Digitus : Journal of Computer Science Applications
E-ISSN : 3031-3244
Volume. 3, Issue 1, January 2025
Page No: 15-28

Blockchain and IoT Integration for Secure Healthcare Data Management: A Narrative Review

Adi Wahyu Setiawan
STMIK Mercusuar, Indonesia
Correspondent: adi.wahyu@mercusuar.ac.id

Received : December 1, 2024
Accepted : January 12, 2025
Published : January 31, 2025

Citation: Dewi, R, K. Nugroho, A. (2025). Sentiment as Signal: Detecting Political Misinformation in Indonesia's 2024 Election via Lexicon Based NLP. Digitus : Journal of Computer Science Applications, 3 (1), 15-28.

ABSTRACT: The convergence of blockchain and Internet of Things (IoT) technologies has the potential to revolutionize secure data management in healthcare systems. This narrative review investigates how this integration addresses critical issues such as data privacy, interoperability, energy efficiency, and systemic barriers in healthcare. Literature was gathered from databases including Scopus, Web of Science, and Google Scholar, using keyword combinations such as "Blockchain AND IoT AND Healthcare" and "Cybersecurity AND IoT AND Data Privacy". Studies published between 2018 and 2024 were included based on clear methodological standards and relevance to healthcare applications. The review reveals that blockchain significantly enhances the security, transparency, and accessibility of personal health data while enabling efficient remote monitoring through IoT integration. It also highlights that smart contracts and AI-augmented systems optimize operations, reduce delays, and lower costs. However, challenges such as poor infrastructure, low digital literacy, and fragmented regulations impede widespread adoption. Notably, the impact of these factors varies across developed and developing countries. These findings suggest that policy reforms, increased investment in infrastructure, and public education are vital to advancing technological uptake. The study concludes that blockchain-IoT systems represent a strategic innovation in healthcare but require holistic, cross-sector collaboration to realize their transformative potential..

Keywords: Blockchain In Healthcare, Internet of Things, Data Security, Interoperability, Health Information Systems, Smart Contracts, Digital Health Transformation.

INTRODUCTION

In recent years, the integration of emerging technologies such as the Internet of Things (IoT) and blockchain into various sectors has gained increasing attention due to their potential to revolutionize traditional systems. Among these sectors, healthcare stands out as a critical domain where the secure and efficient management of personal data is essential. With the global surge in

the use of mobile health applications, wearable sensors, and cloud-based patient monitoring platforms, ensuring the privacy, accuracy, and traceability of health data has become paramount (Fatoum et al., 2021; Badri et al., 2023). Blockchain technology, with its decentralized and immutable characteristics, is increasingly seen as a viable solution to address these needs. It offers not only robust data security but also facilitates greater patient control over personal health records (PHRs), thereby fostering trust and transparency in health data exchange.

A parallel trend involves the deployment of IoT-based PHR systems, which provide continuous health monitoring through wearable devices and mobile applications. These systems are designed to collect, process, and transmit medical information in real time, enhancing decision-making by both patients and providers (Vicoveanu, 2025). However, as these technologies proliferate, so do the risks. The healthcare sector is experiencing a rising number of data breaches, cyberattacks, and unauthorized data sharing incidents. These threats underscore the urgent need for secure infrastructure and governance mechanisms that can effectively handle sensitive medical information (Goyal, 2025).

Several studies have emphasized the transformative potential of combining blockchain and IoT in healthcare. Fatoum et al. (2021) have shown that blockchain improves data integrity and supports user sovereignty over health data, while Vicoveanu (2025) highlights how IoT integration enhances real-time patient monitoring. Nonetheless, these advancements come with considerable challenges. One prominent issue is cybersecurity. The integration of IoT into healthcare systems introduces multiple vulnerable endpoints, increasing the attack surface for malicious actors (Condon et al., 2023; Goyal, 2025). Blockchain may address some of these concerns, yet its implementation is not without complications.

A critical technical challenge is interoperability. Despite blockchain's theoretical advantages, practical deployment in heterogeneous healthcare environments remains limited due to incompatible data formats, proprietary standards, and lack of integration protocols (Barka et al., 2021; Mohan et al., 2024). Additionally, adoption barriers persist among both healthcare providers and patients. Systems are often overly complex or lack user-friendly interfaces, reducing accessibility and acceptance (Elkhodr et al., 2024; Badri et al., 2023; Bhatia et al., 2021). Furthermore, blockchain platforms are often energy-intensive and may not be scalable for large-scale healthcare operations (Attkan & Ranga, 2022).

