Call for Papers

Security and Privacy for eHealth/mHealth Systems in the IoT Era Workshop

The 17th International Conference on Wireless Communications and Mobile Computing

IWCMC 2021

IWCMC 2021 Website: http://iwcmc.org/2021/

Submission Link: https://edas.info/newPaper.php?c=27588

Harbin, China

June 28 — July 2, 2021

Organizing Committee

Chairs:

Khalid Abualsaud, Qatar University, Qatar, abualsaud@ieee.org

Elias Yaacoub, Qatar University, Qatar, eliasy@ieee.org

Tamer Khattab, Qatar University, Qatar, tkhattab@ieee.org

Scope

With the proliferation of the "Internet of Things" (IoT), interconnected digital devices can now enable the collection and exchange of huge amounts of information, thus creating interesting opportunities in different sectors, including agriculture, energy, transportation, education, and more importantly, healthcare. In this context, remote patient monitoring using wearable sensors presents an efficient low cost solution targeting preventive care and continuing care, while reducing the number of doctor visits which, in turn, reduces overcrowding in hospital emergency services.

However, these technological advances also open the door to new threats stemming from a broad range of sources, ranging from attackers with malicious intent to opportunists exploiting system vulnerabilities to cause deliberate or accidental harm. The cyber threat landscape has indeed evolved from individual hackers to highly organized groups and advanced cyber-criminal syndicates, with healthcare as one of the major targets. Moreover, the very nature of IoT eHealth/mHealth devices – small with limited capabilities – renders them a prime target for cyber-attacks that can compromise the highly sensitive nature of the data carried by those, otherwise simple devices. Consequently, to ensure a successful deployment of eHealth/mHealth systems, and to increase the acceptability of citizens for remote patient monitoring, appropriate security measures should be put in place to protect the security and confidentiality of patient data.

Thus, the objective of this workshop is to solicit papers that investigate secure eHealth/mHealth systems using state-of-the-art security techniques. Papers regarding the modeling, design, implementation, deployment and management of secure eHealth/mHealth technologies, system architectures and protocols are welcome.

Topics

Accepted papers will be published in the IEEE IWCMC 2021 proceedings and will be submitted to the IEEE digital library (IEEE Xplore). Authors are welcome to submit papers with topics that include, but are not limited to the following topics with focus on security/privacy prevailing mechanisms:

- Body Area Networks (BANs), Wireless BANs (WBANs)
- Biosensors and sensor networks
- Sensor-based mHealth applications
- Remote patient monitoring
- Ambient Assisted living (AAL)
- Remote diagnosis
- Biomedical data processing
- Healthcare modeling and simulation
- E-Health records management
- Securing E-Health records
- Cloud security for health related data
- Blockchain for healthcare
- Internet of things (IoT) applications for healthcare
- Securing m-health IoT data
- Privacy and security in healthcare
- mHealth and remote patient monitoring in remote and rural areas
- Delay tolerant mHealth networks
- Tactile internet for health applications
- Techniques for remote secure robotic surgery
- Ultra-reliability low latency communications (URLLC) and mHealth
- 5G and beyond connectivity for mHealth
- Edge computing for health applications
- Cloud computing for health application
- Advanced Medical Visualization Techniques
- Virtual reality (VR) and augmented reality (AR) for healthcare
- Machine learning techniques for secure health applications
- Game theoretic approaches to security in eHealth applications

Important Dates

Submission:	January 10, 2021
Acceptance notification:	March 30, 2021
Camera-ready paper submissions:	April 30, 2021

Submission Guidelines

Prospective authors are invited to submit original technical papers—up to 6 pages of length, using the EDAS link: https://edas.info/newPaper.php?c=27588 for possible publication in the IWCMC 2021 Conference Proceedings, which will be submitted to the IEEEXplore. Selected papers will further considered for possible publication in three special issues in the following Journals. For more information, visit: http://iwcmc.org/2021/

1. Wiley Journal of Wireless Communications and Mobile Computing (WCMC)
   https://www.hindawi.com/journals/wcmc/

2. The International Journal of Sensor Networks (IJSNet) http://www.inderscience.com/browse/index.php?journalCODE=ijsnet
3. The International Journal of Autonomous and Adaptive Communications Systems (IJAACS) http://www.inderscience.com/jhome.php?jcode=ijaacs
4. KSII Transactions on Internet and Information Systems: http://www.itiis.org/
5. Peer-to-Peer Networking & Applications: http://www.springer.com/engineering/signals/journal/12083

TPC Members (TBD)