluation and testing involving context-aware tools

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/wcmc/ccit/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Tomas Cerny, Baylor University, Waco, USA
tomas_cerny@baylor.edu

Guest Editors
Jinman Jung, Hannam University, Daejeon, Republic of Korea
jmjung@hnu.kr

Junyoung Heo, Hansung University, Seoul, Republic of Korea
jyheo@hansung.ac.kr

Michael J. Donahoo, Baylor University, Waco, USA
jeff_donahoo@baylor.edu

Sriram Sankaran, Amrita University, Amritapuri, India
srirams@am.amrita.edu

Bestoun S. Ahmed, Czech Technical University in Prague, Prague, Czech Republic
albeybes@fel.cvut.cz

Submission Deadline
Friday, 5 October 2018

Publication Date
February 2019