Moreover, many proposed models and solutions in the existing literature have yet to demonstrate real-world effectiveness. Numerous studies have remained conceptual, focusing on theoretical frameworks without adequate empirical validation (Aldhyani et al., 2023; Babu et al., 2023). Other research initiatives have employed overly complex architectures that strain system performance and limit practical deployment (Kumar et al., 2023). There is also a tendency to overlook the human and social aspects of technological adoption, resulting in systems that may be secure but are difficult to integrate into everyday clinical workflows (Agrawal & Kumar, 2022; Ju et al., 2024; Singh et al., 2023).

A substantial knowledge gap persists concerning the broader implications of blockchain and IoT integration, particularly in understanding its social, cultural, and ethical dimensions. Fatoum et al.

(2021) noted that many studies concentrate exclusively on technical feasibility while neglecting the societal impact of these technologies. Issues such as trust in digital systems, patient consent, and the cultural perception of data ownership remain underexplored (Hasan et al., 2022; Condon et al., 2023). Ahmed et al. (2024) further point out the lack of research concerning technology adoption in low-resource settings, where infrastructural limitations and varying degrees of digital literacy may significantly affect implementation success.

The need for interoperability across platforms and the user's readiness to embrace technology also raises important concerns about system readiness. Khodadadi and Towfek (2023) emphasize the importance of understanding these dynamics, particularly when attempting to implement cross-platform solutions in decentralized environments. These deficiencies underscore the urgency for more holistic research approaches that integrate technical development with policy, ethics, and user-centered design.

Given these considerations, the primary objective of this review is to critically examine the challenges and opportunities associated with the integration of blockchain and IoT in healthcare data management. This includes identifying unresolved issues related to data security, patient privacy, and platform interoperability, while also highlighting the factors that contribute to or hinder successful adoption. In doing so, this study aims to bridge the gap between technological capability and practical application, offering insights for researchers, system developers, and healthcare policymakers alike. Previous research has shown that while blockchain can substantially enhance data security, its full potential remains unrealized due to fragmented systems and policy mismatches (Zerraza et al., 2024; "Data Management and Security in Blockchain Systems," 2024).

In particular, this review seeks to generate strategic recommendations for designing user-friendly, secure, and scalable systems that can facilitate the responsible and widespread use of these technologies. It will explore frameworks that mitigate privacy risks while ensuring usability, accessibility, and alignment with healthcare operational workflows. Furthermore, the study will analyze best practices and case studies to extract lessons for future implementations in similar contexts (Vicoveanu, 2025; S. Anitha & Murugan, 2024).

While significant attention has been paid to technology deployment in high-income countries with robust digital infrastructure, there is limited research addressing the challenges faced in low- and middle-income countries. Mohan et al. (2024) and Goyal (2025) underscore that most studies originate from developed nations, resulting in a lack of nuanced understanding of how these technologies function in resource-constrained environments. This imbalance has contributed to a global knowledge disparity that marginalizes certain regions from the benefits of digital health transformation.

Additionally, there are underexplored areas within the healthcare sector itself. For instance, while much research has concentrated on chronic disease management or hospital data systems, mental health services have received relatively less attention. Yet, these services could greatly benefit from secure and private digital platforms that offer remote consultation, support, and monitoring (Agrawal & Kumar, 2022; Li et al., 2020). By extending the scope of investigation to include

overlooked populations and health domains, this review aspires to provide a more inclusive perspective on the potential of blockchain and IoT integration.

In sum, this review aims to advance the academic discourse by filling critical gaps in the literature through a comprehensive analysis of the current state, challenges, and future directions of blockchain and IoT technologies in healthcare. By adopting an interdisciplinary lens, this study not only contributes to technical knowledge but also highlights ethical, social, and policy considerations necessary for building a more secure, equitable, and efficient digital health ecosystem.

METHOD

This narrative review adopted a rigorous and systematic approach to identify, analyze, and synthesize peer-reviewed literature relevant to the integration of blockchain and Internet of Things (IoT) technologies in healthcare data management and information security. The methodology was structured to ensure transparency, reproducibility, and academic rigor, with clearly defined strategies for literature search, keyword formulation, inclusion and exclusion criteria, and article selection and evaluation.

