Wireless Communications and Mobile Computing

WILEY | **Hindawi**

Special Issue on
Recent Advances in Mobile Cloud Computing

CALL FOR PAPERS

Mobile devices like smartphones, laptops, tablets, computers, and so forth are upgraded day by day in the market and have also become an essential need for everyone. However, mobile devices face many resource and other challenges (battery life, storage, bandwidth, security, etc.). To solve these problems, researchers have introduced a trusted and dependable solution, called Mobile Cloud Computing (MCC), which refers to an infrastructure where both data storage and data processing happen outside the mobile device. Moreover, mobile cloud applications move the computing power and data storage away from the mobile devices and into powerful and centralized computing platforms located in clouds, which are then accessed over the wireless connection based on a thin native client. As in every new technology, some challenges face the vision of the Mobile Cloud Computing, which are the administrative policies and security concerns (i.e., secure data storage, secure computation, network security, data privacy, location privacy, etc.).

This special issue aims to investigate the opportunities and requirements for Mobile Cloud Computing dominance. In addition, it seeks novel contributions that help mitigate Mobile Cloud Computing challenges.

Potential topics include but are not limited to the following:

- Privacy-preserving protocols in Mobile Cloud Computing
- Access control mechanisms in Mobile Cloud Computing
- Cryptography cloud storage
- MCC pricing and billing models
- MCC support for VANETs and MANETs
- Lightweight authentication mechanisms in MCC architecture
- Access control models in MCC
- The future perspective for MCC: challenges and open issues
- MCC quality of service (QoS) improvements techniques
- Social engineering, insider threats, and advanced spear phishing
- Forensics of virtual and MCC environments
- Security protocols in MCC
- Mobile malware collection, statistics, and analysis
- Reverse engineering and automated analysis of mobile malware
- Benchmarking and evaluation of mobile security solutions
- Android device forensics
- Security and privacy in mobile operating systems
- Mobile system vulnerability detection and remediation

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

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

Lead Guest Editor
Dharma P. Agrawal, University of Cincinnati, Cincinnati, USA
dpa@cs.uc.edu

Guest Editors
B. B. Gupta, National Institute of Technology, Kurukshetra, India
bbgupta@nitkkr.ac.in

Shingo Yamaguchi, Yamaguchi University, Yamaguchi, Japan
shingo@yamaguchi-u.ac.jp

Konstantinos E. Psannis, University of Macedonia, Thessaloniki, Greece
kpsannis@uom.edu.gr