Wireless Communications and Mobile Computing

WILEY | Hindawi

Special Issue on

Security Threats and Challenges in Future Mobile Communication Systems

CALL FOR PAPERS

According to the numbers from Statista, there are about 3.5 billion smartphone users worldwide. This figure translates to 45% population of users across the globe. Mobile phones have surpassed their capacity just as calling devices, now they are functioning like personal assistants. Mobile phones are used for banking, online shopping, bill payments, social media presence, booking appointments, conference calls, etc. There are small businesses that are solely run through mobile phones. The smartphones help handle the business and manage the ledger. The share of banking and shopping apps is humongous among other mobile apps and the same can be said for the traffic generated by them. In this scenario, security is of foremost importance in mobile communication. There has been an immense growth in mobile communication, and in the presence of high-speed 4G networks, there is a large market of mobile applications. The opportunities that mobile applications are providing are immense but at the same time, it raises the serious question of security, which is equally important at each level, at the customer end, service provider's end, and at the level of the network provider. The devices are also becoming secure from a pattern/pin-based login, almost all mobile devices shift towards fingerprint or face recognition-based authentication. An averagely active mobile customer uses applications related to social media, banking transactions, and online shopping. A security hassle in social media applications poses the danger of personal information getting leaked in public. Therefore, most social media applications are providing password or pin-based authentication.

Although, given to the weak nature of password/pin-based security, these applications are now shifting towards fingerprint-based authentication. The banking apps are boon to customers, using these apps, banking transactions can be carried out in a jiffy. Security is a prime concern in such apps, and almost all banking applications provide a two-stage authentication process. This app features fingerprint-based or pin/password-based logins and provides an additional layer of security in the form of a one-time password (OTP) for transactions. A similar kind of authentication and security is required in online shopping applications. Even in the presence of such security precautions, there is a substantial chance of security breach due to hacking and phishing attacks. Security at the service provider end is another major challenge in mobile applications; there is often news of password leaks from the servers of service providers due to hacking attacks. Thirdly, there is a network provider side and encryption plays an important role in securing communication over wireless networks. There are recent developments in technologies such as the Internet of Things (IoT), which helps improve mobile phones. Mobile phones act as a point of control and management for IoT devices, therefore not noticing security concerns may lead to a disastrous outcome. Apart from these, medical and health-based applications are also a major part of the mobile application market. Therefore, there is a considerable requirement in research in the field of security in mobile communication. To enhance mobile communication security, the disciplines like signal/image processing, data handling, deep learning, and IoT have to come together in conjunction.

The aim of this Special Issue is to bring together original research and review articles discussing the security threats and challenges in future mobile communication systems.

Potential topics include but are not limited to the following:

- Protocols for access control, authentication, and authorization in future mobile communications
- Abnormity detection and control protocols for mobility in future mobile communication
- Security framework for future mobile communication networks
- AI-based protocols to resist compulsive attacks in mobile communication
- Deep learning integrated identification and authentication protocols for mobile communication
- Secure data acquisition and mining for user demand cells in future mobile communication
- Security in edge and fog computations in future mobile communication
- Network and transport layer security for 5G and beyond cellular communication
- Machine learning (ML) integrated end-to-end security protocol for mobile communications
- Security framework for mobile E-services in future mobile communication
- Blockchain-based authentication of information transmission for cooperative mobile users
- Secure cloud-based mobile computation in future mobile communication

Authors can submit their manuscripts through the Manuscript Tracking System at https://review.hindawi.com/submit?specialIssue=550320.

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

Lead Guest Editor
Deepak Kumar Jain, Chongqing University of Posts and Telecommunications, Chongqing, India
deepak@cqupt.edu.cn

Guest Editors
Joel J. P. C. Rodrigues, Federal University of Piauí, Piauí, Brazil
joeljr@ieee.org

Maode Ma, Nanyang Technological University, Singapore
emdma@ntu.edu.sg

Fei Hao, Shaanxi Normal University, Xi'an, China
fhao@snnu.edu.cn

Submission Deadline
Friday, 18 March 2022

Publication Date
August 2022