International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Review Article)

Check for updates

Individual mobile data in institutional EHRs: The emerging role of information from the Internet of Medical Things (IoMT)

Shumiya Alam [1], Tanmoy Das [2], Md Abu Rayhan [2], Akash Das [2], Md Riaz Ahmad Shuvo [2, *] and Asad-Uz-Zaman [1]

[1] *Department of Electrical and Electronics Engineering, Bangladesh University of Engineering and Technology, West Palashi Campus, Dhaka 1205, Bangladesh.*

[2] *Department of Electrical and Electronics Engineering, Canadian University of Bangladesh, Merul Badda, Dhaka 1212, Bangladesh.*

International Journal of Science and Research Archive, 2023, 10(01), 100–105

Publication history: Received on 26 July 2023; revised on 03 September 2023; accepted on 06 September 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.10.1.0715

Abstract

The use of wearable sensors is revolutionizing the monitoring of patients'vital signs and diseases. In the domains of healthcare and eHealth, the Internet of Things (IoT) and its subset, the Internet of Medical Things (IoMT), along with embedded devices, offer potential for new opportunities and effective solutions. Particularly, their application within the context of Smart Homes exhibits promise. In this regard, the plan to integrate the formal Electronic Health Record (EHR) that is a component of Croatia's Central Health Information System with personal health data collected via wireless sensors, such as personal trackers, has enormous potential because the implementation of this approach would yield enhanced decision-making processes and advancements in healthcare that are tailored to individual needs.

Keywords: E-Health; Wearable sensors; IoT; IoMT; EHRs

1. Introduction

One of the most useful applications of technology based on wearable wire-less sensors is health monitoring. Demand for portable fitness trackers is rising, which is driving the market. Consumers' newfound concern for their own health is to blame. When it comes to tracking your health and fitness, wearable sensors play a vital role. A fitness tracker is a wearable device that records data about a variety of physical fitness-related activities, including steps taken, distance traveled, time in bed, heart rate, and more. The user's smartphone can communicate with these gadgets wirelessly. Based on a raised compound growth rate (CAGR) of 22.6% annually, the research [1] estimates that the worldwide Fitness Bands market will rise by 78 million euros between 2020 and 2027. Smartwatches powered by the Internet of Things (IoT) are also on the rise since they can vastly improve users' quality of life and can function both independently and in tandem with other IoT-enabled gadgets. Every wristwatch includes a fitness tracker, so they can all do things like keep tabs on your vitals. The report [2] estimates that the global smartwatch market will rise from its 2018 volume of 43.87 million shipments to 108.91 million by 2024, growing at a CAGR of 14.5% during the forecast period of 2019–2024. This demonstrates the great potential for improving patient care and making healthcare more individualized that exists in the use of personal wireless data in a more traditional clinical setting. However, there are a number of obstacles that must be overcome by such a system because of the sensitive nature of the data it processes.

Chapter I of this article provides a comprehensive overview of the current options available for managing private medical data acquired through wireless sensors. Chapter II presents a comprehensive examination of the difficulties and circumstances related to the incorporation of the aforementioned data into a structured healthcare system. In

* Corresponding author: Riaz Ahmad Shuvo

Chapter III, we conduct a comprehensive examination of the current advancements in Electronic Health Records (EHR) and propose a framework for the prospective integration of EHR into Croatia's official Central Health Information System. The report concludes by presenting a series of research recommendations for future investigations.

2. Challenges and issues in research works

In order to utilize data within a formal clinical context, it is imperative to acquire data that is precise, reliable, and devoid of errors [3]. creates and evaluates a Quality of Experience (QoE) model for using fitness trackers and smartwatches from two separate perspectives: (a) a Quality of Data (QoD) metric, which is based on the precision and correctness of the data (b) the information's quality (QoI), which is assessed after data collection. Twenty people participated in the study, which used five distinct kinds of wearable technology. Nevertheless, research suggests that [4] there could potentially exist a discrepancy of up to 26% between the recorded distance covered and the step count reported by various wearable devices worn concurrently by an individual. On various devices, there was a minimal link between the number of calories expended and the number of steps taken. This demonstrates how the computations are very dependent on the gadget itself and the manufacturer's secret methodology. Due to these inherent limitations, the utilization of metrics as an accurate prognosticator of health outcomes poses a significant challenge, rendering their application in a professional medical setting unfeasible without the implementation of a rigorous data cleansing protocol. To increase the accuracy of both step and energy expenditure (EE) estimation, regression-based models are compared and reviewed in the paper [5]. Seven fitness trackers were utilized to collect data, while two other devices served as references. In three separate incarnations, twenty young adults wore every device at once. All of the devices' EE measurements and five of the devices' step measurements improved as a consequence of the creation of regression models for each of the devices using reference data. This study examines [6] various data-driven methodologies for the purpose of cleansing eHealth sensor data obtained from the Internet of Medical Things (IoMT) devices. The study further proposes the optimization of these methodologies to enhance the accuracy of the collected data, with the ultimate goal of integrating it into an official Electronic Health Record (EHR) system.

