Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.070014

REVIEW

Blockchain and Emerging Technologies for Secure Data Transmission and Patient Safety: Roadmap for Next-Gen Wireless Healthcare

Urvashi Chaudhary[1,2,*], **Samikkannu Rajkumar**[3], **Dushantha Nalin K. Jayakody**[1,2,4], **Yakubu Tsado**[5] **and Bamidele Adebisi**[6]

[1]COPELABS, ECATI, Lusófona University, Campo Grande 376, Lisbon, 1749-024, Portugal
[2]INESC INOV-Lab, Lisbon, 1000-029, Portugal
[3]Department of Electronics and Communication Engineering, Chennai Institute of Technology, Chennai, India
[4]CIET/DEEE, Faculty of Engineering, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka
[5]Department of Computing & Mathematics, Manchester Metropolitan University, Manchester, UK
[6]Department of Engineering, Manchester Metropolitan University, Manchester, UK

*Corresponding Author: Urvashi Chaudhary. Email: urvashi.iitd@gmail.com

Received: 06 July 2025; Accepted: 30 March 2026; Published: 08 May 2026

ABSTRACT: This research paper explores how wireless communication has played a key role in transforming healthcare and bringing in a new era of personalized, linked, and data-driven medical services. With the proliferation of wireless healthcare applications, ensuring the security and privacy of sensitive medical data has become paramount. We discuss the potential of blockchain technology, to address challenges and to secure next-generation wireless healthcare. We have elaborated how blockchain's core characteristics, such as immutability and decentralization, can create a secure and transparent environment for sharing and storing medical data. Additionally, this paper examines how emerging technologies, like secure communication protocols and Homomorphic encryption, can be integrated with blockchain in safeguarding medical data during transmission and improving overall connectivity in healthcare environments. Furthermore, we discuss the challenges and opportunities associated with implementing blockchain technology in real-world healthcare scenarios. By employing blockchain and physical layer security techniques, healthcare providers can mitigate security risks, preserve patient privacy, and facilitate seamless connectivity, thereby fostering trust and reliability in wireless healthcare systems. Finally this paper highlights the pivotal role of wireless technology in fostering a new era of healthcare that is more patient-centric, efficient, and informed by data-driven insights.

KEYWORDS: Blockchain; 6G; internet of healthcare things (IoHTs); medical data; cryptography; physical layer security (PLS); decentralized trust; HIPAA

1 Introduction

The healthcare industry stands on the precipice of a significant transformation driven by the convergence of wireless technologies and the anticipated arrival of 6G wireless communication. 6G promises to revolutionize wireless communication by offering unprecedented data rates, ultra-low latency, and massive network capacity [1]. These advancements hold immense potential for enhancing the capabilities of next-generation wireless healthcare. The high bandwidth offered by 6G will facilitate the seamless transmission of real-time medical data, including high-resolution medical images, complex biosignals, and detailed sensor data. This will enable remote patient monitoring with exceptional granularity, allowing healthcare providers to make more informed decisions based on a more comprehensive picture of a patient's health [2,3].

The ultra-low latency promised by 6G paves the way for real-time remote surgery and other latency-sensitive medical procedures. Surgeons will be able to perform complex procedures with minimal delay, regardless of geographical boundaries, potentially improving access to specialized care for patients in remote locations [4,5]. However, the increased connectivity and data sharing in wireless healthcare systems also amplify the risks of data breaches, cyberattacks, and unauthorized access to sensitive patient information. A detailed diagram of the conceptual architecture of the blockchain infrastructure network can be visualized in Fig. 1.

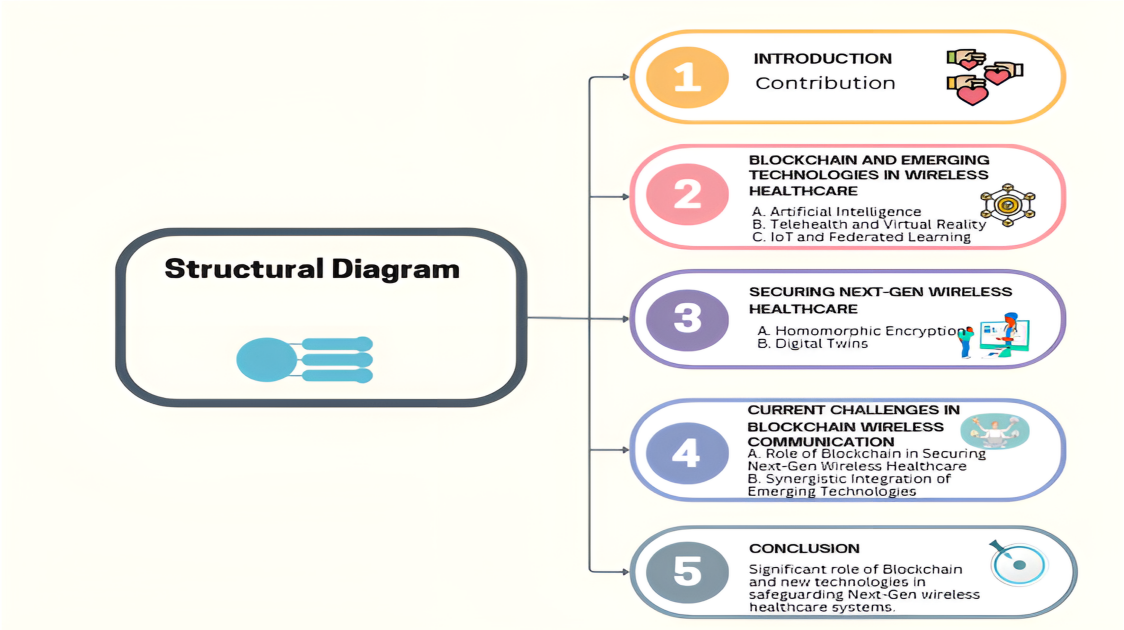

Figure 1: Blockchain-enabled next-gen wireless healthcare: structural overview.

The healthcare industry is a prime target for cyber threats due to the high value of patient data and the potential consequences of compromised information [6]. In an attempt to tackle these security issues and guarantee that wireless healthcare systems are trustworthy, researchers have focused on new technologies such as blockchain and the IoT with regard to healthcare. Blockchain, enabled through its autonomous and scripted processes, secures data communication while enabling the sharing of data in a secured environment. But the security concerns presented by healthcare over wireless will only be amplified in a 6G world, where even more data is transmitted wirelessly and has to remain safe from tampering or unauthorized access. The large number of connected devices within the 6G ecosystem will create a vast attack surface for malicious actors [7]. Therefore, exploring the integration of blockchain and other security-focused technologies with 6G infrastructure becomes even more critical for securing next-generation wireless healthcare.

Blockchain technology emerges as a beacon of hope, offering a secure and reliable foundation for next-generation wireless healthcare. Blockchain is a digital distributed ledger or database used to maintain records of transactional data that maintains the chronological sequence in which certain economic transactions have taken place across multiple computers within an open network. A blockchain that is secure means every transaction on the chain can never be altered or deleted without being detected because they are cryptographically secured. For most applications, this underlying immutability would be a critical point of differentiation, especially in healthcare, where data integrity and auditability are crucial. The health industry can benefit from the utilization of blockchain technology to create a safe and transparent location for the

storage of sensitive patient data on wireless networks that include an audit trail [8]. When combining blockchain with emerging technologies in wireless healthcare, it is important to recognize the inherent security trade-offs. For example, the integration of blockchain with IoT devices enhances immutability and auditability of patient data but can introduce latency and higher energy demands, which may hinder real-time monitoring in critical care scenarios. Similarly, coupling blockchain with AI improves the ability to detect anomalies and support predictive decision-making, yet it also raises concerns related to patient privacy, as sensitive health data must be shared for model training. In the case of 5G networks, blockchain strengthens secure data transmission across distributed infrastructures; however, scalability and interoperability challenges may emerge, especially when multiple healthcare providers and legacy systems are involved. These examples highlight that while blockchain significantly contributes to security and trust, its integration with other technologies must be carefully managed to balance performance, efficiency, and patient safety. The synergistic integration of blockchain, 6G, and IoHT is pivotal for next-generation wireless healthcare. 6G provides the foundational high-bandwidth, ultra-low-latency network (the transport layer) required for real-time IoHT data transmission, such as remote surgery and high-resolution imaging. IoHT devices (Internet of Medical Things (IoMT), wearables, and sensors) act as the data sources (the content generators), continuously generating sensitive patient data. The blockchain layer serves as the immutable security and trust backbone, cryptographically securing the data from these IoHT devices, validating transactions on the 6G network, and providing transparent, auditable access control via smart contracts. This layered approach ensures that the massive data volumes and mission-critical nature of 6G-enabled healthcare are underpinned by robust, decentralized security, directly addressing the amplified cyber risks of a highly connected ecosystem.

