Editorial Preface

Internet of Medical Things (IoMT) Standards and Security Challenges

Jinan Fiaidhi, Thunder Bay, Lakehead University, Canada
Sabah Mohammed, Thunder Bay, Lakehead University, Canada

We are delighted to continue our efforts at IJEACH to create a new forum for the exchange of information and publishing excellent research works of scholars on all aspects of the emerging trends in the digitization of healthcare. One of the hottest technology trends in healthcare is the IoT (Internet of Things). Industries across the board are seeing disruption by smart sensors, smart applications, smart devices, wearables and smart connected healthcare networks. The Internet of Medical Things (IoMT), for example, can help to monitor, inform and notify not only care-givers, but provide patients and providers with actual data to identify clinical issues before they become critical or to allow for earlier invention. However, the accelerated adoption of IoMT means medical device development must be robust against the security vulnerabilities affecting medical devices, a landscape of uncertain liability, new standards and emerging policies and regulations. Consequently, medical device manufacturers should keep abreast of current minimum security standards to prevent cyberattacks like the "WannaCry" ransomware attack in May 2017 (Rodionova). These security vulnerabilities highlight the importance of developing standards, using best practices for compliance. The existing broad, ambiguous standards regulating the IoMT invite litigation, and precise legal boundaries have yet to be drawn. In an effort to regulate the IoMT and ensure public safety, the US Food and Drug Administration (FDA) has issued premarket and postmarket cybersecurity guidance in October 2018, providing nonbinding recommendations to device manufacturers (Schwartz, 2018). However, many questions remain to be answered regarding IoMT standards and security such as (Segura et al., 2018):

- What is the reasonable standard of care in creating a secure IoMT device?
- What constitutes a design defect or failure to warn?
- Are security vulnerabilities considered a design defect?
- For how long must device manufacturers provide security monitoring and software updates after selling a product?
- Does user failure to download security updates act as a superseding cause or a failure to mitigate in cases of liability for defective software?
- Will these security vulnerabilities mean an uptick in shareholder derivative actions?

Craig Badrick estimates that of every 1,000 IoT devices in use, 164 are subject to attacks. As hospitals discover more and more applications for the IoMT, many are beginning to add devices that may actually be putting their operations—and even patient lives—at risk (Badrick, 2019). In fact, the healthcare industry is rapidly moving to a completely digitized environment, and, as a result, devices have been introduced to the hospital ecosystem and bedside workflows to help extend and streamline care throughout the hospital as well as many devices are incorporated to monitor remotely patients at home or work. While using robust medical devices and mobile smartphones have allowed clinicians to become more efficient and mobile with patient care. Unfortunately, this new technology has also opened the door to increased risk and new potential points of exposure for healthcare IT infrastructures. Without enforcing rigorous standards for safely using these medical devices within

the new IoMT platform, then each network-connected medical device within a health provider's ecosystem will opens up the possibility for patient health information exposure as well as the potential for other unauthorized use of critical systems and applications. This issue contains some papers that addresses this issue and we are inviting other authors to contribute to solving the challenging issue of IoMT standards and Security.

IN THIS ISSUE

The first paper in this issue is entitled "A Rule-Based Model for Compliance of Medical Devices Applied to the European Market" by Sofia Almpani, Petros Stefaneas, Theodoros Mitsikas and Panayiotis Frangos from the National Technical University of Athens, Greece and Harold Boley from the Faculty of Computer Science, University of New Brunswick, Canada who has demonstrated a formalization of medical devices regulation as part of a logical KB leading to a computational decision model in PSOA RuleML. This executable formalization was tested by implementing queries on PSOATransRun engine and evaluating the answers retrieved. The resulting KB is capable of answering queries regarding the classification and marketability of medical devices aiming at compliance with the Regulation (EU) 2017/745. This research has created an initial opportunity for decision support using this rule formalization via formal query, analysis, and proof, as well as permitting translation to other formalisms. There are expressive features of Logic Programs, frequently used in practical rule-based applications, which are yet inexpressible in PSOA, and subject of future development, such as Naf and/or classical negation. For medical device companies, there is a continuous necessity to balance compliance, quality, and agility, thus there is a need for automation of procedures to streamline the necessary time to obtain pre-market approval and allocate medical devices product to market. This prototype is publicly accessible, allowing anyone to try the system and view the PSOA code source (see Appendix 1). In addition to representing 2017/745 precisely enough to determine whether the necessary requirements within the scope of the CE-registration procedure would be compliant with law, this development aimed to a formalization that could be verifiable by lawyers, medical experts, and programmers alike. For this reason, it was tried as much as possible to formalize the law so that the PSOA presentation can be read and understood section by section. The rules developed in this work are independent, autonomous pieces of knowledge, enabling future amendments/amelioration of the present regulation (e.g. enrichment of products with UDIs for medical devices as well as post- marketability and clinical evaluation requirements) or extension of the current work, acting as a groundwork for other countries' regulations (e.g., USA, India, Japan, etc.). To support review and audit, this approach also helps make feasible to combine the Medical Devices formalization with supplementary formalizations of relevant policies adopted by regulated companies (e.g., ISO 13485 for Medical devices, ISO TC299 for Robots and Robotic Devices - especially for medical and/or wearable robots, General Data Protection Regulation, etc.).