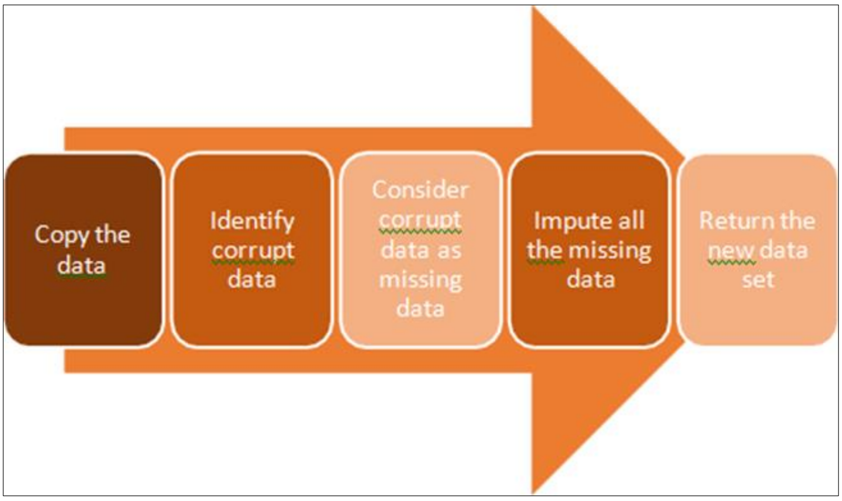

Figure 1 The process of data cleaning

The next significant problem is organizing and reformatting the data collected across various devices into a certain, predetermined format for simple integration into the record of health electronically. This also implies that all data and information transmission must carefully adhere to the most recent standards and laws [7]. The following chapter will provide more detail on this. The fourth key problem cited is privacy and security because health-related data is so sensitive. The establishment of a secure protocol for the incorporation of data into an official healthcare system, such as its integration into Electronic Health Records (EHR), is of paramount importance. Two communication flaws between Fitbit [8], a fitness tracker, and the Web server that hosts it have been identified by article [9]: (a) cleartext login information, in which the user password is sent to the server in cleartext and stored in log files, and (b) cleartext HTTP data processing, in which the data is also sent in cleartext as plain HTTP instructions.

Both situations lack data protection and authentication. Additionally, article [10] offers a thorough security review of some of the most well-liked fitness tracking technologies available today. The primary focus of this study is to examine deceptive user configurations that aim to introduce false information into cloud-based platforms, consequently leading to inaccurate data analytics. The server was compromised through the utilization of a Man-In-The-Middle (MITM) attack, enabling the successful upload of a counterfeit FIT file containing falsified data indicating the completion of 80 million steps. The utilization of the Advanced Encryption Standard (AES) technology is employed in the fitness application model proposed by [11] to ensure the encryption and decryption of data, thereby mitigating the risk of data tampering. The database is used to perform encryption and decryption operations, which are then stored on the server.

3. Proposed model

All of the significant difficulties that would arise from incorporating data from personal trackers into a formal EHR must be addressed in the model. To ensure that data is accurate and error-free, a data cleaning module must be included. This module would employ either neural networks or regression models as well as optimized data-driven data-cleaning procedures. In Figure 1, the data cleaning procedure is displayed.

The prior security incidents indicated that there are several hardware-related flaws. Since then, several firms have created secure hardware and software. These IoMT devices often broadcast their unique identification in addition to the values measured (such as temperature or acceleration), which is essential for classifying, managing, and preserving the data [12]. Figure 2's end-to-end encryption (E2EE) with a device-specific key prevents data manipulation by MITM attacks. This guarantees the data's integrity and confidentiality as it is sent from the device to the server.