Fig. 2 illustrates the technical integration architecture of blockchain within next-generation wireless healthcare systems. The figure emphasizes three core components: the distributed ledger, the consensus mechanism, and smart contracts, which collectively establish the secure backbone of the proposed system. The distributed ledger ensures that patient data and medical records are stored in an immutable and decentralized manner, eliminating risks associated with single-point failures. The consensus mechanism maintains integrity and synchronization across multiple healthcare nodes, guaranteeing that only valid transactions—such as patient record updates or access requests—are recorded. Finally, smart contracts automate healthcare processes, such as granting access rights, triggering alerts during emergencies, and enforcing compliance with HIPAA/GDPR regulations. In addition, Fig. 2 contextualizes these components within specific healthcare applications, including secure data sharing between hospitals, patient-centric record management, and supply chain transparency for medical resources. This integration highlights how blockchain is not used in isolation but rather as a layered infrastructure that interoperates with wireless IoMT devices, clinical systems, and regulatory frameworks.

Blockchain plays an instrumental role in securing futuristic wireless healthcare at multiple levels. The developers of blockchain themselves do not control the data or anything else in a project. A blockchain is not like a usual centralized database in which all data is spread out at a single place, nearly to the extent that it has this syndrome of one-point failure, because here decentralized networks (miners/full nodes) hold different pieces of the pie. This ensures that there is no single point of failure—eliminating the potential risk of a cyberattack to bring down the entire system. Also, if one node is compromised, the other nodes have the data secured. By delivering a distributed on-chain approach like this, transparency and trust in the entire healthcare life science value chain are insured, as all valid parties have timely access to an auditable log of recorded patient data at their disposal [9]. If (for example) one of the nodes were to be compromised by an attacker, this means that the other part should still stay secure. By building a certified electronic health record (EHR), the healthcare system can provide accountability to the patients, as well as

interoperability and trustworthiness by ensuring that all relevant stakeholders have equal access to reliable information. Blockchain gives patients their health data powered by self-sovereign identity (SSI) solutions, enabling patients to take charge of their medical records. Patients will subsequently have the ability to provide authority to designated healthcare professionals, researchers, and other authorized authorities.

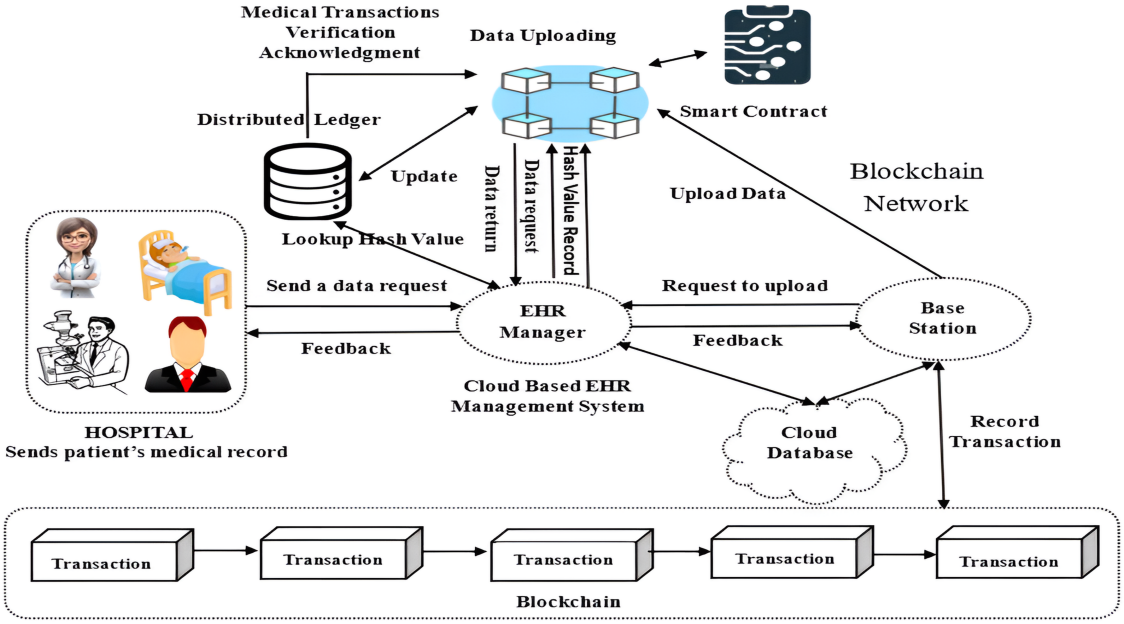

Figure 2: Integrated blockchain cloud architecture for EHR lifecycle management in healthcare.

The proposed blockchain-enabled model significantly surpasses traditional centralized systems by fundamentally enhancing trust, efficiency, and privacy. Trust is established through the core characteristics of immutability and decentralization, which eliminate a single point of failure and provide an unchangeable, cryptographically secured audit trail for all data transactions. Efficiency is improved through the implementation of smart contracts, which automate critical administrative processes such as granting access rights and triggering emergency alerts, minimizing human error and reducing the administrative burden inherent in complex, multi-stakeholder healthcare systems. Crucially, privacy is elevated via a patient-centric security paradigm; cryptographic protocols and fine-grained access control mechanisms, enforced through HIPAA/GDPR-compliant smart contracts, empower patients with control over their health data and ensure that sensitive information is only accessible by authorized parties for verifiable purposes.

The discernible nature of data access arises from the meticulous control that HIPAA-compliant APIs provide to both clinicians and patients, hence promoting patient engagement in healthcare decision-making [10]. The blockchain allows for secure and auditable data exchange between the stethoscope sensors within a wireless healthcare network.

Smart contracts are self-executing and reside on the blockchain, with predefined conditions that trigger a certain event or create an action. In the healthcare industry, smart contracts can help determine when patient data is accessed and send automatic alarms in case of critical health events, along with enabling a secure correspondence between hospital providers (healthcare services) and patients. By automating this process, potential human error is lowered, and the overall administrative burden of healthcare processes is also decreased by a lot. Blockchain technology enhances overall efficacy and scalability of wireless healthcare networks. Distributed ledger technology, such as blockchains, enables healthcare entities to create secure and

interoperable sharing platforms among multiple providers/systems. This ultimately leads to improved patient outcomes and reduced costs when the naked data atomicity barrier is removed as a seamless coordination of care. Information exchange can be achieved with less redundant entry of data by the many stakeholders involved in caring for improving clinical communications [11]. Table 1 presents the existing surveys of blockchain with technologies and their potential applications in wireless communicationstartlongtab

Table 1: A comprehensive overview of blockchain technologies and their potential applications in 6G.

