RADemics

AI-Enhanced Secure Communication Protocols for Wearable and Implantable Medical Devices

Ankita Avthankar, Rakesh. G, P D Selvam
SYMBIOSIS INTERNATIONAL (DEEMED UNIVERSITY), ACADEMY OF MARITIME EDUCATION AND TRAINING DEEMED TO BE UNIVERSITY, JEPPIAAR INSTITUTE OF TECHNOLOGY

AI Enhanced Secure Communication Protocols for Wearable and Implantable Medical Devices

[1]Ankita Avthankar, Teaching Assistant, Department of Computer Science and Engineering, Symbiosis Institute of Technology, Nagpur Campus, Symbiosis International (Deemed University), Pune, Maharashtra – 440008. ankita.avthankar@sitnagpur.siu.edu.in

[2]Rakesh. G, Assistant Professor, Department of Marine Engineering, Academy of Maritime Education and Training, Deemed to be University, 135, ECR- Kanathur, Chennai – 603112. rakeshg@ametuniv.ac.in

[3]P D Selvam, Associate Professor, Department of Information Technology, Jeppiaar institute of Technology, Kunnam, Sriperumbadur T.N., -631604. pdselvam@gmail.com

Abstract

The rapid advancement of wearable and implantable medical devices has revolutionized healthcare by enabling continuous monitoring and real-time data transmission. However, the increasing interconnectivity of these devices within the Internet of Medical Things (IoMT) presents significant cybersecurity challenges. Traditional security frameworks, often too resource-intensive for resource-constrained devices, fail to provide adequate protection against emerging threats. This chapter explores the integration of artificial intelligence (AI) into secure communication protocols for medical devices, offering an adaptive, efficient, and scalable solution to safeguard sensitive health data. AI-driven encryption, anomaly detection, and threat prediction models provide real-time security while minimizing energy consumption and computational overhead. Federated learning and edge intelligence further enhance data privacy by ensuring that medical data remains decentralized and protected during model training. Privacy-preserving techniques, including differential privacy, homomorphic encryption, and secure multiparty computation, are critically examined for their effectiveness in preventing unauthorized access to patient data. Through comprehensive analysis of the current state-of-the-art in AI-enhanced secure medical communication, this chapter provides insights into the future of intelligent, privacy-conscious, and resilient healthcare systems. The findings emphasize the need for transparent, ethically governed AI models that maintain compliance with global data protection standards while advancing the capabilities of next-generation biomedical technologies.

Keywords: Artificial Intelligence, Secure Communication, Wearable Devices, Federated Learning, Privacy Preservation, Medical Cybersecurity.

Introduction

The advent of wearable and implantable medical devices has reshaped the healthcare landscape, empowering healthcare providers with unprecedented access to continuous patient data for monitoring and diagnostics [1]. These devices, ranging from smartwatches to pacemakers and insulin pumps, generate a wealth of real-time data that can significantly enhance personalized treatment plans and remote patient care [2]. As the Internet of Medical Things (IoMT) continues

to expand, the potential for these devices to deliver more accurate and timely health interventions increases exponentially [3]. However, the growing reliance on interconnected devices for critical healthcare tasks introduces significant cybersecurity vulnerabilities [4]. The secure transmission and storage of sensitive health data across wireless networks have become paramount in ensuring patient safety and confidentiality. Traditional cybersecurity approaches, which rely on centralized systems and high computational resources, struggle to meet the needs of resource-constrained medical devices that often lack the processing power, memory, and energy capacity required for such conventional protocols [5].

As a result, the need for efficient, adaptive, and lightweight security models has led to the emergence of Artificial Intelligence (AI)-driven communication protocols for medical devices [6]. AI's ability to process large volumes of data, detect anomalies, and adapt to changing environments makes it an ideal candidate for securing medical communications [7]. Through machine learning, AI can enhance traditional encryption algorithms, dynamically adjusting parameters based on real-time conditions [8]. AI-powered systems are capable of identifying potential security breaches at an early stage, allowing for immediate intervention before a cyber-attack can compromise the integrity of the device or the safety of the patient [9]. This shift toward AI-based solutions not only offers improved security but also reduces the computational burden on medical devices, allowing them to maintain optimal performance while ensuring data protection [10].

Federated learning, a machine learning paradigm that enables model training across decentralized devices without sharing raw data, further enhances privacy preservation in medical communication systems [11]. In the context of medical devices, federated learning ensures that sensitive patient data remains stored on the device and is never exposed to external servers or malicious actors [12]. Instead of transmitting raw data, only model updates are shared, which minimizes the risk of data breaches [13]. This decentralized approach aligns with privacy regulations such as HIPAA and GDPR, ensuring that patient data is protected in accordance with global data protection laws [14]. Through federated learning, medical devices can collaboratively improve AI models while ensuring that privacy is maintained, thus enabling the benefits of AI without compromising patient confidentiality. This approach also makes real-time monitoring and diagnostics possible, as devices can continuously improve and adapt to emerging threats based on localized data [15].