IEEE Transactions on Industrial Informatics

CALL FOR PAPERS

for Special Section on

Security, Privacy and Trust Analysis and Service Management for Intelligent Internet of Things Healthcare

Theme: To build sustainable ecosystem, healthcare reinforced by the Internet of Things (IoT-Health) is a sector that makes a very useful contribution to society. With the aging of the world's population, the ability to monitor and protect people at home reduces costs and increases the quality of life. IoT healthcare has become a market with great potential and giants IT companies such as IBM, Microsoft, and GE Healthcare develop products for specialized medical applications. Using IoT-Health for data collection and workflow automation is a great way to reduce waste, cots, and minimize human errors. However, the security of healthcare information is a major concern, and cybersecurity has become one of the significant threats for healthcare providers as well as governments to achieve sustainable city milestones. IT professionals must continually resolve health data security issues to help patients and the damage that healthcare security breaches can have on their lives.

The motive of this special issue is to focus on the recent advances in emerging technologies and how we leverage the strength of these technologies under the IoT-Health framework to provide a secure and robust network platform. The evolution of technological safeguards using emerging technologies such as Blockchain and Artificial Intelligence (AI) to prevent theft of private and protected information continues to be a multifaceted approach. Advocates of integrating these technologies into the healthcare industry often point to the app's ability to provide multiple checks and balances as a key benefit to improving the security of private health records. The development of a learning model integrating with Blockchain makes it possible to store encrypted data in a reliable and distributed ledger. Both of these techniques have recently been a surge in interest. The integration of these two techniques can further enhance the performance of smart city networks. The people and things are connected with anything and anyone, anytime, anywhere, using network/service. IoT-Health ensures faster decisions, smart services, and good utilization of resources, which can take all-round development and well-being for its citizens. However, the success of any technology to a large extent depends on its devices/nodes/link security vulnerabilities, threats, and attacks. Through this special issue, the different security issues in IoT-Health will be covered.

This special issue aims at how these emerging techniques can lead to an efficient, user-friendly IoT-Health ecosystem. It also focuses on various technologies and concerns regarding energy aware and secure IoT and how it can reduce energy consumption. The objective of this issue is to bring together the latest industrial and academic progress, research, and development efforts within the rapidly maturing IoT-Health ecosystem.

This special section will focus on (but not limited to) the following topics:

- Architectures, protocols, or applications for securing IoT enabled Healthcare
- Privacy preservation in IoT enabled Healthcare
- Risk / Threat and Vulnerability analysis in IoT enabled Healthcare
- Energy aware secure communications for IoT enabled Healthcare
- Intrusion detection Prevention for IoT enabled Healthcare
- Federated learning-based data analytics in IoT-Health
- Homomorphic/Lightweight security protocols and architectures for the IoT-Health
- Privacy enhancing and anonymization techniques in IoT-Health
- SDN and NFV for IoT-Health
- Blockchain and AI enabled solution for IoT-Health

Manuscript Preparation and Submission

Follow the guidelines in “Information for Authors” in the IEEE Transaction on Industrial Informatics http://www.ieee-ies.org/pubs/transactions-on-industrial-informatics . Please submit your manuscript in electronic form through Manuscript Central web site: https://mc.manuscriptcentral.com/tii . On the submitting page #1 in popup menu of manuscript type, select: SS on **Security, Privacy and Trust Analysis and Service Management for Intelligent Internet of Things Healthcare**

Submissions to this Special Section must represent original material that has been neither submitted to, nor published in, any other journal. Regular manuscript length is 8 pages.

Note: The recommended papers for the section are subject to final approval by the Editor-in-Chief. Some papers may be published outside the special section, at the EIC discretion.

Timetable:	Deadline for manuscript submissions	**February 25, 2021**
	Expected publication date (tentative)	October 2021

Guest Editors:

- Dr. Pradip Kumar Sharma, University of Aberdeen, UK pradip.sharma@abdn.ac.uk
- Dr. Uttam Ghosh, Vanderbilt University, USA uttam.ghosh@vanderbilt.edu
- Dr. Lin Cai, University of Victoria, Canada cai@ece.uvic.ca
- Dr. Jianping He, Shanghai Jiao Tong University,China jphe@sjtu.edu.cn

Editor-in-Chief: Prof. Dr.-Ing. Ren C. Luo tii@ira.ee.ntu.edu.tw

http://www.ieee-ies.org/pubs/transactions-on-industrial-informatics