Author	Advantages	Disadvantages
Blockchain for 5G/6G	The advantages for the integration of blockchain technology with 5G/6G networks include enhanced security through decentralized and immutable data storage, improved privacy by protecting sensitive user data, increased efficiency by streamlining network operations, and greater transparency by enabling auditable and verifiable transactions.	One major limitation is the scalability of blockchain networks, which can struggle to handle the massive data volumes and high transaction rates associated with 5G/6G. The high energy consumption of blockchain networks and the complexity of integrating them with existing network infrastructure pose significant hurdles.
Blockchain for AI	Blockchain technology can significantly enhance the capabilities of AI systems by providing secure, transparent, and decentralized data storage and processing. This can lead to improved AI model training, enhanced data privacy and security, and increased trust in AI-powered applications.	The scalability of blockchain networks can be a limitation, especially when dealing with large-scale AI applications that require high-throughput data processing.
Blockchain for AR and VR	Blockchain technology can enhance AR and VR experiences by providing a secure and decentralized platform for asset ownership, ensuring that digital items and experiences are verifiable and tamper-proof.	The scalability issues that can hinder performance, particularly in applications requiring real-time processing. The complexity of blockchain technology can create barriers to entry for developers and users unfamiliar with its mechanisms, potentially slowing down adoption rates.

Shadow deployment provides a valuable mechanism for testing new models and system upgrades in wireless healthcare without disrupting live services, but it also introduces notable limitations and trade-offs across technical and regulatory dimensions. From a system design perspective, sustaining parallel infrastructures increases computational overhead, bandwidth consumption, and storage demands, which may burden resource-constrained clinical settings. Synchronizing real-time patient data across production and shadow environments can also create latency, data drift, and interoperability challenges, especially in heterogeneous IoT-enabled healthcare systems. At the same time, compliance and governance issues emerge,

as duplicating sensitive health data raises concerns under regulations such as HIPAA and GDPR regarding privacy, consent, and liability in the event of errors. To ensure practical enforcement of HIPAA/GDPR compliance within the proposed blockchain-enabled wireless healthcare framework, several mechanisms are incorporated. First, smart contracts are used to embed regulatory rules and automatically enforce access permissions, consent management, and data-sharing policies. Second, HIPAA-compliant APIs and GDPR-aligned consent protocols provide fine-grained control over patient data access, with immutable audit trails that make unauthorized or non-compliant activity immediately detectable. Third, role-based and attribute-based access control (RBAC/ABAC) mechanisms are integrated into the blockchain to guarantee that only authorized personnel can access or process sensitive health data. Fourth, decentralized identity (DID/SSI) management systems empower patients to provide or revoke data access in compliance with GDPR's right-to-consent and right-to-erasure requirements. In addition, governance layers such as regulatory sandboxes and ethics committees provide oversight for evolving blockchain-enabled healthcare systems. Collectively, these mechanisms ensure that compliance is not only conceptual but also actionable and verifiable in practice. Blockchain and related emerging technologies can mitigate some of these issues by ensuring tamper-proof synchronization, immutable audit trails, and decentralized trust; however, challenges related to scalability, throughput, governance, and institutional costs remain. Consequently, shadow deployment in next-generation wireless healthcare requires a balanced strategy that considers not only technical feasibility but also compliance, patient safety, and organizational capacity.

Blockchain mitigates some of the inherent weaknesses in centralized systems because its transactions are auditable and no one is able to edit or update it without appropriate approval, all due to distributed trust processes and cryptographic principles. In the paper, more robust security features are needed due to increased use of Internet of Things devices, as shown by health service facilities. Blockchain is especially well-suited for this purpose because it can foster cooperative trust and enable secure data interaction [12]. When combined with complementary emerging technologies, blockchains have the ability to provide a scenario for a completely safe and connected healthcare environment. One example is federated learning, in which machine learning models are collaboratively trained on decentralized data sets to ensure the privacy of the data. This approach ensures that private patient data is kept within certain organizations but also allows for providers and medical researchers to utilize the anonymized population-based information [13].

To overcome blockchain's transaction throughput and latency constraints in high-volume 6G healthcare scenarios, mitigation strategies such as sharding (to enable parallel transaction validation), off-chain solutions including state channels and side chains (to process frequent interactions without burdening the main chain), and hybrid blockchain–edge/cloud architectures (to optimize resource allocation while ensuring security) can be employed. These approaches collectively enhance scalability and responsiveness, making blockchain viable for real-time, mission-critical healthcare data transmission.

Homomorphic encryption [14], which is used to enable calculations on encrypted data without decrypting them, offers a much more secure level than encryption and is so highly recommended. With this new method, healthcare professionals can analyze and share patient data with transfers without access to sensitive meanings beneath the surface. Secure multiparty computation schemes facilitate safe collaborative healthcare research and analysis by allowing multiple parties to compute a function over their private inputs without revealing the actual details of these individual records. A significant literature [15–18] has been published on the topic of blockchain-supported wireless communications. These publications extensively discuss the fundamental principles, network structure, technologies that facilitate blockchain implementation, research obstacles, and potential areas for future investigation. Furthermore, numerous studies [19–21] have thoroughly examined the reciprocal integration of blockchain and AI. The integration of blockchain and AI for wireless communications can significantly enhance network performance across many

services and applications. Several literary works have provided summaries and evaluations of the subject matter of the integration of blockchain and AI in wireless communications. In particular, very few studies have focused on the simultaneous implementation of blockchain and AI for future wireless communications. The research mentioned in reference [22] provided a limited discussion on the possibilities of combining blockchain with machine learning (ML) in wireless communication systems. In a similar vein, the study in [23] provided a concise overview of the use of reinforcement learning (RL)-empowered blockchains in Industrial IoT (IIoT) networks. Despite its promising potential, the integration of blockchain into wireless healthcare also faces notable challenges. Interoperability remains a key concern, as blockchain solutions must seamlessly integrate with heterogeneous healthcare information systems and comply with diverse standards. Furthermore, certain blockchain consensus mechanisms, particularly those based on proof-of-work, can be energy-intensive, raising sustainability and cost-related issues. Scalability is another limitation, as the high volume of real-time patient data may exceed the transaction throughput capacity of many blockchain networks, leading to latency and performance bottlenecks. Addressing these challenges is essential to ensure that blockchain adoption in healthcare is both practical and sustainable.

This paper examines the various security concerns faced by contemporary and future wireless healthcare systems, with a particular focus on how advanced innovations, including blockchain technology, can address these challenges. Here, in this rapidly changing environment of ecology, we present a holistic architecture for enhancing connectivity and securing transmission. Our analysis focuses on a secure healthcare system requirement in wireless networks of next generations and an exhaustive valuation of the pros and cons of existing security measures. This paper presents a unified view on the recent state of research in terms of security for next-generation wireless healthcare. It demonstrates the power of blockchain in modernizing data protection and interconnectedness on this platform. This will enable a greater trust between stakeholders and lead to an ecosystem that is not only stronger but also much more resistant, efficient, and patient-first, allowing them to reap the benefits of connected healthcare without compromising security or violating privacy constraints around sensitive health information.

1.1 Contributions

Our paper offers a thorough analysis and outlook on the prevailing stage of research on blockchain and emerging technologies for 6G wireless communications in comparison to the studies that have been published. We anticipate that this study will hold considerable importance in conducting more groundbreaking research in this promising field. This research paper offers several novel contributions to the burgeoning field of next-generation wireless healthcare security:

1. **Holistic Security Framework:** We propose a comprehensive security framework that moves beyond simply applying blockchain to specific healthcare use cases. We present a holistic approach that considers the interconnected nature of next-gen wireless healthcare ecosystems, addressing security challenges across data transmission, device connectivity, and stakeholder collaboration.
2. **Synergistic Integration of Emerging Technologies:** Recognizing the limitations of standalone solutions, we advocate for a synergistic integration of blockchain with other emerging technologies like federated learning, homomorphic encryption, and secure multi-party computation. This integrated approach enables a more robust and multifaceted security posture, addressing a wider range of vulnerabilities and attack vectors.
3. **Focus on Practical Implementation:** This research goes beyond theoretical frameworks by providing practical insights into the implementation challenges and opportunities associated with deploying these technologies in real-world healthcare settings. We discuss considerations related to scalability,

interoperability, regulatory compliance, and stakeholder adoption, bridging the gap between theoretical concepts and practical deployment.