The second paper in this issue is entitled "A Fuzzy Markup Language-Based Approach for a Quality of Location Inference as An Environmental Health Awareness" by Majed Alowaidi, Mohammad Al-Ja'afreh, Ali Karime and Abdulmotaleb El Saddik all from University of Ottawa, Canada. This article presented a fuzzy inference solution to provide a quality of location (QoL) for medical devices as an awareness notification for people's health as day-to-day environment status in terms of air and noise pollution. The authors used a fuzzy markup language (FML) approach and the VisualFML tool as the platform to model the fuzzy inference system (FIS). FML was adopted because of its independence of platforms, in other words it can be used in several machines. From the FIS results observation, the time of the captured sensory data is an important aspect in defining quality of location feedback in addition to the sensory set place FIS plays a key factor to reduce any ambiguity in the values of raw data that might happen when inferencing a change of people's environments statuses. The article's aim is to provide status notifications about locations' environments, so it can infer broad people's surroundings changes based on converting raw sensory data in a much meaningful

notification. Also, the aim is to show the importance of including weekday's timeframes in analyzing IoMT sensory data in perspective of indoor and outdoor locations.

The third paper in this issue is entitled "Mitigation of linear accelerations and shear forces during drop head simulated falls" by Stephen Carlson, Carlos Zerpa, Eryk Przysucha and Paolo Sanzo, all from the School of Kinesiology, Lakehead University, Canada. The authors argues that despite helmet technological improvements used in variety of sports like Hockey, injuries to the head and brain continue to occur. Researchers believe that training hockey players to develop stiffer necks may help mitigate accelerations induced to the head during impact. Researchers also believe that understanding helmet performance across different impact locations and angles during head collisions helps inform helmet manufacturers in the development of testing protocols for brain injury prevention. Based on these beliefs and concerns, this article examined the relationship between neck surrogate compliance and neck strength for angles of flexion, extension and lateral flexion during static testing. The study also examined the dynamic interaction of neck compliance, helmet location, and angle of impact in mitigating linear acceleration and shear forces. The results of this study highlight the need to develop new helmet testing protocols and simulations studies to better assess the risk of concussion on athletes due to a fall in the sport of ice hockey. These testing protocols need to include not only measures of linear and rotational accelerations but also measures of shear forces to better guide helmet designers in the development of outer shell material, liner structures and helmet geometry to mitigate risk of concussions.

The fourth paper in this issue is entitled "On the Separation of Normal and Abnormal Stem Cell-Derived Cardiomyocytes' Calcium Transient Signals" by Martti Juhola, Henry Joutsijoki, Kirsi Varpa, Kirsi Penttinen and Katriina Aalto-Setälä all from Tampere University, Finland. In this paper the authors attempt to understand the microscopic dynamics of the beating heart using the Calcium imaging of cardiomyocytes as a method for monitoring calcium cycling activity in vitro. Typically, the use of such imaging offers a promising platform for studying the pathophysiology of various disorders and drug responses in human cells. The classification of the entire calcium transient signals was performed with two different approaches: first the correct reference class labels of the transient signals were given by the biotechnology expert and, second, their correct class labels were determined based on the results produced by the peak recognition and classification. On one hand, we might assume that a human assessor is better at solving complicated classification tasks on the basis of extensive experience. On the other hand, we might also see the systematic approach of the computation as better, since the decisions of any human expert include slight variation over time. Overall, for the sake of these reasons, it is not guaranteed that the former approach is always the better approach. In any case, special software—in other words, efficient algorithms for the present classification task—will be needed to develop techniques for the analysis of massive numbers of iPSC-derived cardiomyocytes in medical laboratories in the future. In the present research, the authors have extended 56% of the data set of calcium transient signals, added three new peak variables to our computation, ran our tests in more versatile ways, and obtained around 5% better classification accuracies compared to the authors previous tests. In general, the results are promising and enable good opportunities to continue developing these classification methods and also to extend them to experiments with iPSC-derived cardiomyocytes exposed to different drugs. The classification method will be required to analyze in-depth cardiomyocyte functionality that has been altered by different disorders, and will provide more information regarding the calcium cycling phenotype in these cells.

Sabah Mohammed
Jinan Fiaidhi
Editors-in-Chief
IJEACH

ACKNOWLEDGMENT

The EiCs and the ERB team would like to thank IGI Global for the kind support all the way.

REFERENCES

Badrick, C. (2019, January 4). Best Practices in IoMT Security. *Turn Key Technologies*. Retrieved from http://www.turn-keytechnologies.com/blog/network-solutions/best-practices-iomt-security

Rodionova, Z. (2016, Thursday 21). Healthcare is now top industry for cyberattacks. *The Independent*. Retrieved from https://www.independent.co.uk/news/business/news/healthcare-is-now-top-industry-for-cyberattacks-says-ibm-a6994526.html

Schwartz, S. (2018, October 18). Premarket Submissions for Management of Cybersecurity in Medical Devices, Draft Guidance for Industry and Staff. *Food and Drug Administration (FDA)*. Retrieved from https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf

Segura, M., Butler, C. M., Tabibkhoei, F., & Smith, R. (2018, January 3). The Internet Of Medical Things Raises Novel Compliance Challenges, Medical Devices Online. *Med Device Online*. Retrieved from https://www.meddeviceonline.com/doc/the-internet-of-medical-things-raises-novel-compliance-challenges-0001