Chapter 12
Securing Digital Transformation in Healthcare Systems

Nazhatul Hafizah Kamarudin
https://orcid.org/0000-0002-6972-7967
Universiti Kebangsaan Malaysia, Malaysia

Mohammad Arif Ilyas
UCSI University, Malaysia

ABSTRACT

The Internet of Things (IoT) has experienced rapid growth, and as a result, the e-health system has established a robust infrastructure that enables the delivery of viable healthcare services over the network. Healthcare organizations recognize the importance of adopting the latest technologies to improve healthcare services and reduce operational costs. Integrating IoT into the healthcare system offers numerous benefits, including secure patient identification and efficient data collection. However, many existing e-health systems primarily focus on patient data acquisition and medical embedded components, paying little attention to crucial aspects like real-time monitoring and, most importantly, the security of the e-health system. This chapter strives to enable the smooth integration and sustained expansion of digital transformation within the e-health system by addressing the urgent need to strengthen security measures and improve accountability. Securing the extensive advancements in digital transformation within e-health is of utmost importance. To safeguard the security and accountability of digital transformation in the healthcare system, it is essential to develop multilevel authentication protocols alongside the implementation of deep learning techniques.

INTRODUCTION

With increasing numbers of people visiting the healthcare center, the need for remote healthcare monitoring system is highly needed to assist the situation. Therefore, advancements in electronics and biomedical applications have become growing attention recently since these areas contribute to e-health monitoring systems. Security challenges in e-health systems will lead to an e-health transformation and

with the development of IoT applications, e-health security systems need to be improved and upgraded. Acknowledging the current security problems with the digital transformation in the healthcare system and limited constraints faced by e-health system, this chapter will present a comprehensive security method solution in terms of the security authentication protocol and deep learning features in order to provide seamless and secure e-health while ensuring its practicality and efficiency. The proposed security method solution for e-health authentication is mainly to establish secure communication in the mobile e-health networking environment. Through this chapter, the authors aim to discuss the unique identity-based authentication and focus on the e-health authentication scheme. There has been significant research on the mobile e-health authentication system in order to enhance the efficacy and security of the e-health system. As demand for e-health applications has increased, a secure authentication protocol has become the main concern in e-health networking. Improvement in communication technology as well as sensor networking has assisted the development of e-health applications in order to provide effective healthcare services to people.

Considering the progressively advancing digitalization of healthcare systems and the mounting dependence on electronic health (e-health) applications, it is of utmost significance to prioritize the establishment of resilient security protocols. The reinforcement of the authentication process in e-health applications is fundamentally dependent on the pivotal function of image detection security. The authentication process for users operating within the healthcare industry is of paramount importance, primarily due to its ability to safeguard the confidentiality of patient information, facilitate secure entry to medical records, and restrict unlawful access to e-health systems. The range of visual indicators that can be utilized in the field of biometrics encompasses various physical attributes such as facial characteristics, retinal patterns, fingerprints, and other distinctive biometric markers. E-health authentication applications can achieve a robust and dependable approach for validating the identity of healthcare practitioners, patients, and authorized personnel endeavoring to obtain access to sensitive medical information by capitalizing on image detection methodologies.

The implementation of e-health in healthcare organizations offers various well-defined advantages, such as cost reduction, improvement in quality of care, efficient storage of data, and enhanced healthcare services. However, ensuring the security requirements of the e-health system remains a crucial factor. The process of implementing new technology in e-health is often intricate and time-consuming, yielding uncertain results. Throughout the years, extensive research has primarily focused on the implementation process of e-health, neglecting the analysis of outcomes and security requirements for the system. While e-health technology is mostly perceived as a means to enhance service efficiency and reduce errors, concerns regarding security and safety have diminished people's trust in e-health, thus impeding its utilization within healthcare organizations.

The advancements in mobile technology have revolutionized the use of mobile devices, such as smartphones and tablets, across various applications. The development of sensor networking connection and the Internet of Things (IoT), coupled with the widespread adoption of mobile phones, has made it increasingly viable to leverage mobile technology in medical applications. In recent times, individuals have witnessed the rapid growth of portable technology infrastructure and the emergence of diverse applications for mobile devices. These devices now serve a dual purpose, not only facilitating communication but also integrating with sensor networking, thereby simplifying and enhancing mobile e-health communication. The rapid progress in mobile technologies has paved the way for mobile e-health, also known as m-health, initiatives that have introduced personal health monitoring systems. These advancements have significantly improved the healthcare services provided by healthcare professionals.

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/securing-digital-transformation-in-healthcare-systems/325863

Related Content

Digital Technologies for a Quality School: A Didactical Experience Supported by Web Forum
Orlando De Pietro, Maurizio De Roseand Antonella Valenti (2014). *International Journal of Digital Literacy and Digital Competence (pp. 44-58).*
www.irma-international.org/article/digital-technologies-for-a-quality-school/119475

A Human Factors View of the Digital Divide
Kayenda T. Johnsonand Tonya L. Smith-Jackson (2013). *Digital Literacy: Concepts, Methodologies, Tools, and Applications (pp. 1510-1532).*
www.irma-international.org/chapter/human-factors-view-digital-divide/68521

New Media and Learning: Innovative Learning Technologies
Mustafa Serkan Abdusselamand Ebru Turan Guntepe (2018). *Promoting Global Competencies Through Media Literacy (pp. 41-63).*
www.irma-international.org/chapter/new-media-and-learning/192418

Multicultural and Global Children's Literature as Agents of Change
Roberta Robinson (2019). *Handbook of Research on Media Literacy Research and Applications Across Disciplines (pp. 90-100).*
www.irma-international.org/chapter/multicultural-and-global-childrens-literature-as-agents-of-change/232051

Exploring Teachers' Value Beliefs of Integrating Digital Literacy in K-12 Classrooms
Ayesha Sadaf (2019). *International Journal of Digital Literacy and Digital Competence (pp. 1-14).*
www.irma-international.org/article/exploring-teachers-value-beliefs-of-integrating-digital-literacy-in-k-12-classrooms/236670