4. **Patient-Centric Security Paradigm:** We emphasize a patient-centric approach to security, recognizing the importance of empowering patients with greater control over their health information. Our proposed framework prioritizes patient privacy and data ownership, ensuring that patients remain active participants in safeguarding their sensitive health data.
5. **Contribution to a Secure and Equitable Healthcare Ecosystem:** Ultimately, this research contributes to the development of a more secure, equitable, and patient-centric healthcare ecosystem. By addressing the critical security challenges hindering the widespread adoption of next-gen wireless healthcare, we aim to unlock the full potential of these transformative technologies, leading to improved patient outcomes, enhanced healthcare accessibility, and a more sustainable healthcare system.

1.2 Paper Organization

Section 1 presents the research objectives and contributions of this paper. This introduces the concept of blockchain and its potential applications in healthcare, which highlights the importance of secure data transmission and improved connectivity. Section 2 discusses the current state of wireless healthcare technologies and their limitations by exploring the challenges related to data security, privacy, and interoperability. This also reviews existing approaches to address these challenges. Section 3 presents the proposed framework for indulging blockchain to secure data transmission and improve connectivity in wireless healthcare. Discusses the key components of the framework, including smart contracts, consensus mechanisms, and cryptographic techniques. Also explains how the framework addresses the challenges identified in the background section. Section 4 identifies the key challenges faced by wireless healthcare systems, such as data security, privacy, interoperability, and connectivity, along with the potential negative consequences of these challenges. Finally, Section 5 summarizes the key findings and contributions of the paper with reinforcement and the importance of blockchain and other emerging technologies in securing next-gen wireless healthcare by outlining potential future directions and recommendations.

2 Foundations of Blockchain Integration for Secure and Efficient Wireless Healthcare Systems

2.1 Artificial Intelligence

To enhance medical research, the industry will utilize technologies, including artificial intelligence, to provide user- and customer-centric interfaces and data-driven methodologies for data processing and improved outcomes [24]. A visual representation is shown in Fig. 3 provides a clear and concise overview of the flow, which makes it easier for readers to understand the intricate relationships between different sections of blockchain and AI in wireless networks. Healthcare practitioners will access the blockchain to examine patient medical records, while AI will utilize various proposed algorithms, decision-making capabilities, and extensive data sets. Consequently, the incorporation of the latest technological advancements will yield enhanced service efficiency, diminished costs, and equitable healthcare inside the medical system. AI can facilitate the identification and prioritization of individual patients for drug monitoring and growth, which is essential for efficient medication manufacture and reduced deadlines. AI has been developed to emulate the cognitive processes of clinicians in order to understand health trends and patterns. Data is collected from multiple sources, including the patient, the radiologist, and images presented as unstructured data [25]. AI can conduct complex computational functions and rapidly assess huge volumes of patient data. Nevertheless, certain physicians remain apprehensive regarding the application of AI in healthcare, especially in roles that could affect a patient's welfare, due to the formidable capabilities of AI, which have shown that numerous dynamic and cognitive tasks can be performed more rapidly than by humans [26].

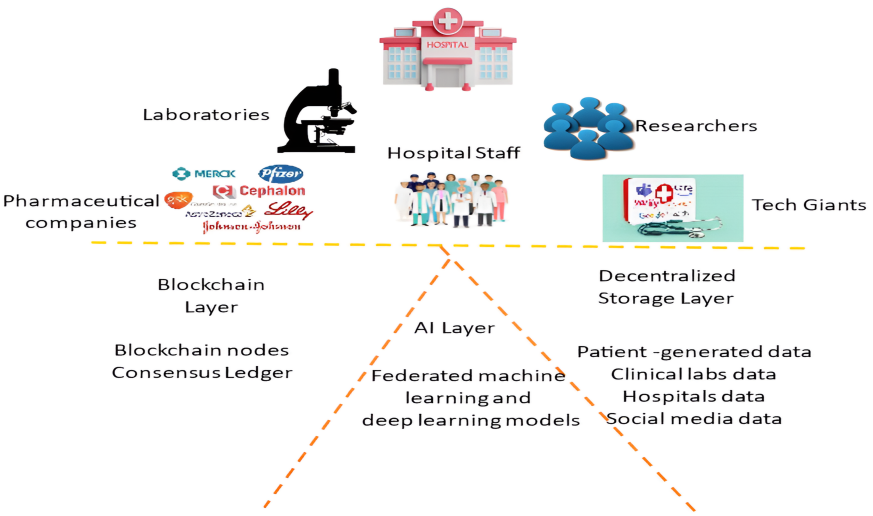

Figure 3: The integration of blockchain and AI technologies to enhance the security and efficiency.

With the advancements made in numerous industries, it appears plausible that the healthcare industry will continue to be the first to experience the positive impact of AI on individual lives that extends beyond usability. AI may identify indicators of Alzheimer's disease in brain scans prior to physicians, as indicated by a recent study published in Neurobiology of Aging, and comparative analyses of scans from healthy brains and those impacted by Alzheimer's disease are being performed using AI [27]. In chatbot counseling, the emphasis on AI undermines the reciprocity and transparency essential in the connection between mental healthcare patients and specialists. Chatbots can be utilized for purposes including setting up online follow-up appointments with a patient's doctor, and they can help customers with their treatment criteria and billing. This utilization enhances [28] patient services and offers round-the-clock assistance with basic applications such as scheduling, accounting, and various therapeutic tools, while reducing overall hospital operating expenses.

A diagram illustrates the integration of blockchain and emerging technologies in healthcare in Fig. 4. As IoT-enabled medical devices continuously generate massive streams of patient data, the challenge shifts from simple data collection to meaningful interpretation. At this point, artificial intelligence becomes indispensable, leveraging advanced analytics and learning algorithms to transform raw IoT data into actionable insights that can improve patient safety and clinical decision-making. While AI offers powerful tools for healthcare data analysis, its effectiveness is often constrained by latency and limited processing resources at the device level. To overcome these barriers, Multi-Access Edge Computing (MEC) complements AI by providing decentralized, near-patient computing power, thereby ensuring real-time analytics and secure decision support in critical healthcare scenarios. Although MEC ensures timely and efficient processing, the distributed nature of healthcare data across IoT, AI, and edge layers introduces new security and trust challenges. Blockchain addresses these concerns by enabling tamper-proof, transparent, and verifiable data transmission, thereby completing the secure foundation for next-generation wireless healthcare.

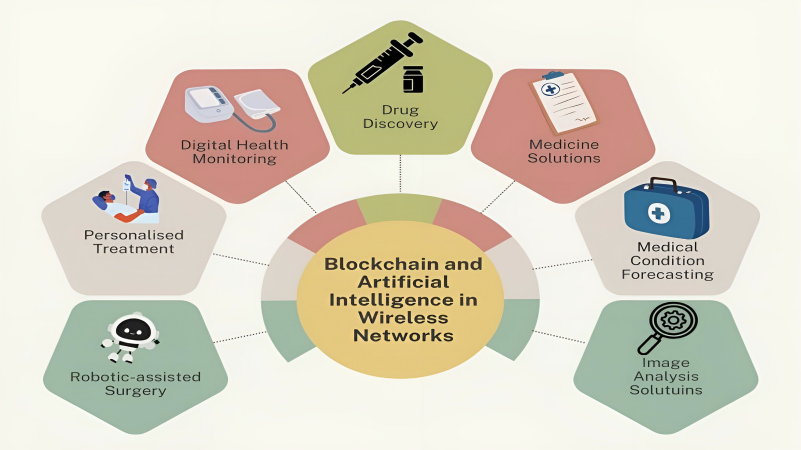

Figure 4: The integration between blockchain and AI, enables real-time monitoring & anomaly detection.

