Chapter 44
Cyber Security and Cyber Resilience for the Australian E-Health Records: A Blockchain Solution

Nagarajan Venkatachalam
https://orcid.org/0000-0002-5545-0549
Queensland University of Technology, Australia

Peadar O'Connor
Queensland University of Technology, Australia

Shailesh Palekar
Queensland University of Technology, Australia

ABSTRACT

Cybersecurity is a critical consideration for all users of electronic health records (EHR), particularly for patients. With the advent of Healthcare 4.0, which is based on the internet of things (IoT) and sensors, cyber resilience has become a key requirement in ensuring the protection of patient data across devices. Blockchain offers crypto-enforced security, data immutability, and smart contracts-based business logic features to all the users in the network. This study explores how blockchain can be a single digital option that can address both the cybersecurity and cyber resilience needs of EHR. The effective use lens is adopted to analyze how blockchain can be leveraged to meet cybersecurity needs while the novel use lens is adopted to analyze how blockchain can be leveraged to address cyber resilience needs originating from IoT. Based on the analysis, this study proposes two Hyperledger-based security models that contribute to individual privacy and information security needs.

DOI: 10.4018/978-1-6684-7132-6.ch044

INTRODUCTION

Electronic Health Records (EHRs) have been widely adopted for exchanging health information between stakeholders (hospitals, labs, insurance companies, government, and patients) in health systems (Del Fiol et al. 2020; Fragidis and Chatzoglou 2018). However, most EHRs still use the traditional client-server architecture for storing and exchanging data. Hence, with client-server-based controls, any errors in controlling data confidentiality, integrity, and accessibility (CIA) can result in significant loss of privacy and increase security threats to all stakeholders whereby the data become vulnerable to cyberattacks and other intruders (Tanwar et al. 2020). In Australia, the lack of adequate investments in cyber-security protocols and security solutions in health systems, use of old legacy computing systems by hospitals, lack of health-management training in cyber security, and the lack of mandatory reporting of cyberattacks are key reasons that make health systems vulnerable (Offner et al. 2020).

On the other hand, health care is transitioning toward Healthcare 4.0, which involves rapid and disruptive technological changes for aligning with Industry 4.0 initiatives. These include building cyber-physical systems and interoperability, and cyber-security solutions. Big data, cloud computing, and Internet of Things (IoT) are identified as the three digital pillars supporting Healthcare 4.0 transformations (Aceto et al. 2020) wherein the key objectives are (i) the continuous, simple, and bi-directional exchange of information; and (ii) accurate monitoring of health conditions and intake of medicines. Personalized health care, telepathology, telemedicine, disease monitoring, and assisted living are core areas of health and economic constraints addressed by the three pillars (Aceto et al. 2020). However, high-impact risks, such as (i) security concerns related to sensitive information and the digital devices storing the information; (ii) compromising privacy and ethical issues relating to ownership, dissemination, and sharing of information; and (iii) poor monitoring of information and system use, highlight serious concerns about the massive drive toward Healthcare 4.0 (Aceto et al. 2020). Based on the abovementioned dynamics, it is imperative that protecting the privacy and security of individual health records and health-related data, as well as securing the bi-directional exchange of information, are critical for realizing the benefits offered by EHR and Healthcare 4.0. For example, a recent survey on the security requirements for IoT-based healthcare systems identified cyber security and cyber resilience as key requirements that need to be addressed for developing and adopting new digital solutions (Nasiri et al. 2019). Based on the above, this study proposes a blockchain-enabled solution to address both requirements.

Blockchain offers an immutable audit trail of data and provides a consistent view for all network participants. The early success of blockchain, with the first disruptive innovation called Bitcoin (Nakamoto 2008), has evolved significantly toward frameworks such as Ethereum and Hyperledger. The power of these blockchain tools enables the enforcement of crypto security and reliable data exchanges between participants. Strategic management scholars refer to blockchain as a "foundational institutional technology" (Davidson et al. 2018), as it represents a digital-transaction ledger containing value exchanges between two peers. Blockchain also guarantees asset ownership for all individuals in the network through intelligent and trusted consensus protocols (Catalini 2017; Pilkington 2016) without the need for traditional centralized governance structures. Hence, this technology has been applied to improving information storage and distribution in supply chains, the finance sector, and other professional services, such as health care. In the health industry, ongoing studies have investigated how blockchain can be leveraged to address the needs of Healthcare 4.0 (Angraal et al. 2017; Griggs et al. 2018); (Gupta et al. 2019; Tanwar et al. 2020). These studies have highlighted the urgent need for developing robust and reliable digital infrastructures to address serious flaws and deficiencies in cyber-security and cyber-resilience