RADemics

Blockchain and IoT for Secure Medical Data Management in Healthcare Applications

Sujit Kumar Sadhukhan, Palak Keshwani
BRAINWARE UNIVERSITY, THE ICFAI UNIVERSITY

Blockchain and IoT for Secure Medical Data Management in Healthcare Applications

[1]Sujit Kumar Sadhukhan, Assistant Professor, Department of Computer Science and Engineering-Cyber Security and Data Science, Brainware university, Kolkata, West Bengal, India. sujitkumarsadhukhan@gmail.com

[2]Palak Keshwani, Assistant Professor, Department of Computer Science and Engineering, Faculty of Science and Technology, The ICFAI University, Raipur, India. palakkeshwani@iuraipur.edu.in

Abstract

The rapid expansion of healthcare Internet of Things (IoT) devices has generated unprecedented volumes of medical data, presenting significant challenges in terms of security, privacy, interoperability, and real-time access. Traditional centralized healthcare systems are often inadequate to address these challenges due to vulnerabilities such as single points of failure, data tampering, and limited transparency. This chapter proposes a hybrid blockchain-IoT framework designed to enable secure, privacy-preserving, and interoperable medical data management across distributed healthcare networks. The framework integrates decentralized blockchain mechanisms with multi-layer IoT architecture, leveraging smart contracts for automated access control, consent management, and auditability while employing off-chain storage and edge computing to enhance scalability and reduce latency. Performance evaluation emphasizes transaction throughput, latency, resource utilization, and consensus efficiency, demonstrating the framework's capability to handle large-scale healthcare data in real-time. Standardization and governance considerations are incorporated to ensure compliance with global healthcare regulations and facilitate interoperability across heterogeneous medical systems. The proposed framework not only enhances data security and integrity but also supports patient-centric healthcare delivery, enabling intelligent decision-making, collaborative research, and seamless multi-institutional data exchange. The findings highlight the transformative potential of hybrid blockchain-IoT architectures in modern healthcare, addressing critical gaps in scalability, privacy preservation, and trust management.

Keywords: Blockchain, Internet of Things, Healthcare Data Security, Interoperability, Smart Contracts, Privacy Preservation

Introduction

The healthcare industry has witnessed unprecedented technological evolution in recent years, largely driven by the proliferation of connected medical devices and the adoption of digital health solutions [1]. Internet of Things (IoT) technologies have emerged as a critical component in this transformation, enabling continuous patient monitoring, remote diagnostics, and real-time health data collection [2]. Wearable sensors, implantable devices, and smart monitoring systems generate high-frequency physiological and behavioral data, allowing healthcare providers to identify trends, predict adverse events, and tailor treatments to individual patients [3]. These advantages, the massive volume, heterogeneity, and sensitivity of IoT-generated medical data present significant challenges. Centralized healthcare infrastructures are often incapable of efficiently managing this data while maintaining security, privacy, and traceability [4]. Such systems are vulnerable to cyberattacks, unauthorized access, and potential data loss, which can compromise patient safety and violate regulatory requirements. Consequently, innovative frameworks that combine advanced technologies and decentralized architectures are essential to ensure the reliable, secure, and efficient handling of medical data in modern healthcare environments [5].

Blockchain technology provides a promising solution to the security, privacy, and interoperability challenges inherent in IoT-based healthcare systems [6]. By creating a decentralized, immutable ledger, blockchain ensures that all medical transactions are verifiable, traceable, and resistant to tampering [7]. This decentralization mitigates the risks associated with single points of failure, which are common in conventional centralized databases. Blockchain supports the implementation of cryptographic techniques that protect sensitive medical information from unauthorized access, enabling patient-centric data ownership [8]. Smart contracts extend these capabilities by automating critical processes such as access control, consent management, and clinical workflow enforcement [9]. Integrating blockchain with IoT devices creates a robust and transparent infrastructure where real-time medical data can be securely recorded, validated, and shared among multiple stakeholders, including hospitals, insurers, regulatory bodies, and patients. The resulting synergy enhances trust, reduces operational inefficiencies, and establishes a foundation for advanced healthcare analytics and predictive modeling [10].

The hybrid blockchain-IoT framework further addresses the challenges of scalability, latency, and interoperability, which are particularly critical in large-scale healthcare deployments [11]. IoT devices often operate in resource-constrained environments, with limitations in processing power, memory, and energy [12]. Blockchain, in its traditional forms, can introduce computational overhead and latency due to consensus mechanisms and transaction verification processes [13]. The integration of edge computing, off-chain storage, and lightweight consensus protocols within a hybrid framework mitigates these challenges, enabling real-time processing and secure storage of massive medical datasets [14]. Interoperability between heterogeneous devices, platforms, and healthcare institutions was facilitated through standardized communication protocols and semantic data models. This ensures that medical information collected from diverse sources can be accurately interpreted and utilized, supporting collaborative care, multi-institutional research, and telemedicine applications. By optimizing both computational efficiency and data integration, the hybrid framework demonstrates its capability to manage complex healthcare ecosystems without compromising performance or security [15].