2.2 Telehealth and Virtual Reality (AR and VR)

The design of blockchain in wired communication networks utilizes the complex machinery with substantial communication resources, including allocated spectrum, transmission power, receiver sensitivity, and the quantity of communication nodes [29]. Consequently, the deterioration of power and security resulting from communication is negligible. However, this is not relevant to the rapidly evolving wireless-connected digital society, which encompasses numerous wireless devices across industries such as finance, healthcare, and supply chain, among others. Table 2 presents the security requirements for wireless communication in smart healthcare systems in medical hospitals along with wireless communication. Due to the upcoming advantages of the 6G network, most of the information exchange occurs through wireless communication [30]. AR (Augmented Reality) introduces new technologies into day-to-day lifestyle, merging virtual and physical environments. AR enables the creation of interactive experiences that demonstrate how medicines and medical devices interact with the human body. This disruptive technology offers healthcare professionals the ability to find better results within the treatment [31]. Thus AR and VR (Virtual Reality) is often combined in the discussions. AR integrates virtual objects into the real world. On the other hand, VR immerses users entirely in a virtual world environment. We require less hardware, headsets, and learning curves for AR when compared with VR.

Table 2: The critical security requirements for wireless communication in smart healthcare systems.

Technique	Description
Data Confidentiality	Ensuring that sensitive patient data remains private and inaccessible to unauthorized parties is paramount in smart healthcare.
Data Integrity	Maintaining the accuracy and reliability of healthcare data is crucial for accurate diagnosis and treatment.
Authentication and Authorization	Implements a robust authentication and authorization mechanism to prevent unauthorized access to healthcare systems and data.

(Continued)

Table 2 (continued)

Technique	Description
Channel coding	Uses error-correcting codes to make the transmitted signal more robust to noise and interference.
Non-repudiation	Establish non-repudiation so that parties cannot deny their involvement in a transaction or communication.
Interoperability	Enabling seamless communication and data exchange between different healthcare systems and devices is essential for providing comprehensive and coordinated care.
Compliance with Regulations	Adhering to relevant healthcare regulations, such as HIPAA in the United States and GDPR in the European Union, is crucial to protect data security and patient privacy.

From the late 20s, data security has become a major concern for everyone, and blockchain becomes handy in these situations. Blockchain is based on smart contracts to ensure reliable data transfer. The blockchain algorithm ensures that every node in the system preserves identical transaction content and sequence, which is the fundamental principle of blockchain technology [32]. Contact tracing involves several reliable IoMT devices utilizing various wireless connectivity technologies, including Bluetooth, LoRA, near field communication (NFC), 6G, and WiFi, to facilitate measurement through localization and positioning algorithms. Trusted edge intelligence is strategically used to improve the accuracy of blockchain data when connected with AR and VR. The blockchain-enabled system guarantees transparency in the storage and utilization of signal data, together with the processing of information, while ensuring the privacy of all users is protected [33].

There are several use cases of AR and VR in blockchain; in some domains their integration in healthcare has opened many interesting opportunities for healthcare professionals. It is observed that when AR and VR are added to blockchain-based solutions as emerging technologies, they improve the way users interact with digital content [34]. The psychological effects of interacting with 3-D environments have enhanced the effectiveness of education and training for healthcare professionals. Many avenues have been opened by VR and AR technologies for virtual market research and real-time consumer feedback. Virtual simulations allow designers to gauge reactions and preferences of different users while again helping them to provide the best user interface. Although the number of integrated use cases is somewhat limited, there is clear evidence that in the healthcare field, this technology is converging. Given the growth estimates and the benefits, it is easy to imagine that many more applications will be developed in the near future, both in software and hardware [35]. The uncertain nature of wireless networking technologies in ensuring the robustness, manageability, and cost-effectiveness of virtual network functions has brought several challenges, as indicated by Rethink Technology Ltd., research.

A detailed diagram of AI and VR/AR in a 6G wireless network in a healthcare network can be visualized in Fig. 5. The ecosystem for the adoption of 5G and making innovation in 6G has been started by many organizations on different levels. One of them is the Flagship research program in 6G, which is funded and supported by the Academy of Finland and headed by the University of Oulu. The development of 6G technology is still in its early phases, and considerable work will be required to realize the ultimate objective of

6G [36]. The principal enablers of 6G wireless networks encompass edge intelligence, homomorphic encryption, blockchain technology, and photonics-based cognition; these elements are essential for optimizing user experience in augmented and virtual reality environments.

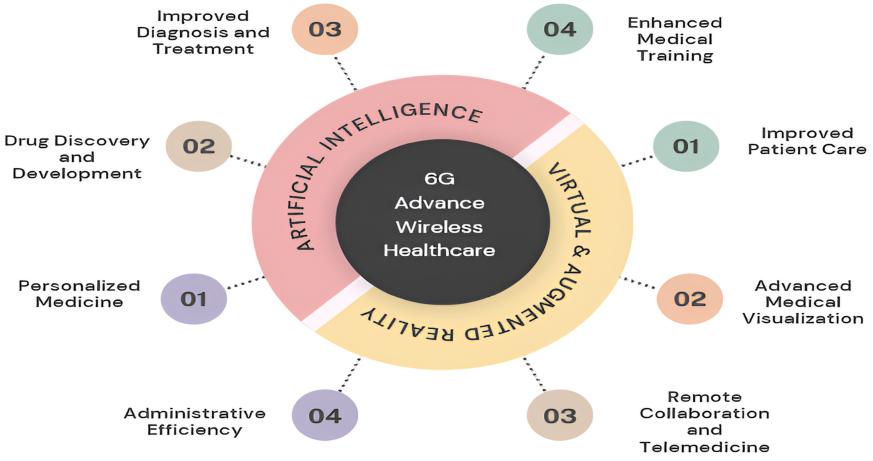

Figure 5: The emerging technologies of AI and AR/VR in the 6G wireless network framework.

The integration of smart contracts within AR and VR environments presents a transformative paradigm for secure data transmission and enhanced patient safety in next-gen wireless healthcare. Case studies illuminate the profound potential of this convergence. For instance, in remote surgical training, smart contracts can automate the licensing and secure sharing of high-fidelity AR/VR surgical simulations, ensuring only authorized medical professionals access sensitive patient data and proprietary techniques. Payment for these simulations could also be automatically disbursed upon completion and verification of training modules, all immutably recorded on the blockchain. Another compelling example lies in VR-based pain management therapies. Smart contracts could govern access to personalized VR therapeutic environments, ensuring only prescribed patients receive the specific treatment protocols [37]. Furthermore, they could securely record and timestamp patient engagement with these therapies, providing an auditable and tamper-proof log for efficacy monitoring and insurance claims, thereby bolstering patient safety by ensuring treatment fidelity and data integrity within these immersive healthcare applications.

Therefore, to address these challenges, a novel 6G architecture must be developed in the AR/VR field. Other technology similar to AR and VR, i.e., XR technology, includes MR, AR, and VR, which holds the potential to provide a fully immersive experience in 6G, surpassing the limitations of 5G's lower latency capabilities. MR, unlike augmented reality, introduces computer-generated graphical objects into the physical world, seamlessly blending the line between the real and virtual worlds. Brain-Computer Interfaces (BCI) are poised to revolutionize healthcare with the advent of 6G, alongside extended reality applications. Both domains necessitate stringent requirements, including ultra-low latency, exceptionally high data rates, and reliability, analogous to extended reality. Recent advancements have included Dynamic Spectrum Management (DSM) techniques, including Spectrum Access System (SAS), Licensed Shared Spectrum (LSA), and Dynamic Spectrum Access (DSA). These strategies enhance spectrum allocation, sensing, and sharing, hence improving the efficiency of radio spectrum management in 6G networks [38].

