Association for Computing Machinery

ACM Transactions on Internet Technology – Special Issue on

Security and Privacy of Medical Data for Smart Healthcare

Special Issue Guest Editors

Dr. Amit Kumar Singh
(Corresponding GE)
National Institute of Technology, Patna, India
amit_245singh@yahoo.com
amit.singh@nitp.ac.in

Prof. Jonathan Wu
University of Windsor, Windsor, ON, Canada
jwu@uwindsor.ca

Prof. Ali Al-Haj
Princess Sumaya University for Technology, Jordan
ali@psut.edu.jo

Prof. Calton Pu
Georgia Institute of Technology, USA
calton.pu@cc.gatech.edu

Important Deadlines

- Manuscript submission: July 15, 2020 **(NEW)**
- First notification: August 31, 2020
- Submission of revised manuscript: September 30, 2020
- Final notification: October 30, 2020
- Final submission (camera-ready): November 30, 2020

ACM TOIT Editor-in-Chief

Prof. Ling Liu
School of Computer Science, Georgia Institute of Technology
ling.liu@cc.gatech.edu

Recently, the prevalent appearance of smart networks as well as the attractiveness of electronic supervision of medical reports made it feasible for digital medical images to be distributed all over the world for smart healthcare services. Further, implementing medical services has become an emerging trend at global level. In these services, medical data are exchanged between healthcare professionals for better diagnosis purpose. The information and communication technology (ICT) has been useful for cost-effective and fast transmission of electronic medical records (EMR) over open channels for smart healthcare applications. However, transmission of medical images or EMR over open networks needs a high degree of security. The modified, altered or corrupted medical data can cause wrong diagnoses and create serious health issues for individuals. In addition, medical identity theft is a growing concern and has contributed to large amount of e-fraud cases across the world. Research established that watermarking based methods are among the best traceability techniques in the healthcare domain.

The objective of this special issue is to attract high-quality research and survey articles that promote research and reflect the most recent advances in addressing the security and privacy issues of the medical data for smart healthcare applications. We welcome researchers from both academia and industry to provide their state-of-the-art technologies and ideas covering all aspects of security and privacy solutions for medical/healthcare applications.

Potential topics include but are not limited to the following:

- Watermarking, steganography, hidden data
- Multimedia big data analytics for smart healthcare
- Health data management
- Cryptographic algorithms and protocols
- Security and privacy of smart healthcare media data
- Privacy in the Internet of Things for smart healthcare
- Protection systems against person identity theft
- Bio-signal processing
- Media cloud applications for healthcare
- Display or secure transmission of images
- Medical image processing
- Biometrics
- Imaging
- Medical image data compression
- Cybersecurity for healthcare
- Blockchain for medical records

Submission Instructions:
Please refer to https://dl.acm.org/journal/toit/author-guidelines
Please select “Special Issue on Security and Privacy of Medical Data for Smart Healthcare” in the TOIT Manuscript Central website.