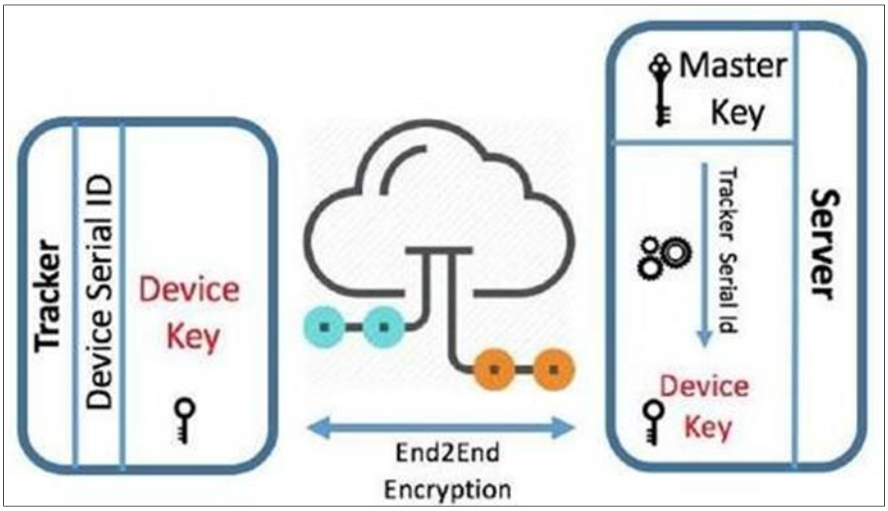

Figure 2 Encryption block

Additionally, under this paradigm, the module that guarantees that the data being transferred complies with current standards and regulations and the data cleaning module each covers a portion of security. Currently, the Health Level 7 Fast Healthcare Interoperability Resources (HL7 FHIR) specification is evolving as the next-generation standards framework for the transfer of EHR data [13].. FHIR is an HL7-established standard for healthcare data transmission that is used for electronic healthcare data sharing.

A Resource is its fundamental building component, and the composition encompasses a collection of metadata, standardized data, and a segment that is easily comprehensible to humans (Figure 3). A solitary device has the potential to produce in excess of 4 million sensor data points on a daily basis, resulting in the creation of significant data files that necessitate analysis in order to verify the precision of the data inputted into the patient's electronic health record. The amalgamation of unprocessed health data, its subsequent examination, and its conversion into HL7 FHIR data have the potential to generate medically significant information that is appropriate for incorporation into an authorized Electronic Health Record (EHR).

Figure 3 Resource from – HL7 FHIR

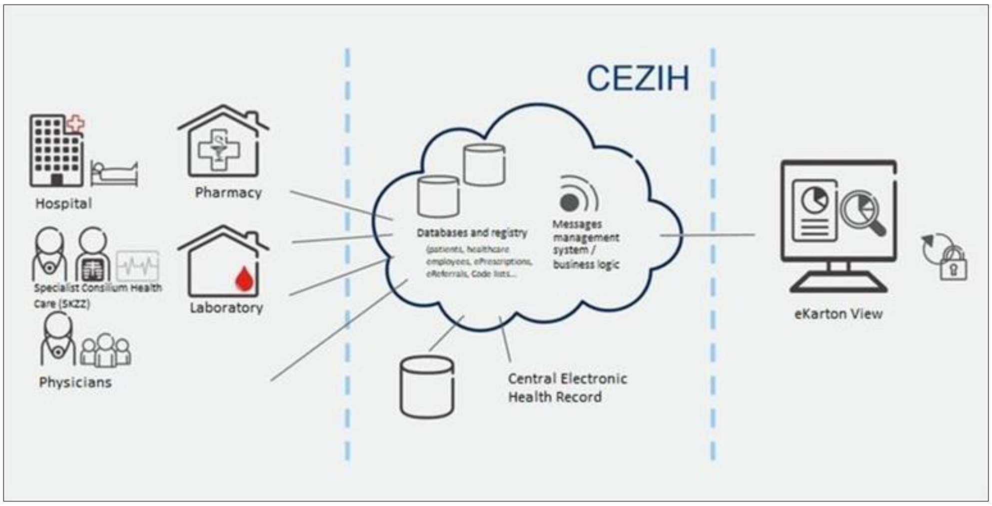

Figure 4 CEZIH – Central Health Information System

Figure 4 displays the current Central Health Information System (CEZIH) for Croatia. It enables smooth communication between the patient and healthcare professionals (such as chemists, doctors, lab technicians, and experts). Authorized users can see a patient's medical records using the electronic health record, or e Karton, in the system at hand. The

Smart Card and PIN number of the physician would be used to access the system. Patients must have the option to authorize specific doctors as well as outright reject the system. In the event that the patient is unable to provide consent and the doctor determines that access is essential, the technology would also offer emergency access, often known as the ”break the glass” option. The objective is to include IoMT and wearable sensor technologies that gather personal health information into the e Karton as a component of the main health information network. During this procedure, the most common and important forms of healthcare data are translated, standardized, and visualized. After that, they are connected with the EHR web application that already exists to build the core health information system.

