# Chapter 13
# Study on Healthcare Security System-Integrated Internet of Things (IoT)

**S. A. Karthik**
*BMS Institute of Technology and Management, India*

**M. Deivakani**
*PSNA College of Engineering and Technology, India*

**R. Hemalatha**
*St. Joseph's College of Engineering, India*

**R. Vijaya Kumar Reddy**
*Koneru Lakshmaiah Education Foundation, India*

**R. Aruna**
*AMC Engineering College, India*

**Sampath Boopathi**
*Muthayammal Engineering College, India*

## ABSTRACT

*The internet of things (IoT) has the potential to transform healthcare by fusing the most significant technological and scientific advances in the fields of automation, mobility, and data analytics to improve patient care. IoT links sensors, actuators, and other devices to a network in order to collect and disseminate communication messages that an organization may then evaluate. To track health parameters, the suggested paradigm focuses on sensors, communications protocols, and cloud technologies. The study looks at the crucial elements of a healthcare IoT system. For the control, security, and protection of IoT networks, data confidentiality and authentication are crucial. For the purpose of resolving security challenges, flexible infrastructure is necessary. The goal of the chapter is to discuss IoT security concerns in healthcare devices and offer recommendations for future research to enhance the use of IoT devices.*

## INTRODUCTION

Thanks to the abundance of IoT devices that are available in various locations and the enormous amounts of data and information they contain, Internet of Things (IoT) healthcare systems offer a solid foundation for smart sensor technology. Huge volumes of data are released by IoT-based healthcare systems, yet

DOI: 10.4018/978-1-6684-7684-0.ch013

Copyright © 2023, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

security and privacy are crucial concerns. IoT sensors and their released data can be supported by object and cloud network topologies. The Internet of Things (IoT) is a system of linked, intelligent sensors that can perceive their surroundings and share data and processes from many areas. It is utilised in a variety of industries, including smart transportation, finance, railroads, and healthcare. Different domains are involved with smart IoT-based sensors, particularly in smart healthcare systems. The majority are offered in stores. IoT infrastructure security design is crucial for a variety of technological, scientific, and commercial reasons, including privacy and security. Security concerns are governed by IoT architectures, technologies, and design approaches. The internet of things architecture is divided into layers, and each layer makes use of a different topology and piece of hardware to maintain sensor data standardisation, privacy protection, and parameter coordination(Polu, 2019).

To track and manage the healthcare system, IoT systems need a range of data and sensors. Wireless sensors are crucial for distant security, whereas vision-based sensors improve monitoring capacity. These sensors use the concept of physical position based and are vision-based. Home-based deployment of a wireless sensor for patient eyesight that is linked to an LPWAN base station and a cloud with machine learning capabilities (Toghuj & Turab, 2022).

- Smart gadgets are those that can communicate with one another and are connected to a network or other devices. Since they only make up a minor portion of the notion, it is inaccurate to refer to them as IoT. It is preferable to refer to intelligent objects or intelligent things rather than merely devices. IoT may be used for basic calculations, communication, discovery, message reception and response (Janardhana et al., 2023; Reddy et al., 2023; Selvakumar et al., 2023). The ability to make anything intelligent is made possible by the fact that sensors are now more affordable, simple to install, and affordable than ever. They are not required for intelligent things, though.
- Bluetooth, NFC, Wi-Fi, low-power wide-area networks, and LoRa are just a few examples of the smart objects that require wireless networks to communicate with one another.
- RFID technology is a significant advancement over conventional barcodes because it makes it possible to create microchips for wireless data exchange. It has writing capabilities, requires no line-of-sight contact, and can read several tags simultaneously.
- Big data from intelligent objects, such as temperature, pressure, altitude, motion, proximity to other objects, biometrics, sound, etc., must be combined and analysed using cloud computing. One of the main problems with IoT is the integration of all this data. A platform called cloud computing enables on-demand network access to computational resources. It receives data from intelligent devices, processes and interprets it, and then presents web-based visualisations. As a result, there will be a large market with lots of potential to add value for IoT application users. These data are analysed using machine learning techniques and big data analytics. Artificial intelligence known as machine learning enables computers to become smarter by learning from the data they are fed. The quantity of data produced by IoT applications necessitates a large increase in storage space, despite the fact that big data has been a hot issue. Big businesses utilise edge computing to preprocess data before sending it to the cloud.

Confidentiality is at the nexus of privacy and security in healthcare, where both are mutually advantageous. The foundation of network security systems are security, privacy, and protection, and IOT healthcare systems offer five levels: perception layers, edge layers, transport layers, processing layers, application layers, and business layers. IoT focuses on the autonomous interaction of smart items with-

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/study-on-healthcare-security-system-integrated-internet-of-things-iot/327536

## Related Content

Accountability for Service Compliance: A Survey
Jinhui Yao, Shiping Chenand David Levy (2012). *International Journal of Systems and Service-Oriented Engineering (pp. 16-43).*
www.irma-international.org/article/accountability-service-compliance/64197

Modelling and Development of Energy Systems Through Cyber Physical Systems With Optimising Interconnected With Control and Sensing Parameters
Kaliappan Seeniappan, Chinnahajisagari Mohammad Akram, S. Soundararajanand L. Natrayan (2023). *Cyber-Physical Systems and Supporting Technologies for Industrial Automation (pp. 280-295).*
www.irma-international.org/chapter/modelling-and-development-of-energy-systems-through-cyber-physical-systems-with-optimising-interconnected-with-control-and-sensing-parameters/328505

Development and Validation of the Method for Value Assessment of SOA-Based IS Projects
Alexey Likhvarevand Eduard Babkin (2014). *International Journal of Information System Modeling and Design (pp. 49-82).*
www.irma-international.org/article/development-and-validation-of-the-method-for-value-assessment-of-soa-based-is-projects/106934

Determining the Requirements for E-Selection in a Small Recruitment Company: Using the Regulative Cycle
Tanya Bondarouk, Huub J. M. Ruëland Paul Timmermans (2013). *Software Development Techniques for Constructive Information Systems Design (pp. 1-37).*
www.irma-international.org/chapter/determining-requirements-selection-small-recruitment/75738

Variant Logic for Model Driven Applications
Jon Davisand Elizabeth Chang (2014). *Advances and Applications in Model-Driven Engineering (pp. 1-34).*
www.irma-international.org/chapter/variant-logic-model-driven-applications/78608