To ensure clarity in understanding the end-to-end data movement within the proposed architecture flow of healthcare information across the AR/VR, AI, and blockchain layers. Data acquisition begins with immersive AR/VR-enabled medical interfaces and IoMT sensors, which capture real-time physiological and contextual parameters from patients. This raw data is transmitted via secure wireless links to nearby edge

computing nodes, where preliminary AI-driven analytics, such as anomaly detection and contextual filtering, are performed to minimize communication overhead and enhance response time. The processed information is then forwarded to advanced AI modules deployed in cloud or fog environments for deep analytics, diagnostic support, and predictive modeling. Once validated, the outcomes are cryptographically hashed and stored within the blockchain ledger, where immutable records ensure provenance, authenticity, and traceability of all medical transactions. Each stage introduces distinct latency and security characteristics—AR/VR and edge layers typically incur minimal latency (1–3 ms) due to local processing, AI analytics introduce moderate computational delay (5–10 ms) depending on model complexity, and blockchain storage/verification adds cryptographic and consensus-related latency (8–15 ms). To mitigate the latter, optimization strategies such as sharding, off-chain computation, and hybrid blockchain-edge architectures are employed. This structured flow not only ensures secure and efficient data transmission but also maintains patient safety and compliance with privacy regulations throughout the entire digital healthcare ecosystem. A detailed diagram of blockchain and emerging technologies in a healthcare network can be visualized in Fig. 6.

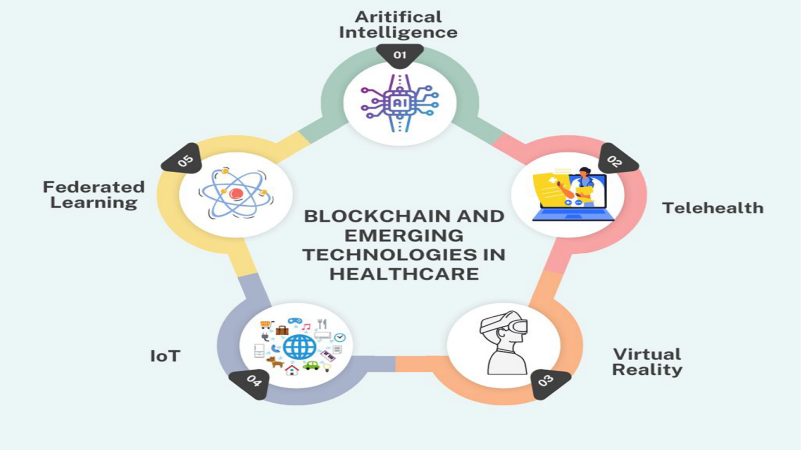

Figure 6: This diagram illustrates the integration of blockchain and emerging technologies.

2.3 IoT and Federated Learning

The most recent advancement in telecommunications is 6G communication, which is currently being developed. With each new generation of communication comes adjustments to the operating standard, norms, and communication framework. The bandwidth usage and allocation ratios for current-generation devices are optimized, reflecting insignificant communication streams and a low risk of data breaches through communication channels [39]. However, 3G, 4G, and 5G networks have limited resources and infrastructure that fall short of the theoretical spectrum calculations. Computation ratio models need to be validated through physical attribute mapping on devices commonly used in IoMT and IoT. IoT has transformed the world, driving various technological trends from Industry 1.0 to Industry 5.0, as well as advancements in AR/VR/MR, blockchain, and more [40].

Reports indicate that the IoT market in 2023 remained robust, with the number of connected IoT devices reaching approximately 16.7 billion and IoT enterprise spending around 235 billion dollars. Furthermore, while 5G focuses on ground-based communications, 6G will extend its reach to explore communications in space and the deep sea. IOT with 6G wireless communication is transforming industrial revolution 5.0 in every aspect of human life, including smart healthcare and smart education/training [41].

New forms of IOT-enabled interaction are being explored, including holographic, five-sense, and even brain-computer approaches, which will create new verticals in turn. IOT with powerful communication like 6G can improve smart healthcare systems. IoT-enabled applications will impose more stringent demands on wireless communication networks [42]. IOT with 6G will greatly enhance smart education and training systems, as innovations like holographic communications, five-sense communications, high-quality VR/AR, mobile-edge computing, and AI will contribute to creating more interactive and user-friendly learning environments for health professionals [43]. By demonstrating processes through holography and enabling interaction with objects, this approach helps future doctors retain more information, reduce costs, and avoid the risks associated with traditional training methods. Each data entry is time-stamped and encrypted in Blockchain, making unauthorized alterations nearly impossible [44]. The speed and bandwidth provided by 6G networks were leveraged to facilitate rapid and reliable data transfer, enabling seamless communication between devices and healthcare providers. As a result, patient monitoring, diagnosis, and treatment have been improved [45]. IoT is scaling for many organizations, consumer giant Nestle announced 2.8 million connected devices through the AWS IoT platform. IoT may no longer be the 'cool' buzzword it once was. In 2023, companies shifted their focus to the potential of AI, but IoT continued to scale quietly in the background. Meanwhile, the Nasdaq Composite, a key index for technology companies, rose by 43 percent in 2023 after experiencing a 33 percent decline in 2022. Not only did investors celebrate the potential peak in interest rates, but they also saw new opportunities in AI. In 2023, chip maker Nvidia saw a remarkable 246 percent gain, while Amazon, Microsoft, and Alphabet posted gains of 77 percent, 58 percent, and 57 percent, respectively, each outperforming the Nasdaq. The global GDP growth for the year was 3.0 percent, stronger than many had anticipated at the start of the year, though it still lagged behind the historical average by 0.8 percentage points. Hence, AI-enabled security protocols in healthcare are a promising feature of Reliance.

3 Securing Next-Gen Wireless Healthcare

3.1 Homomorphic Encryption

This section provides a summary of current research and approaches related to protecting patient privacy in healthcare systems based on the IoT. In recent years, blockchain technology has been utilized to safeguard the anonymity of remote data, bolstered by an integrity verification mechanism, within the information management systems of IoT [46]. This approach did not rely on any external third parties. The challenge was addressed by designing a system that leverages blockchain technology, bilinear pairings, and a cryptographic framework. This enables the efficient verification of public batches of signatures. The technology safeguards the confidentiality of data transmitted across IoT networks. Encryption techniques are widely used for safeguarding individual privacy. Homomorphic encryption has been thoroughly examined as a viable method for safeguarding data privacy in IoT healthcare applications. The homomorphic encryption framework enables data proprietors to delegate data computations to untrusted parties while safeguarding their privacy [47]. Table 3 represents the analysis of advantages of blockchain wireless communication in healthcare system. Concerns of scalability and efficiency persist in relation to homomorphic encryption. Data must be encrypted during blockchain data transmission. Outdated encryption methods used in blockchain data transmission often result in data loss due to their vulnerability to decryption. Homomorphic encryption is employed to safeguard data by allowing for the detection and correction of errors during the encryption process, thereby ensuring data integrity [48]. Fully homomorphic encryption is a distinct form of encryption. In contrast to the general homomorphic encryption algorithm, fully homomorphic encryption permits the execution of any complex operation on encrypted data without necessitating the decryption key. The complete computing procedure might be delegated to external parties. Blockchain, with its inherent openness, traceability, reliability, and decentralized nature, ensures a high level of compatibility,

confidentiality, and security in IoT applications [49]. Homomorphic encryption is utilized within the framework to provide an additional layer of security for health data. Homomorphic encryption ensures that the data remain encrypted during the training process, while blockchain provides decentralization and transparency in calculations.

Table 3: Key benefits that blockchain technology offers to the healthcare industry.

Enhanced Data Security	Blockchain enhanced the data security in healthcare by providing the decentralized and immutable ledger. This means the patient's data is distributed over the network, a number of computers, and it is difficult for the eavesdropper to locate the position of crucial data or information.
Streamlined clinical trials	Blockchain can streamline clinical trials by securely and efficiently managing patient data, consent, and trial progress. It enables real-time data sharing and analysis, accelerating the development of new treatments and therapies.
Empowered Patients	Blockchain empowers patients by granting them control over their health data. Patients can securely share their information with authorized healthcare providers, researchers, and insurers while maintaining privacy and ownership.
Reduced administrative costs	Blockchain can automate various administrative tasks in healthcare, such as claims processing, billing, and insurance verification. This reduces administrative overhead and frees up resources for patient care.

