Abstract

The monitoring devices of the healthcare system are components of the Internet of Medical Things and are connected to cloud services, servers, clients and databases. These devices monitor the patient's status remotely by recording and transferring particular measurements to patient record management systems. Patient data appear to be very sensitive as it is used and interpreted as the health record of the patient. There are security and privacy requirements for data generated by IoT technology in healthcare, and there are multiples studies that conduct thorough threat analysis in order to reduce IoT devices attacks. It is important to provide the results of current studies more accessible to the healthcare manager. Therefore, it is required to identify, evaluate and categorise the summaries of each study over IoT security issues, solutions and challenges. This study employed a systematic review method to provide in-depth information about IoT threats analysis. Our finding provided the security threats affecting patient electronic health records collected and processed through medical wearables and sensor-based IoT devices and cloud information management such as DDoS, man-in the-middle attack, eavesdropping, physical data tampering, privacy attacks, false data injection, and brute force attacks, hardware misconfiguration, data exfiltration, tampering, email spoofing, social engineering (phishing), security misconfiguration, exhaustive search attacks, sensor hijacking, cloning, flooding attacks, on-off attacks, and worm-based cyber threats. Additionally, the study identified suitable countermeasures, controls, and solutions that healthcare facilities can implement to protect patient health data collected through IoMT and stored in a cloud environment such as data anonymization, privacy-preserving data aggregation scheme, proxy re-encryption, cryptography, user access control, authorization, blockchain, anti-DDoS and hybrid privacy preservations systems. Finally, the study outlined the challenges healthcare institutions face when securing patient health records in a cloud environment and medical IoT devices such as difficulties in securing massive data collected by IoMT, hackers introducing frequent and sophisticated threats that bypass implemented security controls, security teams facing difficulties in security devices located in an extensive area network. Besides, healthcare service providers lack concrete system development knowledge for some of the recommended solutions, such as blockchain technology. Ultimately, this study is crucial for the healthcare sector, medical device manufacturer, clinicians, authorities, and patients seeking to prevent malicious actors from infiltrating IoMT devices and information.