RADemics

Cryptographic Support for Privacy Preservation in IoT Based Healthcare Systems

M. Abinaya, Bramah Hazela
KARPAGA VINAYAGA COLLEGE OF ENGINEERING AND TECHNOLOGY, AMITY SCHOOL OF ENGINEERING AND TECHNOLOGY

Cryptographic Support for Privacy Preservation in IoT Based Healthcare Systems

[1]M. Abinaya, Assistant Professor, Department of Computer Science and Engineering, Karpaga Vinayaga College of Engineering and Technology, Chengalpattu, Tamil Nadu, India. abimohan216@gmail.com

[2]Bramah Hazela, Assistant Professor, Department of Computer Science and Engineering, Amity School of Engineering and Technology, Lucknow, Amity University Uttar Pradesh. bramahhazela77@gmail.com

Abstract

The integration of Internet of Things (IoT) technologies in modern healthcare systems has revolutionized patient monitoring, diagnostics, and personalized treatment, this transformation also introduces critical security and privacy concerns due to the continuous collection, processing, and wireless transmission of sensitive medical data across resource-constrained devices. Traditional cryptographic methods are often unsuitable for these environments, necessitating the adoption of lightweight cryptographic solutions that balance robust security with minimal energy and computational overhead. This chapter presents a comprehensive analysis of the current landscape, limitations, and future directions of cryptographic mechanisms in IoT-based healthcare systems, with a focus on lightweight algorithmic design, encryption latency in time-critical operations, and energy-aware security protocols for battery-operated and energy-harvested biomedical devices. Emerging challenges related to regulatory compliance, algorithm agility, and standardization are critically examined, alongside an exploration of novel research opportunities in optimizing cryptographic performance for ultra-low-power medical applications. The synthesis of these insights aims to guide the development of next-generation secure healthcare infrastructures that ensure both patient safety and long-term device reliability.

Keywords: Lightweight Cryptography, IoT Healthcare, Privacy Preservation, Biomedical Devices, Energy-Efficient Security, Standardization.

Introduction

The integration of Internet of Things (IoT) technologies into healthcare has profoundly changed how clinical services are delivered, monitored, and managed [1]. Through interconnected medical sensors, wearable devices, and cloud-based platforms, healthcare providers can continuously track patient vitals, manage chronic diseases, and offer remote consultations in real time [2]. This digital shift, known as the Internet of Medical Things (IoMT), enhances diagnostic accuracy, patient engagement, and operational efficiency [3]. These advancements are accompanied by a substantial increase in the exposure of sensitive personal health data to digital threats. Unauthorized access, data breaches, and malicious manipulation of health parameters pose significant risks to patient safety and institutional trust [4]. As a result, safeguarding the confidentiality, integrity, and authenticity of data across these distributed and dynamic environments has become a critical research concern [5].

Medical IoT devices operate under stringent energy, memory, and processing constraints, especially in the case of implantable and wearable technologies [6]. These devices must function autonomously for extended periods, often in conditions where battery replacement or recharging was impractical or impossible [7]. Traditional cryptographic methods such as AES and RSA, while secure, impose significant computational and power demands that exceed the capacity of many healthcare-grade IoT devices [8]. Consequently, these algorithms are unsuitable for real-time encryption, secure authentication, and data exchange in low-resource settings [9]. Lightweight cryptographic schemes, developed specifically for resource-constrained environments, offer a viable alternative. They provide comparable security with reduced overhead, making them suitable for devices that must prioritize energy conservation, data transmission efficiency, and long-term functionality [10].