To gather comprehensive and up-to-date literature, searches were conducted across several widely recognized academic databases, including Scopus, Web of Science, and Google Scholar. These databases were selected due to their extensive indexing of multidisciplinary and high-impact scientific publications, particularly in the fields of computer science, engineering, healthcare, and information systems. The search was conducted between January and April 2025 and was restricted to publications released from 2018 to 2024. This temporal range was selected to capture the most recent advancements and ensure the review reflects the state-of-the-art developments in blockchain and IoT applications within the healthcare sector.

The formulation of search queries was guided by a comprehensive list of keywords and Boolean logic operators to enhance the sensitivity and specificity of the literature search. The following keyword combinations were employed across databases to identify relevant articles: "Blockchain AND IoT AND Healthcare," "Data Security AND Blockchain AND IoT," "Personal Health Records AND Blockchain," "Cybersecurity AND IoT AND Healthcare," "Decentralized Data Management AND Blockchain," "Smart Contracts AND IoT AND Data Privacy," "Remote Patient Monitoring AND Blockchain," "Interoperability AND IoT AND Blockchain Technology," "Energy Management AND Blockchain AND IoT," and "Artificial Intelligence AND Blockchain AND Healthcare." These combinations were carefully selected to ensure that the scope of retrieved literature would not only capture the technical implementations of blockchain-IoT integrations but also highlight their social, ethical, and organizational implications, as emphasized by recent studies (Fatoum et al., 2021; Ahmed et al., 2024; Badri et al., 2023; Babu et al., 2023).

All retrieved records were screened in two phases. In the initial phase, titles and abstracts were examined to determine their relevance to the objectives of this review. Duplicates and obviously irrelevant records were removed. In the second phase, the full texts of the remaining articles were reviewed to assess their eligibility based on predefined inclusion and exclusion criteria. This dual-stage process ensured a focused and high-quality selection of literature, reducing the risk of bias and improving the reliability of the findings.

The inclusion criteria for selecting literature were as follows. First, the studies had to be published in peer-reviewed journals between 2018 and 2024. This criterion was set to capture the evolving nature of blockchain and IoT technologies and their implementation in real-world healthcare settings (Fatoum et al., 2021; Ahmed et al., 2024; Badri et al., 2023). Second, eligible articles were those that presented empirical data, systematic reviews, or studies with clearly defined methodologies that contributed to the understanding of healthcare data management through blockchain and IoT. The studies had to directly address the application of these technologies in health systems, with specific focus on data security, patient privacy, interoperability, or system architecture. Third, the geographic scope was not restricted to any specific region, allowing for an inclusive perspective that considered both developed and developing countries. This broader perspective aimed to identify disparities in technology adoption and highlight contextual factors that may influence implementation strategies. Lastly, the review focused on studies that addressed applications in the healthcare sector, particularly those involving the management of personal health information, cybersecurity, or digital health infrastructure (Vicoveanu, 2025; Aldhyani et al., 2023).

To maintain the quality and relevance of included studies, a set of exclusion criteria was also applied. Articles were excluded if they did not specifically explore the integration of blockchain and IoT within healthcare contexts or data security frameworks. This ensured the review remained narrowly focused on its central theme. Further, theses, dissertations, white papers, and conference abstracts that had not undergone peer-review were omitted from the analysis to preserve academic credibility. Articles published before 2018 were also excluded to avoid outdated insights that may no longer reflect current technological capabilities or healthcare policies (Hasan et al., 2022; Badri et al., 2023).

Regarding the type of studies included, this review embraced both quantitative and qualitative research, including randomized controlled trials (RCTs), cohort studies, case-control studies, case studies, simulation models, and systematic reviews. Empirical studies that employed machine learning models, pilot systems, or experimental prototypes were included if they demonstrated practical implementations or outcomes of blockchain and IoT in healthcare. Simulation-based studies and proofs of concept were considered valuable for understanding the theoretical underpinnings and potential scalability of emerging systems. Studies that employed mixed-methods designs were particularly appreciated for offering insights into both technical performance and user perspectives, especially in patient-provider interactions and ethical considerations.

Once selected, each article underwent a structured evaluation to assess methodological quality and relevance. The evaluation involved examining the study design, data collection procedures, sample

size, system architecture, outcome metrics, and implications for practice or policy. Studies that provided robust analytical frameworks or comprehensive discussions on interoperability, cybersecurity threats, privacy-by-design principles, and the integration of smart contracts in health systems were prioritized. Additionally, articles that engaged with socio-technical dimensions, such as digital literacy, user adoption barriers, and healthcare equity, were considered highly relevant.

