Special Issue Call for Papers

Special Issue on Secure Cloud Computing for Mobile Health Services

Guest Editors:

Dr. Haidar Abbas  
King Saud University, Riyadh  
Email: haidera@kth.se

Prof. Sudip Misra  
Indian Institute of Technology, Kharagpur  
Email: smisra@sit.iitkgp.ernet.in

Dr. Sana Ullah  
ISEP, Polytechnic Institute of Porto  
Email: sana.ullah.2013@ieee.org

Prof. Yuh-Shyan Chen  
National Taipei University  
Email: yschen@mail.ntpu.edu.tw

The huge amount of medical and biological data has been managed electronically and it has demanded the seamless availability of E-health applications anywhere anytime. This demand has paved the ways for cloud and modern healthcare technologies deployment in telemedicine and mobile healthcare services. While on the other hand, this rapidly evolving cloud computing technologies and their deployment in mobile healthcare systems also pose many unseen threats disguised in this technology giant. And these might affect the conducive working environment of a healthcare organization and its smooth processes from patient’s data privacy to healthcare records protections and their secure transmission among various healthcare locations. These unseen threats could be due to the vulnerabilities inherited/disguised in any of the cloud deployment model (Public/Private) or service delivery model (IaaS, PaAS ,SaaS) that appear with the time after the technology is deployed. Since by the time, the critical healthcare processes would be relying on the newly deployed cloud technology; appearing such issues would affect adversely and become intolerable. Many healthcare organizations has faced numerous loses including public confidence due to these security flaws in recent years. Although the cloud security efforts and technologies have evolved significantly but it still remains a challenging task (due to novel unseen and continuously emerging threats) and requires a continuous struggle to address these issue. The other significant reason is the repeated and sophisticated security attacks that continuously introduce malicious softwares and pose threats to patient’s data privacy and healthcare security.

The aim of this special issue is to provide original and the latest contributions, and to review and survey research and development on information assurance, data privacy and applications security in mobile healthcare systems that would help users to strengthen their security parameters. Topics of interest include, but are not limited to, the following:

- Data storage and management (physical storage & availability issues, maintenance, etc.)
- Healthcare data protection
- Healthcare application’s security
- Vulnerability assessment in healthcare systems
- Unified and ubiquitous access (platforms, infrastructures, interfaces) of healthcare systems
- Secure healthcare information exchange based on mobile agents
- Healthcare data/system integrity
- Data security and data privacy for mobile healthcare devices
- Identity theft and related abuses
- Healthcare data security strategies
- Intrusion detection in healthcare care systems
- Healthcare security policies and procedures
- Healthcare data tampering
- Healthcare database security
- Trust management

Important Dates

- Paper submission: Nov. 15, 2014
- 1st round review notification: Dec. 30, 2014
- 1st revision due: Jan. 30, 2014
- 2nd round review notification: Feb. 28, 2015
- 2nd revision due: Mar. 25, 2015
- Final acceptance notification: April 30, 2015

www.Springer.com/12083