12-12-2022

Securing the Internet of Things in Healthcare: A Systematic Literature Review

Arun Aryal
California State University Los Angeles, aaryal@calstatela.edu

Crystal Wu
California State University Los Angeles, cwu11@calstatela.edu

TREO
Technology, Research, Education, Opinion

Securing the Internet of Things in Healthcare

A Systematic Literature Review

Arun Aryal, aaryal@calstatela.edu
Crystal Wu, cwu11@calstatela.edu

The increasing embeddedness of smart devices in healthcare systems is radically reshaping the traditional clinical setting. The Internet of Things (IoT) enables devices, such as remote patient monitoring technologies, that reduce costs and generate real-time health data, thereby adding value to both the patient and healthcare provider (Kashani et al., 2021). As separate research streams, the implementation of IoT in healthcare and information security risks are well studied. However, it remains challenging to understand the security risks of information from the use of the Internet of Medical Things (IoMT) technology in healthcare systems. Among the extant literature, few provide a comprehensive literature review specifically investigating the information security risks related to IoT technologies in the healthcare domain. This paper will: (1) inform practitioners and researchers of the current state of research, (2) identify research gaps, and (3) suggest new avenues for future research.

This paper reviewed studies about the information security of IoT in healthcare. To conduct the systematic literature review, we followed the multiple-step approach outlined by Kitchenham and Charters (2007). Following a defined research protocol, we searched online databases such as EBSCOhost and IEEE Explore to identify all relevant literature. We used the keywords “IoT” or “Internet of Things,” “Information Security” or “IT Security” or “InfoSec,” and “Healthcare” to find papers published between 2015 to 2022. The initial search returned over 300 articles. We further filtered our preliminary search results based on the inclusion and exclusion criteria and quality-assessment criteria. We removed duplicate and irrelevant papers, favoring more detailed and seminal publications. After completing this process, we performed a qualitative analysis of 40 research articles, extracting data features from the selected papers.

While the current study is still in its infancy, it establishes the foundations for an ongoing research paper that aims to provide researchers and practitioners with an understanding of current and future threats to health information assets from IoMT technologies. According to the preliminary results of our analysis, the key constructs in this emerging topic include scalability, interoperability, reliability, privacy, and security. One of our key findings points to securing data from remote patient monitoring technologies using blockchain. This study provides insights regarding the security of information assets from the implementation of IoT as a disruptive technology in healthcare.

References

Kashani, M. H., Madanipour, M., Nikravan, M., Asghari, P., & Mahdipour, E. (2021). A systematic review of IoT in healthcare: Applications, techniques, and trends. *Journal of Network and Computer Applications*, *192*, 103164.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering.