Chapter 6
Designing a Secure and Lightweight Ecosystem for Internet of Medical Things (IoMT) in Healthcare

M. Robinson Joel
https://orcid.org/0000-0002-3030-8431
Kings Engineering College, India

K. Martin Sagayam
Karunya Institute of Technology and Sciences, India

V. Ebenezer
Karunya Institute of Technology and Sciences, India

J. Jerlin Rajan
Karunya Institute of Technology and Sciences, India

A. Jenefa
https://orcid.org/0000-0002-6697-1788
Karunya Institute of Technology and Sciences, India

Deepak Mandali
Karunya Institute of Technology and Sciences, India

ABSTRACT

The surge in internet of things (IoT) devices, especially in healthcare's internet of medical things (IoMT), demands a nuanced balance between security and resource constraints. This chapter outlines a design framework for a lightweight and secure IoMT ecosystem, focusing on lightweight cryptography, secure routing protocols, and critical trade-offs. Careful selection of cryptographic algorithms like AES-CCM and Keccak addresses medical device limitations. Proposing routing protocol for low power and lossy networks (RPL) for resource-constrained contexts, the chapter advocates secure neighbor discovery algorithms and cryptographic protocols to fortify the network, ensuring communication legitimacy. Building a secure IoMT involves navigating trade-offs, balancing latency vs security, scalability vs security, and maintaining current security protocols while minimizing damage. Reliable authentication and access control are crucial, verifying identities and safeguarding medical information security and privacy.

DOI: 10.4018/979-8-3693-2109-6.ch006

INTRODUCTION

The initial stages of creating a safe and robust Internet of Medical Things (IoMT) (Razdan & Sharma, 2022) ecosystem for the healthcare industry include risk assessment and threat modeling. Here is a methodical approach to accomplish. Healthcare companies can find any threats and weaknesses that could jeopardize patient data security, integrity, and availability as well as essential medical services by carrying out a thorough risk assessment. Stakeholders examine the devices, networks, and data flows that make up the IoMT ecosystem (Ashfaq et al., 2022) in order to pinpoint its strengths, weaknesses, and potential dangers. Medical equipment, patient data, communication routes, and backend systems are examples of assets. Threats include a broad spectrum of possible threats, including physical tampering, malware infections, data breaches, unauthorized access, and service interruptions. Insecure device setups, out-of-date software, shoddy authentication procedures, and insufficient access controls can all lead to vulnerabilities. Organizations use threat modeling to prioritize mitigation activities by assessing the impact and likelihood of various threat scenarios. This entails taking into account the skills and intentions of possible attackers in addition to the possible effects of successful attacks on patient safety, privacy, and the reputation of the institution. Healthcare organizations can successfully limit the most severe risks by developing customized security controls and risk management strategies based on a methodical analysis of threats and vulnerabilities. In the end, risk assessment and threat modeling are proactive approaches that foresee and tackle security issues in the IoMT ecosystem. This helps healthcare companies make well-informed choices regarding risk tolerance, resource allocation, and security investments.

Begin by recognizing possible dangers and threats to the Internet of Medical Things (IoMT) ecosystem, including as unapproved access, data breaches, device tampering, and interruptions in service. Undertake a comprehensive risk assessment and threat modeling exercise to comprehend the security needs and obstacles unique to your setting. The creation of a safe Internet of Medical Things (IoMT) environment for the healthcare industry requires the implementation of risk assessment and threat modeling. Risk assessment entails locating possible dangers and weak points in the IoMT ecosystem. Analyzing the ecosystem's numerous elements, including as user interfaces, data storage systems (Cai et al., 2016), communication networks (Al-Sarawi et al., 2017), and medical equipment, is part of this process. Healthcare companies can efficiently manage resources and prioritize their security efforts by evaluating the possible impact and likelihood of various dangers. Threat modeling, on the other side, aims to comprehend the strategies, methods, and processes that attackers could employ in order to take advantage of weaknesses in the IoMT ecosystem. This entails figuring out possible threat actors, their reasons for acting, and the precise attack vectors they might use. Organizations can predict possible security breaches and create proactive defense methods (Colbaugh & Glass, 2011) to reduce these risks by modeling various attack scenarios.

When combined, threat modeling and risk assessment offer a thorough grasp of the security environment encompassing the IoMT ecosystem as shown in Figure 1. This makes it possible for healthcare institutions to put strong security measures in place to safeguard private patient information and guarantee the availability and integrity of vital medical services. Examples of these measures include intrusion detection systems, encryption, access controls, and security monitoring. Healthcare companies may improve the security posture of their systems and lessen the ever-changing dangers posed by cybercriminals (Sabillon, 2016) and malicious actors (Fortino, 2020) by including risk assessment and threat modeling into the design, development, and deployment stages of IoMT solutions. Healthcare companies may improve the security posture of their systems and lessen the ever-changing dangers