Chapter 8
A Digital Trust Architectural Model for Connected Medical Devices in the Healthcare Environment

Palanivel Kuppusamy
https://orcid.org/0000-0003-1313-9522
Pondicherry University, India

ABSTRACT

The healthcare sector has seen a digital revolution in smart devices, information systems, cloud services, and smart technology. The advancement of digital healthcare services has made treatment easier and more accessible. However, the healthcare sector is now the target of most cyberattacks that are impacted by data breaches. Healthcare data breaches are exposing a larger volume of records, and resulting in financial losses. Protection models are needed to analyze the pattern of healthcare data breaches and detect and forecast outcomes. This chapter aims to study the importance of cyberattacks and propose a digital trust architectural model for connected medical devices in the real-time healthcare environment.

INTRODUCTION

Emerging technologies can be integrated into all areas of business including the healthcare sector. The healthcare sector takes advantage of emerging technology that monitors patients' health using smart devices (e.g., smartwatches), blood pressure cuffs, and healthcare sensors. These devices and sensors provide alerts when patients have a healthcare issue, such as a heart attack, high blood pressure, or high sugar levels. These devices can collect and evaluate medical data, enabling healthcare professionals to act before a problem arises.

Access to proactive, and personalized healthcare can be gained through remote technologies. They assist individuals in taking control of their health outcomes, and they must enable self-care for everybody. In the future of healthcare, a direct channel to the doctor is provided by Web portals, telehealth, remote

DOI: 10.4018/979-8-3693-2109-6.ch008

health monitors, and provider chat sessions that operate around the clock. However, a few concerns may be the COVID-19 pandemic, the shortage of clinicians, and remote technology. Due to a shortage of clinicians, numerous healthcare professionals and the teams that support them are expected to have put in lengthy hours of work despite having fallen victim to infection, tragedy, and death.

Healthcare Data Security

The above concerns lead to challenges such as data transfer, a trove of data, data ownership, and business leverage in a cloud environment. Additionally, health data that is connected to banks, credit cards, and financial organizations can be stolen by criminals. For example, a Finnish company faced demands for money to keep their private notes private. It leads to data breach issues in healthcare systems. Data breaches (*Verizon, 2023*) in the healthcare sector are becoming common and can be brought on by a variety of events, such as malware that steals credentials, an insider who divulges patient information on purpose or by accident, or misplaced laptops or other devices. Customers are paying more attention to data protection as a result of the rising frequency of reported data breaches and penalties. Hence, data breaches must embed trust and security throughout the healthcare solution design and delivery pipeline.

Healthcare institutions can incorporate digital security methods for data breaches. Creative trust-building tools such as blockchain technology (Baltic of Estonia), creating data vaults (data stores or Pods), encryption, and data protection governance models such as GDPR and the CCPA must be used in healthcare solutions for ensuring data privacy.

But despite technology's advantages, only patients and doctors use it when they have faith in it (*Lisa Esch, 2021*). The integration of technologies into the healthcare business needs digital trust for doing business (*Charalambous et al., 2016*). The digital technologies have created new business and communication opportunities. At the same time, they have exposed individuals and organizations to unknown risks, such as data breaches, cyberattacks, and online fraud.

Challenges in the Connected Medical Devices

Data security can ensure digital trust (NTT whitepaper), requiring all healthcare organizations to focus on resilience and cybersecurity. A cybersecurity provider might open up the possibility of developing reliable, safe, and patient-focused products that both patients and healthcare professionals want. A reliable digital model that has been protected can pave the way for a smooth lifetime of care for both patients and providers.

With the quantity of linked medical devices in the healthcare setting increasing at an exponential rate, realizing the potential for safer and more accurate care presents a difficult task. *Marc Goodman (2019)* claimed that looking into an assault on linked medical devices is difficult. They might provide cybercriminals with more areas to attack. The coroner is used to discovering evidence of tampered medical devices on the body, yet it may not even be there, and alternatively, it could be on a remote computer server.

In addition, there are many other ways that threat actors can infiltrate the Internet of Medical Things (IoMT).

i. *Perimeter-based Challenges.* Complicated enterprise architectures with several security levels, including network division, security of applications, security in the cloud, and container security, are now possible thanks to developments in networking and cloud computing. Security and IT