RADemics

IoT Security and Privacy Challenges in Smart Healthcare with AI Based Threat Detection and Risk Mitigation Strategies

S Mani Kuchibhatla, Ashok Kumar. V, R. Bharathi

ACE ENGINEERING COLLEGE, VEL TECH RANGARAJAN DR. SAGUNTHALA R&D INSTITUTE OF SCIENCE AND TECHNOLOGY, M. KUMARASAMY COLLEGE OF ENGINEERING

IoT Security and Privacy Challenges in Smart Healthcare with AI Based Threat Detection and Risk Mitigation Strategies

[1]S Mani Kuchibhatla, Professor, EEE, ACE Engineering College, Ghatkesar, Hyderabad, India. ksmani.mtech@gmail.com

[2]Ashok Kumar. V, Assistant Professor, Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu 600062 . ashokvijay872@gmail.com

[3]R. Bharathi, Assistant Professor, Information Technology, M. kumarasamy College of Engineering, Thalavapalayam, Karur. bharathimkce@gmail.com

Abstract

The integration of Internet of Things (IoT) technologies within smart healthcare systems has revolutionized medical diagnostics, patient monitoring, and treatment personalization, the widespread deployment of interconnected medical devices introduces a complex landscape of security and privacy risks, exposing sensitive health data to cyber threats and unauthorized access. As healthcare systems generate vast volumes of real-time data across distributed environments, traditional security mechanisms fall short in ensuring end-to-end protection, especially under the resource constraints of IoT devices. Artificial intelligence (AI) has emerged as a transformative force, enabling proactive threat detection, intelligent risk scoring, and adaptive mitigation strategies that operate in dynamic healthcare ecosystems. This chapter presents a comprehensive analysis of IoT security architectures in smart healthcare, examining vulnerabilities at each system layer and highlighting AI-driven frameworks for intrusion detection, anomaly recognition, and privacy-preserving data analytics. Advanced methods such as federated learning, differential privacy, homomorphic encryption, and secure multi-party computation are explored as essential tools for safeguarding patient information while maintaining model utility and interoperability. The convergence of AI and cybersecurity offers a resilient approach to managing evolving threats without compromising clinical efficiency or regulatory compliance. Key challenges, including scalability, explainability, and cross-border data governance, are critically assessed, along with future directions for building robust, ethical, and intelligent healthcare infrastructures.

Keywords: Smart Healthcare, IoT Security, Privacy Preservation, Artificial Intelligence, Threat Detection, Federated Learning

Introduction

The transformation of healthcare through the adoption of Internet of Things (IoT) technologies has led to the emergence of smart healthcare systems that rely on interconnected devices, real-time data streams, and remote monitoring capabilities [1]. These systems enable enhanced patient engagement, streamlined clinical workflows, and personalized care delivery [2]. Wearable

biosensors, ambient monitoring units, and intelligent medical devices are now routinely integrated into clinical settings and patient homes, enabling continuous health tracking and early detection of anomalies [3]. This exponential growth of IoT in healthcare has introduced an expanded attack surface that adversaries can exploit, resulting in growing concerns about data breaches, device hijacking, and service disruptions [4]. As healthcare becomes increasingly digitized, ensuring robust security and privacy mechanisms becomes indispensable for preserving the integrity, confidentiality, and availability of patient data [5].

While the benefits of smart healthcare technologies are substantial, the complexity of securing distributed IoT architectures presents significant challenges [6]. Medical IoT environments typically consist of heterogeneous devices with varying hardware capabilities, operating systems, and communication protocols [7]. Many of these devices have limited computational power, storage capacity, and battery life, which restrict the deployment of conventional security solutions such as heavy encryption or real-time intrusion detection [8]. A medical data is highly sensitive and subject to strict regulatory requirements such as HIPAA and GDPR. As a result, the integration of advanced, lightweight, and context-aware security frameworks has become a critical research area [9]. It is essential to address not only the vulnerabilities of individual devices but also the systemic risks arising from interconnected data pipelines and distributed control mechanisms [10].