Data extracted from the final pool of studies were synthesized thematically. Themes were identified through iterative reading and coding of texts, focusing on recurring concepts such as scalability, interoperability, patient empowerment, regulatory frameworks, and system sustainability. These themes were further analyzed to reveal patterns, divergences, and critical gaps in the current knowledge base. The thematic synthesis approach enabled the integration of diverse perspectives and findings from various disciplinary backgrounds, ranging from computer science and biomedical engineering to public health and ethics.

In summary, this methodological framework provided a systematic and comprehensive pathway to identify high-quality literature on blockchain and IoT integration in healthcare. By combining precise search strategies with stringent inclusion and exclusion criteria, and employing a structured evaluation process, this review sought to ensure the reliability, relevance, and analytical depth of its findings. The selected studies formed the empirical and conceptual foundation for the ensuing results and discussion sections, contributing to a nuanced understanding of the opportunities and limitations associated with deploying these technologies in healthcare data management.

RESULT AND DISCUSSION

The analysis of the selected literature reveals several recurring themes that characterize the current understanding of integrating blockchain and Internet of Things (IoT) technologies within the healthcare data management domain. These themes, which have emerged consistently across quantitative and qualitative studies, center on issues of data security and privacy, interoperability, healthcare service enhancement, cost and energy efficiency, and the integration of artificial intelligence (AI) with blockchain-enabled systems. This section discusses each of these themes in depth and explores the critical factors that influence their development, implementation, and effectiveness.

One of the most dominant themes in the literature is data security and privacy, particularly in the context of managing personal health records. As healthcare data becomes increasingly digitized and distributed through mobile applications, wearable sensors, and cloud-based systems, the risks associated with unauthorized access and breaches have risen significantly. Blockchain technology, known for its decentralized and immutable architecture, has been widely proposed as a solution to these challenges. Numerous studies confirm that blockchain enables individuals to control access to their medical data, thereby enhancing trust and reducing vulnerabilities (Fatoum et al., 2021; Ahmed et al., 2024; Vicoveanu, 2025). Through the application of smart contracts, patients can specify data access conditions, and healthcare providers can interact with these datasets securely and transparently.

Interoperability emerged as another key theme, especially concerning the integration of data across disparate health information systems. Blockchain is perceived as a potential enabler of seamless data exchange, overcoming the limitations posed by fragmented systems and heterogeneous data formats. Studies by Khodadadi and Towfek (2023) and Hasan et al. (2022) highlight that blockchain can serve as a trusted infrastructure for maintaining consistent and verifiable records, which improves clinical decision-making and facilitates patient mobility across providers. Nevertheless, achieving interoperability is contingent on the development of shared standards and protocols, which remain underdeveloped in many healthcare systems.

Another prominent theme is the impact of blockchain and IoT integration on healthcare delivery, particularly in terms of enhancing personal health record (PHR) systems and enabling remote patient monitoring. Research demonstrates that such integration leads to more proactive and personalized care models by continuously collecting real-time health data and storing it securely on blockchain networks (Ahmed et al., 2024; Vicoveanu, 2025; Badri et al., 2023). In pandemic and post-pandemic scenarios, remote monitoring has been invaluable, enabling patients with chronic conditions to receive care without frequent hospital visits. This has not only improved health outcomes but also optimized resource allocation in overwhelmed healthcare systems.

Energy efficiency and cost reduction are additional areas of interest, with several studies exploring the economic implications of implementing blockchain in healthcare settings. Agrawal and Kumar (2022) report measurable improvements in system performance, with a throughput increase of 8.5% and a reduction in communication latency by 15.3% in blockchain-enabled infrastructures. Anitha and Murugan (2024) add that blockchain contributes to reduced operational costs through its automation capabilities and reduction in data redundancy. These efficiency gains are critical for healthcare institutions facing budgetary constraints, especially in developing regions.

A final theme that frequently appears in the literature is the integration of blockchain with artificial intelligence (AI) and machine learning. This hybridization is viewed as a way to enhance the analytical capabilities of healthcare systems. AI-driven models can process the vast volumes of data generated by IoT devices, while blockchain ensures data integrity and traceability. Studies by Elkhodr et al. (2024) and Barka et al. (2021) show that combining AI and blockchain can support clinical diagnostics, early warning systems, and personalized treatment recommendations, further expanding the scope and utility of digital health ecosystems.

The prevalence and significance of these themes are substantiated by both quantitative and qualitative data. Quantitative studies provide empirical evidence supporting the effectiveness of blockchain-enabled systems in securing health data and improving system efficiency. For example, Duhayyim et al. (2022) demonstrated that a blockchain-based electronic health record system maintained high resilience against data breaches and unauthorized access, significantly outperforming conventional models. Similarly, the research by Agrawal and Kumar (2022) offered statistical validation of operational improvements linked to blockchain deployment.

