IEEE Transactions on Industrial Informatics

CALL FOR PAPERS

for Special Section on

Cybersecurity Intelligence in the Healthcare System

Theme: The involvement of recent technologies in the healthcare system can improve the treatment experience and quality of human life. The technologies include many number of smart devices, mobile Health (mHealth), networks, servers, patient's health applications, patient records, and decision support system to make the system efficient and lead to a high quality of care. But, it parallelly also increases the cybersecurity risk and challenges in health care. The healthcare data plays an essential role in patient treatment, diagnosis, and decision purpose. One small change or breach of the patient data could be played the life of the patient. Thus, the attacker always tries to get sensitive healthcare data. Cybersecurity vulnerability is continuously increasing due to the Internet-based service and malicious users. This may increase the chances of threats and attacks in the healthcare system, which could hamper the integrity of systems and lead to privacy issues. The situation becomes more vulnerable when healthcare transactions are done outside the domain.

Distributed denial of service (DDoS), insider attack, and Malware, including ransomware attacks, disturb patient care service. These attacks can lead newest Cybersecurity challenges like Phishing, Cloud threats, Software vulnerabilities, BYOD policies, network penetration, and side-channel. The cybersecurity solution includes protecting of digital healthcare information from different network vulnerabilities. It provides a set of standards security solution and protocols which will ensure that the security of healthcare network. Such security solution includes multifactor authentication, Intrusion detection and prevention system, firewalls, Digital forensics, anti-virus software, access control, vulnerability identification techniques, Backup and restoration of data, encryption, and many more. These provided cybersecurity solution's main aim is to overcome healthcare security flaws. But, these are not sufficient due to the size and diverse nature of the healthcare system. It is essential to improve cybersecurity techniques to make a good trade-off between technology and security practices. Several recent researches are also shown the limitation and loopholes present in such solutions. Thus, there is a need for revolutionary approaches and advanced field support for the healthcare system that improves the system quality and achieves the desired level of privacy.

This special section is intended to elaborate on the recent cybersecurity trends and challenges present in the healthcare system. The current state of security strategies (solutions) and applications are also included. In this special section, various researchers and academicians from multiple backgrounds can submit/demonstrate their novel and unpublished work and address research challenges present in the healthcare system.

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

The current state of cybersecurity for health care; Understanding cybersecurity threats in healthcare; Advances in critical healthcare infrastructure security; Cybersecurity solutions for the healthcare system; Case studies for improving cybersecurity; Cyberattack metrics and assessment; Cyber risk and threat management; Fog /cloud/edge computing-based healthcare solutions; Strategies for earlier analysis and prediction of cybersecurity threats in Healthcare; Mobile healthcare; Healthcare data protection via physical access and control strategy ; Healthcare system protection via trust and agreement between stakeholders; Healthcare physical security; Security awareness policies and procedures; Cybersecurity culture for healthcare; Healthcare applications for addressing cybersecurity practices

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 **Cybersecurity Intelligence in the Healthcare System**

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 15, 2022**
	Expected publication date (tentative)	September 2022

Guest Editors:

Dr. Ashish Singh, Kalinga Institute of Industrial Technology (KIIT), India ashish.singhfcs@kiit.ac.in

Dr. Abhinav Kumar, Siksha 'O' Anusandhan University, India abhinavkumar@soa.ac.in

Dr. Zahid Akhtar, State University of New York Polytechnic Institute, USA akhtarz@sunypoly.edu

Dr. Muhammad Khurram Khan, King Saud University, Kingdom of Saudi Arabia mkhurram@ksu.edu.sa

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