4. Conclusion

There is tremendous promise for enhancing personalized healthcare by utilizing the data gathered by personal wireless trackers. This can be attributed, at least in part, to the increasing prevalence of trackers such as fitness bands and smartwatches, which are widely adopted due to their affordability, practicality, and inconspicuousness. Second, as they continuously gather data, they may provide doctors with a deeper and more thorough understanding of the patients' daily states and circumstances, enabling them to make wiser and more informed healthcare decisions. The incorporation of personal health information into a formal medical information system, however, faces a number of difficulties. A valuable and very delicate resource is medical data. Problems with data quality might arise at many stages, for as when collecting sensor data or processing it. Therefore, the process of verifying the syntax and validating the semantics of medical data is a crucial step in mitigating health and security risks associated with inaccurate data. Additionally, all communication must follow rules and standards and guarantee data structure definition (DSD). If these issues are to be resolved, Electronic Health Records (EHRs) that can hold useful, clinically applicable, processed data collected by sensors will be necessary. This will lead to the implementation of personalized healthcare services based on established standards, thereby bringing us closer to achieving uninterrupted access to care. The primary objective of this study is to enhance the current Central Health Information System in Croatia, while also exploring its potential relevance to other established healthcare systems. Each of the primary issues mentioned will hopefully be addressed and thoroughly investigated in subsequent work.

Compliance with ethical standards

Acknowledgments

The ”IoT Lab” of the Canadian University of Bangladesh (CUB) and the ”IICT Lab” of Bangladesh University of Engineering and Technology (BUET) provided all sorts of support for this research work.

Disclosure of conflict of interest

There are no conflicts of interest to declare.

References

[1] D. Pal, A. Tassanaviboon, C. Arpnikanondt, B. Papasratorn, Quality of experience of smart-wearables: From fitness-bands to smartwatches, IEEE Consumer Electronics Magazine 9 (2019) 49–53.

[2] L. Ciabattoni, F. Ferracuti, S. Longhi, L. Pepa, L. Romeo, F. Verdini, Real-time mental stress detection based on smartwatch, in: 2017 IEEE International Conference on Consumer Electronics (ICCE), IEEE, 2017, pp. 110–111.

[3] D. Pal, A. Tassanaviboon, C. Arpnikanondt, B. Papasratorn, Quality of experience of smart-wearables: From fitness-bands to smartwatches, IEEE Consumer Electronics Magazine 9 (2019) 49–53.

[4] C. G. Bender, J. C. Hoffstot, B. T. Combs, S. Hooshangi, J. Cappos, Measuring the fitness of fitness trackers, in: 2017 IEEE Sensors Appli- cations Symposium (SAS), IEEE, 2017, pp. 1–6.

[5] I. Perova, P. Zhernova, O. Datsok, Y. Bodyanskiy, O. Velychko, Recog- nition of human primitive motions for the fitness trackers, in: Lec- ture Notes in Computational Intelligence and Decision Making: Pro- ceedings of the XV International Scientific Conference "Intellectual Systems of Decision Making and Problems of Computational Intelli- gence"(ISDMCI'2019), Ukraine, May 21–25, 2019 15, Springer, 2020, pp. 364–376.

[6] V. Andalibi, H. Honko, F. Christophe, J. Viik, Data correction for seven activity trackers based on regression models, in: 2015 37th Annual Inter- national Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), IEEE, 2015, pp. 1592–1595.

[7] A. Koren, M. Jurˇcevi´c, D. Huljeni´c, Requirements and challenges in integration of aggregated personal health data for inclusion into formal electronic health records (ehr), in: 2019 2nd International Colloquium on Smart Grid Metrology (SMAGRIMET), IEEE, 2019, pp. 1–5.

[8] L. M. Feehan, J. Geldman, E. C. Sayre, C. Park, A. M. Ezzat, J. Y. Yoo, C. B. Hamilton, L. C. Li, Accuracy of fitbit devices: systematic review and narrative syntheses of quantitative data, JMIR mHealth and uHealth 6 (2018) e10527.

[9] M. Rahman, B. Carbunar, M. Banik, Fit and vulnerable: Attacks and defenses for a health monitoring device, arXiv preprint arXiv:1304.5672 (2013).

[10] H. Fereidooni, T. Frassetto, M. Miettinen, A.-R. Sadeghi, M. Conti, Fit- ness trackers: fit for health but unfit for security and privacy, in: 2017 IEEE/ACM International Conference on Connected Health: Applica- tions, Systems and Engineering Technologies (CHASE), IEEE, 2017, pp. 19–24.

[11] A. R. Shekar, Preventing data manipulation and enhancing the security of data in fitness mobile application, in: 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT), IEEE, 2019, pp. 740–745.

[12] W. Zhou, S. Piramuthu, Security/privacy of wearable fitness tracking iot devices, in: 2014 9th Iberian Conference on Information Systems and Technologies (CISTI), IEEE, 2014, pp. 1–5.

[13] R. Saripalle, C. Runyan, M. Russell, Using hl7 fhir to achieve interop- erability in patient health record, Journal of biomedical informatics 94