Qualitative studies, on the other hand, have enriched the understanding of user experiences and perceptions. Interviews and surveys with healthcare professionals and patients reveal increased trust in digital health systems due to blockchain's transparent and tamper-proof nature (Fatoum et al., 2021; Vicoveanu, 2025; Badri et al., 2023). These insights are valuable for identifying organizational and interpersonal barriers that may hinder technology adoption. For instance,

Khodadadi and Towfek (2023) emphasize that while technical benefits are clear, adoption is often slowed by unfamiliarity with blockchain concepts among healthcare staff and lack of institutional support structures.

Beyond thematic synthesis, the analysis also identifies a set of socio-economic, technological, and policy-related factors that significantly influence the success or failure of blockchain and IoT integration in healthcare. From a social perspective, public perception of digital technologies and general trust in healthcare institutions play a vital role in acceptance. Educational efforts that raise awareness about the benefits and safeguards associated with blockchain systems are shown to positively impact adoption rates (Fatoum et al., 2021; Bhatia et al., 2021). Furthermore, literacy in digital health tools is critical, particularly among elderly populations or communities with limited prior exposure to digital infrastructure.

Economic considerations, especially in low- and middle-income countries, are central to the feasibility of implementing blockchain and IoT technologies. Cost-intensive requirements for hardware, network infrastructure, and skilled personnel present formidable obstacles. As Condon et al. (2023) and Badri et al. (2023) highlight, without adequate financial investment and support, these technologies risk remaining confined to high-income settings, exacerbating existing health inequities. Budget constraints also affect training programs, maintenance, and long-term system upgrades, which are essential for sustainable integration.

From a technological standpoint, the availability, maturity, and scalability of both blockchain and IoT solutions determine their real-world applicability. Technologies must demonstrate operational efficiency, interoperability, and minimal latency, especially in environments with complex data workflows such as hospitals (Ahmed et al., 2024; Elkhodr et al., 2024; Barka et al., 2021). Without these capabilities, the integration may produce more burden than benefit.

Policy and regulatory frameworks further shape the implementation landscape. Data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union, impose strict guidelines on how health data should be stored and accessed. These policies, while essential for privacy, can complicate blockchain deployment due to its immutability and distributed nature (Condon et al., 2023; Ghaderi & Ghaderi, 2025). Therefore, successful implementation requires alignment between technological functionalities and legal requirements, necessitating cross-disciplinary collaboration.

The influence of these factors varies across regional and sectoral contexts. In developing countries, economic and regulatory constraints are more pronounced. Babu et al. (2023) and Aldosary & Alkhatib (2024) document how limited public infrastructure, weak policy frameworks, and lower levels of digital literacy impede blockchain and IoT adoption. By contrast, in developed nations, technological readiness and social acceptance play a more significant role. For example, in countries such as Germany or the Netherlands, citizens demonstrate high levels of trust in digital health services, supported by robust infrastructure and clear policy direction (Fatoum et al., 2021; Vicoveanu, 2025; K et al., 2024).

The European context also illustrates how regional policy can influence implementation. The GDPR mandates strict user consent and data portability provisions, which have encouraged the development of blockchain systems that prioritize privacy-by-design. In these systems, data is

stored off-chain with blockchain serving as a reference layer to ensure integrity and traceability (Condon et al., 2023; Ghaderi & Ghaderi, 2025).

Within the healthcare sector specifically, the use of blockchain and IoT for remote patient monitoring has shown considerable promise. During the COVID-19 pandemic, several healthcare systems deployed wearable IoT devices connected to blockchain networks to track symptoms and treatment efficacy while maintaining data security. Although this approach enhanced care accessibility and continuity, it also raised significant challenges regarding secure data transmission and real-time processing capabilities (Vicoveanu, 2025; Badri et al., 2023; S. Anitha & Murugan, 2024).

In conclusion, the integration of blockchain and IoT technologies in healthcare is shaped by a constellation of interrelated themes and contextual factors. While there is strong evidence supporting the potential benefits of these technologies, their successful implementation depends on addressing technical, organizational, economic, and regulatory challenges. Future research and policy must aim to build adaptable and inclusive digital health systems that account for these diverse influences across global contexts.