This allows for outsourcing the entire computational process, potentially reducing the cost of data encryption [50]. The data information on the blockchain is encrypted into ciphertext using a homomorphic encryption algorithm. The smart contract on the blockchain can process encrypted data without revealing the underlying plaintext information, thereby significantly enhancing user data privacy [51]. During the medical insurance claim process, third-party data users receive solely the encrypted ciphertext of the patient's EHR insurance information, which remains indecipherable due to the Paillier homomorphic encryption scheme. The insurance company also receives the encrypted EHR ciphertext but does not have access to the sensitive EHR information. Despite the limitations of Paillier encryption, it still allows for additive and subtractive homomorphic operations, thereby protecting patient EHR information propagated during data sharing and analysis [52].

Integrating blockchain-based IoT with homomorphic encryption allows us to utilize the integrated benefits of such advancements. Careful selection and utilization of their respective advantages will enable us to develop more secure IoT smart devices in the near future [53]. Ignoring fast-developing trends and emerging technologies such as blockchain and IoT has ceased to be a possibility since they are essential in shaping the future. While blockchain-based IoT systems attempt to secure and protect IoT data, they still face privacy concerns and vulnerabilities. Integrating blockchain-based IoT with homomorphic encryption has considerable promise to improve IoT data security and privacy [54].

However, research on the integration of IoT, blockchain, and homomorphic encryption remains restricted. Recent research suggests that the combination of blockchain and IoT creates a peer-to-peer

system where interactions occur in an untrusted yet auditable environment. However, few proposed solutions have focused on leveraging this technology to protect individual IoT data privacy from an end-to-end perspective [55]. Compared to traditional methods, homomorphic encryption offers a solution to security challenges in data sharing and model sharing with multiple data protection requirements. The development of homomorphic encryption while safeguarding user privacy and data security remains an ongoing challenge. The blockchain serves as a distributed data storage, eliminating the single point of trust issue, while the proposed smart contract functions as a data aggregation controller. By integrating homomorphic encryption on top of the blockchain, individuals can handle the raw data disclosure problem and the single point of trust issue and enable calculations on encrypted IoT data [56].

3.2 Digital Twins

The digital twin concept is increasingly prevalent across diverse fields, including medicine, logistics, and engineering, serving as a digital representation of both potential and actual physical assets, processes, individuals, locations, systems, and gadgets [57]. These replicas can be utilized for multiple reasons, including analysis of current events and forecasting of intervention results. The extensive data on individual lives and regular behaviors presents the potential for digital twins in healthcare, which could facilitate the study and diagnosis of various illnesses, simulate therapies or medical treatments, and forecast their outcomes [58]. Predictions may be formulated for individuals or entire groups. The implementation of digital twins in healthcare is intricately connected to the increasing accessibility of personal health data, as individuals may easily collect information regarding their biomarkers, physical activities, and general well-being [59].

Blockchain ensures transparency and responsibility through encryption and regulatory procedures. Every blockchain user is allocated to a public address, which is entirely transparent, enabling authorized individuals to access their assets and transaction history. This guarantees an unparalleled degree of accessibility in digital twins [60]. Blockchain-based access control governs all information pertaining to digital twins, including laws and regulations, in a decentralized manner, facilitating autonomous operation. Moreover, blockchain-based access control improves security via secure socket layer certificates assigned to each digital twin, with certificate information administered on blockchains [61]. The creation of digital twins on blockchain enables precise global identification and tracking. Blockchain enables digital twins to securely access distributed data sets from several places without the need for third-party intermediaries. Blockchain-based digital twins enhance record keeping, provenance tracking, and auditability by facilitating straightforward access to and monitoring of digital twins data [62]. The complete history of digital twins, from inception to the current state, may be delineated by blockchain technology. This precise provenance monitoring can be employed to examine and identify fraud in any aspect of digital twins. Big data-driven technologies process and analyze extensive data gathered from sensory sensors that monitor physical assets, facilitating digital twinning. Blockchain technology, a developing and facilitating innovation, aims to provide monitoring services for digital twins, resulting in improved security, transparency, reliability, and immutability [63].

Recent developments in digital twins and 6G mobile networks have facilitated the IIoT. A variety of edge intelligence applications, including intelligent transportation and smart cities, are expected to provide high-quality services to users within the IIoT framework. Data processing utilizing AI algorithms underpins the delivery of intelligent services within the IIoT architecture [64]. Notwithstanding these facilitating technologies and recent advancements, the divergence between the results of data analysis and the accurate depiction of the condition of their physical systems continues to provide a considerable challenge in the formulation of resilient control algorithms for the physical systems. Within this framework, the digital twin paradigm appears as a highly promising technology for 6G networks, facilitating near instantaneous

wireless connectivity and exceptionally stable communication. Enabled by digital twins, 6G networks may connect physical systems with the digital realm in real time to achieve resilient edge intelligence in IIoT [65]. Federated learning parameters are documented on the blockchain rather than the parameter server, considerably augmenting parameter security and strengthening the trustworthiness of user models.

4 Security Challenges in Blockchain Wireless Communication

The adoption of wireless communication technologies in healthcare has brought about significant benefits, such as improved patient monitoring, remote patient care, and enhanced operational efficiency. However, the increased reliance on wireless networks and connected medical devices has also introduced a new set of security challenges that must be addressed. These challenges include:

1. Data Privacy and Integrity: Healthcare data are sensitive in nature (patient records, diagnostic information, and biometrics), which needs stronger security to not let unauthorized personnel sneak into the system.
2. Device and Network Security: Wireless medical devices and their networks are exposed to a variety of cyber threats (eavesdropping, man-in-the-middle attacks, and device hijacking), jeopardizing patient safety as well as data confidentiality.
3. Interoperability and Standardization: Non-standardized security protocols and the inability for devices to effectively interoperate can leave a number of open doors from which sensitive data could be stolen in transit or interfere with the seamless exchange of said information.

   To ensure the security of these transactions, countermeasures have been applied in terms of traditional ones (i.e., encryption and access control) with their limited capacity to maintain integrity over centralized approaches that are pushed for halving emergent technologies such as blockchain.

4.1 Role of Blockchain in Securing Next-Gen Wireless Healthcare

Decentralization, transparency and immutability of the blockchain make it a potential solution to solve different security issues related to next-generation wireless healthcare [66] Their reference to the advantages of blockchain in securing wireless healthcare are related as follows: Benefits of Blockchain for Wireless Healthcare

1. Decentralized Data Management: A blockchain-based system allows the storage and management of healthcare data on a decentralized network, reducing single-point failure risk as well as modulating security against cyber threats.
2. Secure Data Transmission: Blockchain's cryptographic mechanisms (e.g., hashing and digital signatures) can preserve the integrity and confidentiality of data communication over a wireless connection, preventing unauthorized access and tampering with it.
3. Tamper-Proof Auditing: The immutability of blockchain provides an auditable, transparent, and tamper-resistant record for healthcare data exchanges, enabling traceability of the source and ensuring accountability.
4. Patient Empowerment: Blockchain-based systems, being the key to the achievement of patient empowerment, enable patients to gain better control over their health data and share this information privately and securely with healthcare providers, as well as be an active part of the data exchange protocol. Additionally, blockchain integration into next-gen wireless healthcare may promise its overall security, but combined with other emerging technologies, the application of blockchain can foster its security and quality. Table 4 represents the different IoHT International Projects and Grants funded by different international agencies in healthcare.

Table 4: Definition of acronyms and notations.

