Chapter 12
Securing IoT Devices for Bio-Medical Image Sharing

Vinay Kumar Nassa
https://orcid.org/0009-0005-3472-8037
Ellenki College of Engineering and Technology, Hyderabad, India

Mukta Sharma
https://orcid.org/0000-0001-6784-3932
School of Life Science and Technology, IIMT University, Meerut, India

Sonia Duggal
https://orcid.org/0000-0003-0713-5904
School of Computer Applications, Manav Rachna International Institute of Research and Studies, India

Rohit Tripathi
Department of Electronics Engineering, J.C. Bose University of Science and Technology, YMCA, Faridabad, India

S. Prayla Shyry
Sathyabama Institute of Science and Technology, Chennai, India

Joshuva Arockia Dhanraj
https://orcid.org/0000-0001-5048-7775
Chandigarh University, India

Ashish Jolly
https://orcid.org/0000-0002-0849-8232
Department of Computer Science, Government PG College Ambala Cantt, India

ABSTRACT

Enhanced patient care and diagnostic capabilities have been made possible as a result of the rapid integration of Internet of Things (IoT) devices in the healthcare industry. This has resulted in a transformation in the sharing of biomedical images. Nevertheless, this technological advancement also presents significant security challenges that need to be addressed in order to protect sensitive patient data. The critical security priorities for the Internet of Things (IoT) in biomedical image shar-

DOI: 10.4018/979-8-3693-9821-0.ch012

ing are discussed in this chapter. Particular attention is paid to the importance of implementing robust authentication and authorization mechanisms, data encryption, and advanced anomaly detection techniques.

INTRODUCTION

Medical systems have been greatly impacted by the integration of smart devices, sensors (Dhanasekar, S. et al., 2023), and cutting-edge communication technologies, which has improved patient care and operational efficiency. The quality and delivery of services in medical environments can be enhanced by this technology, which makes it possible to collect, analyze, and transmit data in real-time (Pandey, B. K. et al., 2024a). Improvements in data sharing, remote patient monitoring, and general clinical setting management have resulted from it. Constant monitoring is a big advantage, especially for people with long-term illnesses. Important metrics like heart rate, blood pressure, and glucose levels can be monitored by devices (Du John. et al., 2022) like smart watches, fitness trackers, and specialized medical sensors (Shahul, A. et al., 2024).

Healthcare providers can instantly access this data, which makes it possible to identify possible health issues early and take appropriate action. By enabling personalized care and reducing the need for frequent hospital visits, remote monitoring improves patient outcomes while lowering overall costs (Pandey, D. et al., 2024). Connected medical imaging systems have also revolutionized diagnostics. Modern medical devices such as CT scanners, MRI machines, and X-ray machines make it possible to share images with medical specialists easily, leading to faster diagnosis and remote consultations. This feature improves patient care by speeding up treatment and increasing the effectiveness of diagnostic procedures (Pandey, B. K. et al., 2024b). Smart technologies help hospitals manage resources and equipment more effectively. Automated systems keep track of patient information, oversee medication inventories, and keep an eye on the availability and state of vital medical equipment. These solutions send out alerts for required maintenance and repairs, which helps to prevent equipment malfunctions(Pandey, B. K. et al., 2024c).. All things considered, automation streamlines hospital operations and guarantees that patients receive timely and effective care. Although there are many advantages to these innovations, there are security risks as well. The growing interconnectivity of systems and devices makes sensitive patient data more susceptible to cyberattacks. Strong encryption, safe authentication, and adherence to legal frameworks like HIPAA and GDPR are necessary to guarantee the security and privacy of this data (Swapna, H. R. et al., 2024a).