The findings of this narrative review substantially contribute to the existing body of knowledge regarding the integration of blockchain and Internet of Things (IoT) technologies in healthcare data management. These results reinforce theoretical frameworks that underscore the value of digital infrastructure in enhancing data security, interoperability, and operational efficiency. Specifically, Fatoum et al. (2021) posit that blockchain's decentralized architecture facilitates improved control over personal health information, aligning with broader theories of information system optimization through digitization. The notion that patients can autonomously govern access to their data aligns with concepts in digital sovereignty and privacy-by-design models.

However, the results also challenge the prevailing assumption that technological availability directly translates to successful adoption. As Hasan et al. (2022) observe, countries with limited resources often face significant obstacles despite access to modern technologies. These include inadequate digital infrastructure and socio-economic constraints, which indicate that theoretical models focusing solely on the technical capabilities of blockchain and IoT are insufficient. In fact, these findings demand a revision of conventional technology adoption models to incorporate socio-cultural and economic determinants, particularly in under-resourced contexts.

Additionally, the literature expands upon existing theories of trust and interoperability within healthcare systems. Vicoveanu (2025) demonstrates that blockchain not only facilitates real-time data synchronization across institutions but also builds trust among stakeholders. This insight supports the proposition that technology-mediated trust must be integrated into models of patient-provider interactions. The implication is a theoretical refinement in how digital technologies are conceptualized within the social fabric of healthcare systems, where trust is not merely interpersonal but structurally embedded via transparent technologies such as blockchain.

From a systemic and structural perspective, several foundational issues hinder the implementation of blockchain and IoT in healthcare. First, infrastructural inadequacies represent a core challenge. As documented by Hasan et al. (2022) and further supported by Badri et al. (2023), the absence of robust communication networks significantly impairs the scalability and reliability of blockchain

solutions, particularly in remote health monitoring. Without foundational digital infrastructure, advanced technologies cannot achieve their intended impact, thus impeding progress in e-health innovations.

Regulatory inconsistency further complicates adoption. Bhatia et al. (2021) report that fragmented and often underdeveloped data protection laws contribute to public skepticism. In jurisdictions lacking comprehensive data privacy frameworks, such as those similar to the EU's GDPR, the perceived risks associated with data breaches outweigh the potential benefits of digital health platforms. Therefore, the lack of cohesive governance structures inhibits stakeholder engagement, including both patients and healthcare providers.

Education and digital literacy represent another pivotal structural barrier. As noted in the methodology and reaffirmed by Khodadadi and Towfek (2023), limited awareness of blockchain and IoT functionalities among healthcare professionals hinders successful implementation. Without adequate training, both technological and ethical nuances remain underappreciated, leading to underutilization or misapplication of these innovations. This insight calls for systemic educational reforms and the inclusion of blockchain-related modules in medical and technical curricula.

In response to these challenges, the literature proposes several actionable strategies. One significant recommendation is the adoption of blockchain-based smart contract systems to enhance data transparency and minimize fraudulent activities. Ahmed et al. (2024) present a secure prescription management model that leverages blockchain to authenticate transactions, reduce errors, and streamline communication among pharmacists, physicians, and patients. These smart contracts serve not only as regulatory mechanisms but also as instruments of trust-building within healthcare ecosystems.

Another critical recommendation is capacity building through education. Programs aimed at both end-users and healthcare providers have been shown to significantly increase technology acceptance. Khodadadi and Towfek (2023) emphasize that awareness campaigns and structured training are instrumental in overcoming psychological and procedural resistance. Their study illustrates how healthcare institutions that invest in ongoing education are more likely to adopt blockchain applications successfully, especially in high-stakes environments like emergency care or chronic disease management.

Empirical evaluations further validate the effectiveness of blockchain-based interventions. Badri et al. (2023) report that blockchain-enhanced remote patient monitoring systems are not only more secure but also yield cost efficiencies through optimized resource allocation. These systems offer improved continuity of care and reduce the need for physical consultations, which is particularly beneficial during global health crises such as the COVID-19 pandemic. The dual advantage of security and efficiency strengthens the case for wider adoption.

Despite these promising results, current research is not without limitations. Most studies are constrained by geographical focus, often limited to either highly developed or narrowly defined emerging economies. As such, there remains a critical need for cross-regional comparative research that accounts for cultural, regulatory, and infrastructural variability. For example, while European countries benefit from GDPR-aligned frameworks, many regions in Asia and Africa lack similar

legislative rigor, thereby facing unique implementation barriers (Condon et al., 2023; Ghaderi & Ghaderi, 2025).

