Chapter 10
Future Trends, Open Challenges, Emerging Technologies, Open Research Questions, Policy Implications for Internet of Medical Things

Bella Mary I. Thusnavis
Karunya Institute of Technology and Sciences, India

Paul J. John
https://orcid.org/0000-0002-3371-1277
Karunya Institute of Technology and Sciences

Ramya Katukojwala
Karunya Institute of Technology and Sciences, India

Hannah Elsa Abraham
Karunya Institute of Technology and Sciences, India

Sibiya vasantha Packiavathy
Karunya Institute of Technology and Sciences, India

P. Muthu Subramanian
https://orcid.org/0000-0003-0885-6623
Coimbatore Institute of Technology, India

ABSTRACT

The Internet of Medical Things (IoMT) is transforming healthcare by providing remote patient monitoring, personalized treatment, and advanced diagnostics.

DOI: 10.4018/979-8-3693-7225-8.ch010

However, protecting this enormous network of networked medical equipment is a predicament. A possible approach is provided by lightweight trust architectures that are created with devices with little resources in mind. The future developments in IoMT security are examined in this chapter, with particular attention paid to how blockchain and artificial intelligence, two cutting-edge technologies, might improve lightweight trust structures. In this chapter, open research problems related to data privacy, access control, and key management are highlighted. In conclusion, the possible way of lightweight trust architectures affect policy is addressed, highlighting the necessity of legislative frameworks that strike a compromise between security best practices and innovation. An extensive overview of the future environment for reliable and secure IoMT installations is given in this study.

1. INTRODUCTION

The new era of applying Artificial Intelligence and Internet of Things that we had a monitoring medical device which records customizing data for treatment and health care revolution is already in the society. However, this interconnectedness raises a critical question: can one safeguard them and the given information that is contained in this mosaic of miscellaneous devices and a huge system of devices from the daily hazards and the rules of interaction? New rather lighter forms of digital trust architectures seem plausible; but, can these concepts be scaled up with technology? This remains the case because threats are always unearthing themselves and data processing as a business activity remains on the rise. To what extent, these architectures can grow or extend over to this constantly shifting ground? Besides, the ethical concerns have to be noted as well: We are therefore sympathetic to data protection principles but not with data protection in a way that will inhibit the effective and responsible utilization of data. This raises another question on whether these architectures can be designed with the above mentioned ethical principles.

Moustafa et al (2023) states that lightweight digital trust architectures have been identified as a potential solution to securing the vast network of IoMT devices, but their ability to keep pace with evolving threats and ethical considerations requires further investigation. Despite their drive to create an IoMT that is reliable and safe for the future, researchers and developers are examining a number of unanswered issues. Perhaps, that lightweight trust structures develop with the Internet of Medical Things (IoMT) by encouraging open communication and ongoing innovation. This will possibly pave the way for a day when patient privacy and medical progress coexist.

Emerging technologies hold immense potential to solve global challenges, personalize experiences, and unlock a future brimming with innovation and progress. Some of them include: