RADemics

Cybersecurity, Privacy, and Ethics in Intelligent Healthcare Platforms

Thivya Rajkumar, Nagarathna. A
VELALAR COLLEGE OF ENGINEERING AND TECHNOLOGY, NATIONAL LAW SCHOOL OF INDIA UNIVERSITY

Cybersecurity, Privacy, and Ethics in Intelligent Healthcare Platforms

[1]Thivya Rajkumar, Assistant Professor, Department of Artificial Intelligence and Data Science, Velalar College of Engineering and Technology, Thindal, Erode, Tamil Nadu, India. thivyarajkumarvcet@gmail.com

[2]Nagarathna. A, Associate Professor of Law, National Law School of India University, Bangalore, Karnataka, India. nagarathnasachidanand@gmail.com

Abstract

Intelligent healthcare platforms have emerged as transformative digital ecosystems integrating artificial intelligence, Internet of Medical Things, cloud computing, and advanced data analytics to enable real-time patient monitoring, predictive diagnostics, and automated clinical decision support across distributed healthcare environments. Rapid digitalization of medical services has significantly increased exposure to cybersecurity threats, privacy violations, and ethical challenges associated with algorithmic decision-making and large-scale healthcare data exchange. Sensitive medical information, including electronic health records, genomic data, and continuous physiological signals, faces persistent risks from ransomware attacks, adversarial machine learning, unauthorized access, and data leakage within interconnected healthcare infrastructures. Conventional security mechanisms remain insufficient to address the complexity of cloud-edge integrated healthcare systems and heterogeneous medical device networks. Privacy preservation challenges intensify due to extensive data sharing requirements for artificial intelligence model training, cross-institutional collaboration, and remote healthcare delivery, while ethical concerns arise from algorithmic bias, lack of transparency, accountability ambiguity, and reduced interpretability in automated clinical decisions. This chapter critically examines the architectural framework of intelligent healthcare platforms and explores major security, privacy, and ethical challenges while analyzing advanced protection strategies including zero-trust security architecture, blockchain-enabled healthcare governance, encryption-based safeguards, federated learning, and privacy-preserving artificial intelligence models. Emphasis remains on strengthening secure healthcare data management, resilient communication networks, and trustworthy AI governance mechanisms aligned with global regulatory standards. The discussion highlights the necessity of integrated frameworks that unify cybersecurity resilience, privacy protection, and ethical accountability to ensure safe, transparent, and patient-centric intelligent healthcare systems in evolving digital healthcare landscapes.

Keywords: Intelligent Healthcare, Cybersecurity, Privacy Preservation, Ethical AI, Zero-Trust Architecture, IoMT Security

Introduction

Intelligent healthcare platforms represent a significant evolution in modern medical ecosystems, driven by the convergence of artificial intelligence, Internet of Medical Things, cloud computing, edge intelligence, and advanced data analytics [1]. These platforms enable continuous

health monitoring, predictive disease detection, automated diagnostic assistance, and personalized treatment planning across hospital environments and remote care settings [2]. The integration of smart medical devices, wearable sensors, electronic health records, and interconnected hospital information systems has transformed traditional healthcare delivery into a data-centric and technology-driven model [3]. Real-time acquisition and processing of physiological and clinical data support faster medical interventions and improved clinical outcomes [4]. The increasing adoption of digital healthcare infrastructures across global healthcare institutions reflects a paradigm shift toward intelligent, interconnected, and patient-focused healthcare services that enhance accessibility, efficiency, and accuracy in medical decision-making processes [5].

The architectural foundation of intelligent healthcare platforms relies on multilayered systems that integrate sensing devices, communication networks, data storage infrastructures, and artificial intelligence-based analytical engines [6]. Medical sensors and IoMT devices continuously collect patient health indicators such as heart rate, glucose levels, oxygen saturation, and blood pressure, transmitting them through wireless communication protocols into centralized or distributed computing environments [7]. Cloud computing platforms provide scalable storage and high-performance processing capabilities for large volumes of heterogeneous healthcare data, while edge computing systems enable localized processing for time-sensitive clinical applications [8]. Artificial intelligence models process these datasets to generate diagnostic predictions, risk assessments, and treatment recommendations [9]. The interoperability among healthcare applications, hospital systems, and remote monitoring devices ensures seamless data exchange and coordinated healthcare delivery across geographically distributed environments [10].

The expansion of intelligent healthcare platforms has introduced complex cybersecurity challenges due to increased system connectivity and dependency on digital infrastructures [11]. Healthcare systems have become prime targets for cyberattacks because of the high value and sensitivity of medical data [12]. Threats such as ransomware attacks, phishing campaigns, malware intrusion, insider threats, and distributed denial-of-service attacks disrupt healthcare operations and compromise patient safety [13]. Vulnerabilities within IoMT devices, cloud platforms, and application programming interfaces further expand attack surfaces within healthcare ecosystems [14]. AI-driven healthcare systems also face emerging risks such as adversarial attacks, data poisoning, and model inversion techniques that compromise algorithmic integrity and decision accuracy. These cybersecurity concerns necessitate advanced defense mechanisms capable of protecting distributed healthcare infrastructures against evolving cyber threats [15].