Chapter 1
Advancing Lightweight Digital Trust Architectures in the Internet of Medical Things: A Multi-Dimensional Analysis

Sayani Das
https://orcid.org/0000-0003-0076-7466
Institute of Mass Communication, Film, and Television Studies, India

Archan Mitra
https://orcid.org/0000-0002-1419-3558
Presidency University, India

ABSTRACT

This research investigates the development of a lightweight digital trust architecture within the internet of medical things (IoMT). Employing a multi-faceted methodology, it commences with a systematic literature review, identifying gaps in IoMT security and digital trust frameworks. A theoretical framework, tailored for IoMT, is proposed, integrating resource-efficient cryptographic protocols, dynamic trust management, and scalable authentication mechanisms. The framework's practical applicability is examined through three case studies: a smart hospital system, remote patient monitoring, and IoMT in clinical trials, showcasing its efficacy in diverse IoMT applications. The study highlights the balance between security robustness and computational efficiency in IoMT, suggesting an iterative approach for adapting to evolving technologies and threats. This research contributes significantly to the understanding of digital trust in IoMT, providing a foundation for secure, efficient medical IoT solutions.

INTRODUCTION

The rapidly growing sector of the Internet of Medical Things (IoMT) has become a crucial element in the modern healthcare industry. This topic comprises a variety of networked medical equipment and

DOI: 10.4018/979-8-3693-2109-6.ch001

apps that are used to better patient outcomes, improve healthcare delivery, and increase the overall efficiency of medical services. The incorporation of Internet of Medical Things (IoMT) in the healthcare industry represents a significant change, characterised by enhanced connection, real-time data surveillance, and tailored patient care (Alsubaei, Abuhussein, & Shiva, 2017). With the ongoing development of the Internet of Medical Things (IoMT), it is crucial to focus on the crucial element of digital trust, especially when considering lightweight architecture solutions. This chapter explores the intricacies of creating and executing digital trust frameworks in the Internet of Medical Things (IoMT), with a focus on the two-fold goals of establishing strong security measures and optimising performance in IoMT devices and networks.

The importance of the Internet of Medical Things (IoMT) in contemporary healthcare cannot be exaggerated. IoMT devices encompass a variety of technologies, including wearable health monitors and sophisticated diagnostic systems. These devices play a crucial role in creating a healthcare environment that is highly networked and driven by data (Li, Da Xu, & Zhao, 2018). These technologies not only enhance the ability to monitor health in real-time but also allow for remote patient care, hence increasing the availability and accessibility of healthcare services. Nevertheless, the increasing number of IoMT devices has heightened the intricacy of data security and privacy issues. Stringent security measures are necessary to safeguard health data due to its sensitive nature, in order to prevent potential breaches and misuse (Mantas et al., 2020).

Digital trust in the context of the Internet of Medical Things (IoMT) pertains to the level of confidence individuals have in the security, integrity, and dependability of IoMT devices and the data they manage. The idea is complex and includes elements of cybersecurity, data privacy, and adherence to regulatory norms (Kumar & Mallick, 2020). Ensuring digital trust is of utmost importance, as it forms the foundation for the readiness of both healthcare practitioners and patients to embrace and depend on Internet of Medical Things (IoMT) technology. If there is not enough trust in the security and privacy of these systems, the potential of IoMT to transform healthcare could be greatly diminished.

The establishment of digital trust frameworks in the Internet of Medical Things (IoMT) poses distinct and complex obstacles. A major issue is the limitations on resources that are inherent in numerous IoMT devices. These devices frequently possess constrained computational capabilities and battery longevity, hence limiting the use of conventional, computationally demanding security solutions (Alsubaei et al., 2017). Hence, there is an increasing demand for lightweight digital trust frameworks that can offer strong security without overwhelming the limited resources of IoMT devices. These architectures must achieve a careful equilibrium between security and efficiency, guaranteeing that the performance of IoMT devices remains uncompromised.

When examining lightweight digital trust architectures for the Internet of Medical Things (IoMT), a number of important factors become apparent. Initially, the architecture must possess the ability to withstand a diverse range of cyber risks, such as data breaches, unauthorised access, and tampering. Due to the delicate nature of health data, any breach in security could have significant consequences, including infringements on privacy and potential threats to patient well-being (Zhang, Yang, & Chen, 2019). Furthermore, the architecture must possess the capability to scale and adjust in order to support the wide array and growing quantity of IoMT devices. As the Internet of Medical Things (IoMT) network grows, the digital trust framework needs to be able to scale proportionally, without compromising on performance or security.

Moreover, the architecture must guarantee adherence to pertinent legal standards and guidelines, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the