Moreover, the majority of existing studies employ qualitative or small-sample designs, limiting their generalizability. Larger-scale quantitative studies are necessary to validate early findings and assess long-term impacts. Studies using longitudinal data could offer insights into the sustainability of blockchain-IoT integrations and track evolving user behavior over time.

Another research gap lies in the ethical and equity dimensions of technology adoption. Few studies have interrogated how blockchain and IoT might exacerbate existing disparities in healthcare access or create new forms of exclusion. There is a risk that technological determinism may obscure social inequities, whereby solutions are implemented without due consideration for marginalized groups who may lack digital access or comprehension. Future studies must adopt inclusive research methodologies that explicitly address equity, fairness, and cultural relevance.

In summary, the integration of blockchain and IoT into healthcare presents a complex yet promising frontier. The literature underscores both the transformative potential and the multifaceted challenges associated with this technological convergence. A comprehensive approach that includes robust infrastructure, coherent policy, user education, and inclusive design is essential to realizing the benefits while mitigating associated risks. Although the field is still maturing, current evidence provides a strong foundation upon which to build more resilient, transparent, and efficient healthcare systems. Continued interdisciplinary collaboration between technologists, healthcare practitioners, policymakers, and social scientists will be pivotal in advancing this agenda.

CONCLUSION

This narrative review examined the integration of blockchain technology and the Internet of Things (IoT) in the domain of healthcare data management, with a focus on security, interoperability, efficiency, and socio-technical challenges. The findings reaffirm that blockchain enhances data integrity, transparency, and patient control over personal health records, thereby strengthening public trust in digital health systems. The analysis also underscores the pivotal role of interoperability in ensuring seamless communication across healthcare platforms, while highlighting how blockchain-enabled IoT can transform patient monitoring and personal health data sharing.

Despite the optimism, this review identified systemic challenges including technological readiness gaps, economic constraints, inconsistent regulatory environments, and low digital literacy—particularly in low- and middle-income countries. These barriers hinder the adoption of advanced technologies even where technical infrastructure exists. Therefore, policy interventions that prioritize education, infrastructural investments, and data privacy protections are crucial. Implementing blockchain-based smart contracts and AI-assisted data analytics is a promising strategy to improve efficiency and resilience.

Future research should explore longitudinal, cross-country comparisons of blockchain-IoT systems in healthcare to assess their long-term impacts on clinical and operational outcomes. Furthermore, interdisciplinary investigations into user perceptions, policy harmonization, and cost-effectiveness analysis are recommended to deepen understanding and support policy formulation. Ultimately, addressing the challenges of energy efficiency, trust, and equitable access will be key to unlocking the full potential of blockchain-integrated IoT solutions in global healthcare ecosystems.

REFERENCE

Agrawal, S. and Kumar, S. (2022). Mlsmbqs: design of a machine learning based split & merge blockchain model for qosaware secure iot deployments. *International Journal of Image Graphics and Signal Processing*, 14(5), 58–71. https://doi.org/10.5815/ijigsp.2022.05.05

Ahmed, I., Turki, M., Baklouti, M., Dammak, B., & Alshahrani, A. (2024). Towards an optimized blockchain-based secure medical prescription-management system. *Future Internet*, 16(7), 243. https://doi.org/10.3390/fi16070243

Aldhyani, T., Khan, M., Almaiah, M., Alnazzawi, N., Hwaitat, A., Elhag, A., … & Alshebami, A. (2023). A secure internet of medical things framework for breast cancer detection in sustainable smart cities. *Electronics*, 12(4), 858. https://doi.org/10.3390/electronics12040858

Aldosary, M. and Alkhatib, M. (2024). Exploring the landscape: a systematic review on the issues, technologies, and solutions related to the integration of blockchain with iot. *Interciencia*. https://doi.org/10.59671/u6enr

Attkan, A. and Ranga, V. (2022). Cyber-physical security for iot networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex & Intelligent Systems*, 8(4), 3559–3591. https://doi.org/10.1007/s40747-022-00667-z

Babu, E., Rao, M., Swain, G., Nikhath, A., & Kaluri, R. (2023). Fog-sec: secure end-to-end communication in fog-enabled iot network using permissioned blockchain system. *International Journal of Network Management*, 33(5). https://doi.org/10.1002/nem.2248

Badri, N., Nasraoui, L., & Saïdane, L. (2023). A comprehensive review of blockchain integration in remote patient monitoring for e-health. *International Journal of Network Management*, 34(2). https://doi.org/10.1002/nem.2254

Barka, E., Dahmane, S., Kerrache, C., Khayat, M., & Sallabi, F. (2021). Sthm: a secured and trusted healthcare monitoring architecture using sdn and blockchain. *Electronics*, 10(15), 1787. https://doi.org/10.3390/electronics10151787

Bhatia, D., Mishra, A., & Mukherjee, M. (2021). Amalgamation of blockchain technology and internet of things for healthcare applications. In *Emerging Technologies for Healthcare Applications* (pp. 571–592). https://doi.org/10.1007/978-3-030-67490-8_22

Condon, F., Franco, P., Martínez, J., Eltamaly, A., Kim, Y., & Ahmed, M. (2023). Energyauction: iot-blockchain architecture for local peer-to-peer energy trading in a microgrid. *Sustainability*, 15(17), 13203. https://doi.org/10.3390/su151713203

Duhayyim, M., Al-Wesabi, F., Marzouk, R., Musa, A., Negm, N., Hilal, A., … & Rizwanullah, M. (2022). Integration of fog computing for health record management using blockchain technology. *Computers Materials & Continua*, 71(2), 4135–4149. https://doi.org/10.32604/cmc.2022.022336

Elkhodr, M., Khan, S., & Gide, E. (2024). A novel semantic iot middleware for secure data management: blockchain and ai-driven context awareness. *Future Internet*, 16(1), 22. https://doi.org/10.3390/fi16010022

Fatoum, H., Hanna, S., Halamka, J., Sicker, D., Spangenberg, P., & Hashmi, S. (2021). Blockchain integration with digital technology and the future of health care ecosystems: systematic review. *Journal of Medical Internet Research*, 23(11), e19846. https://doi.org/10.2196/19846

Ghaderi, Y. and Ghaderi, M. (2025). Society 5.0 in the cloud: harnessing the power of modern information technologies. *Metaverse*, 6(1), 3232. https://doi.org/10.54517/m3232

Goyal, N. (2025). Security and privacy in iot, fog, and blockchain networks. In *Trends and Applications in IoT* (pp. 371–398). https://doi.org/10.4018/979-8-3373-0300-0.ch015

Hasan, K., Chowdhury, M., Biswas, K., Ahmed, K., Islam, M., & Usman, M. (2022). A blockchain-based secure data-sharing framework for software defined wireless body area networks. *Computer Networks*, 211, 109004. https://doi.org/10.1016/j.comnet.2022.109004

K, D., Jayavadivel, R., Nachiappan, B., Mohanraj, A., Shankar, B., & Najmusher, H. (2024). Blockchain technology for secure and trustworthy iot systems. In *Blockchain and IoT Security* (pp. 39–68). https://doi.org/10.4018/979-8-3693-9616-2.ch003

Khodadadi, E. and Towfek, S. (2023). Internet of things enabled disease outbreak detection: a predictive modeling system. *JISIoT*, 10(1), 84–91. https://doi.org/10.54216/jisiot.100107

Kumar, P., Meenakshi, S., Shalini, S., Devi, S., & Boopathi, S. (2023). Soil quality prediction in context learning approaches using deep learning and blockchain for smart agriculture. In *Smart Agriculture Technologies* (pp. 1–26). https://doi.org/10.4018/978-1-6684-9151-5.ch001

Li, D., Deng, L., Cai, Z., & Souri, A. (2020). Blockchain as a service models in the internet of things management: systematic review. *Transactions on Emerging Telecommunications Technologies*, 33(4). https://doi.org/10.1002/ett.4139

Mohan, H., Shukla, K., Tightiz, L., & Padmanaban, S. (2024). Enhancing data security and privacy in energy applications: integrating iot and blockchain technologies. *Heliyon*, 10(19), e38917. https://doi.org/10.1016/j.heliyon.2024.e38917

S. Anitha, R. and Murugan, M. (2024). Privacy-preserving collaboration in blockchain-enabled iot: the synergy of modified homomorphic encryption and federated learning. *International Journal of Communication Systems*, 37(18). https://doi.org/10.1002/dac.5955

Singh, P., Sinha, P., & Raghav, A. (2023). A blockchain iot hybrid framework for security and privacy in a healthcare database network. In *Emerging Trends in IoT* (pp. 210–225). https://doi.org/10.4018/978-1-6684-6894-4.ch011

Vicoveanu, D. (2025). Patient health record smart network challenges and trends for a smarter world. *Sensors*, 25(12), 3710. https://doi.org/10.3390/s25123710