Acronym Notations	Definition	Acronym Notations	Definition
AI	Artificial Intelligence	**AR**	Augmented Reality
APIs	(Application Programming Interface)	**BCI**	Brain-Computer Interface
DSM	Cyber Physical Systems	**DSA**	Dynamic Spectrum Access
EHR	Electronic Health Record	**HIPPA**	Health Insurance Portability and Accountability Act
IoHT	(Internet of Healthcare Things	**IIoT**	Industrial Internet of Things
IoT	Internet of Things	**IoMT**	Internet of Medical Things
LoRA	Long Range	**LSA**	Long Term Evolution
ML	Machine Learning	**NFC**	Near Field Communication
PLS	Physical Layer Security	**SSI**	self sovereign identity
SAS	Spectrum Access System	**6G**	Sixth Generation Wireless Technology

4.2 Synergistic Integration of Emerging Technologies

To address the complex security challenges in next-generation wireless healthcare, a synergistic integration of blockchain with other emerging technologies is crucial [67]. A roadmap for secure wireless healthcare must integrate legal and ethical considerations alongside technical solutions. Key priorities include ensuring compliance with data protection laws such as HIPAA and GDPR, clarifying data ownership and liability in blockchain-enabled systems, and establishing enforceable guidelines for smart contracts. Ethically, frameworks for transparent consent management and equitable access should be embedded to protect patient autonomy and prevent disparities in care. Finally, adaptive governance models—such as regulatory sandboxes and ethics committees—can provide ongoing oversight as technologies and healthcare practices evolve. Some key technologies that can be co-opted with blockchain include:

1. Federated Learning: Federated learning enables collaborative model training without the need to share sensitive patient data, mitigating privacy concerns and enhancing the security of AI-driven healthcare applications
2. IoT and Edge Computing: Merging blockchain with IoT devices and edge computing can establish a firm, decentralized base for the acquisition of data from wireless medical equipment that is used in healthcare.
3. Homomorphic Encryption: Homomorphic encryption allows data to be processed while still in encrypted form, which has given a new way of secure sharing and analysis in healthcare.
4. Quantum-Resistant Cryptography: As quantum computing advances, the integration of quantum-resistant cryptographic algorithms can future-proof blockchain-based healthcare systems against emerging threats.

By leveraging the synergies between blockchain and these complementary technologies, we can create a robust and secure ecosystem for next-generation wireless healthcare, addressing the critical security challenges and paving the way for a more patient-centric, equitable, and sustainable healthcare system.

5 Conclusion

This paper has addressed the significant role of blockchain and new technologies in safeguarding next-generation wireless healthcare systems. Blockchain offers a potential opportunity for safeguarding the confidentiality, integrity, and availability of sensitive patient data by addressing the challenges of data privacy, security, and interoperability. The amalgamation of blockchain with developing technologies, including edge computing, IoT, and AI, can significantly strengthen the security and efficacy of wireless healthcare networks. Edge computing may minimize latency and enhance data processing speeds, whereas IoT equipment can facilitate real-time monitoring and data acquisition. AI can be employed for data analysis, anomaly detection, and predictive maintenance. The integration of blockchain and new technologies offers a viable pathway for enhancing the security and dependability of wireless healthcare systems. Utilizing these technologies, we can establish a more secure, efficient, and patient-centric healthcare environment.

Future research should prioritize enhancing the scalability and interoperability of blockchain networks within the healthcare ecosystem. While current blockchain solutions offer robust security, their ability to handle the immense volume of real-time data generated by ubiquitous wireless IoMT devices and diverse healthcare providers remains a challenge. Investigating advanced consensus mechanisms, sharding, and off-chain solutions will be crucial to ensure seamless and efficient data transmission. Furthermore, pursue a simulation-based model to empirically validate the proposed architecture; developing standardized protocols and APIs for integrating blockchain with legacy healthcare systems is paramount to fostering true interoperability, enabling a holistic view of patient data across disparate institutions. Another critical direction involves exploring the synergistic combination of blockchain with machine learning (ML). This fusion can facilitate intelligent data analysis on secure, immutable records for predictive diagnostics, personalized treatment plans, and drug discovery, all while maintaining patient privacy through techniques like federated learning. Research is also needed to define clear regulatory frameworks and ethical guidelines for the deployment of these technologies in healthcare, addressing concerns around data ownership, consent management, and the legal implications of automated smart contracts in clinical settings. Finally, the development of user-friendly interfaces and robust user authentication methods for both patients and healthcare professionals will be vital for widespread adoption, ensuring that the enhanced security and efficiency offered by these technologies are accessible and intuitively integrated into daily healthcare practices.

Acknowledgement: Not applicable.

Funding Statement: This work was funded by national funds through FCT—Fundação para a Ciência e a Tecnologia, I.P., under projects/supports UID/6486/2025, UID/PRR/6486/2025, and UID/PRR2/06486/2025, UIDB/04111/2025 and URLLC-UAV (2023.08191.CEECIND); by the Scheme for Promotion of Academic & Research Collaboration (SPARC), via SPARC/2024-2025/NXTG/P3524; by COFAC (Lusófona University), via QUARTZ (COFAC/ILIND/COPELABS/2/2025) & COPELABS; and by the European Commission via Marie Skłodowska-Curie Actions (MSCA) as part of the project REMARKABLE (No. 101086387).

Author Contributions: Conceptualization, Urvashi Chaudhary; methodology, Urvashi Chaudhary; validation, Urvashi Chaudhary, Sammikkannu Rajkumar and Dushantha Nalin K. Jayakody; formal analysis, Urvashi Chaudhary; resources, Urvashi Chaudhary; data curation, Urvashi Chaudhary; writing—original draft preparation, Urvashi Chaudhary; writing—review and editing, Urvashi Chaudhary, Samikkannu Rajkumar, Dushantha Nalin K. Jayakody, Yakubu Tsado and Bamidele Adebisi; visualization, Urvashi Chaudhary; supervision, Dushantha Nalin K. Jayakody and Bamidele Adebisi; funding acquisition, Dushantha Nalin K. Jayakody and Bamidele Adebisi. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Kumar A, Masud M, Alsharif MH, Gaur N, Nanthaamornphong A. Integrating 6G technology in smart hospitals: challenges and opportunities for enhanced healthcare services. Front Med. 2025;12:1534551. doi:10.3389/fmed.2025.1534551.
2. Ahad A, Jiangbina Z, Tahir M, Shayea I, Sheikh MA, Rasheed F. 6G and intelligent healthcare: taxonomy, technologies, open issues and future research directions. Internet Things. 2024;25:101068.
3. Chaudhary U, Ali MF, Kumar A, Sharma A, Jayakody DNK. Unleashing the power of wireless communication in healthcare by empowering patient care and connectivity: a comprehensive survey. IEEE Access. 2025;13(2):117239–99. doi:10.1109/access.2025.3578344.
4. Kharche S, Kharche J. 6G intelligent healthcare framework: a review on role of technologies, challenges and future directions. J Mobile Multimedia. 2023;19(3):603–44.
5. Wang C, Divakarachari PB, Jiang H. 6G-enabled intelligent healthcare transport systems: framework and resource allocation strategy. IEEE Trans Intell Transp Syst. 2025;26(10):17993–8004.
6. Vashishth TK, Sharma V, Sharma MK, Sharma R. Healthcare and smart cities applications of secure 6G infrastructure. In: Building tomorrow's smart cities with 6G infrastructure technology. Hershey, PA, USA: IGI Global Scientific Publishing; 2025. p. 399–432.
7. Arastouei N, Khan MA. 6G technology in intelligent healthcare: smart health and its security and privacy perspectives. IEEE Wirel Commun. 2025;32(1):116–21.
8. Attaran M. Blockchain technology in healthcare: challenges and opportunities. Int J Healthc Manag. 2022;15(1):70–83.
9. Ali A. Advancements and transformative applications of blockchain technology. J Eng Comput Intell Rev. 2025;3(1):36–51.
10. Ettaloui N, Arezki S, Gadi T. An overview of blockchain-based electronic health record and compliance with GDPR and HIPAA. In: The International Conference on Artificial Intelligence and Smart Environment. Cham, Switzerland: Springer; 2023. p. 405–12.
11. Thakur A. A comprehensive study of the trends and analysis of distributed ledger technology and blockchain technology in the healthcare industry. Front Blockchain. 2022;5:844834.
12. Srinivasu PN, Bhoi AK, Nayak SR, Bhutta MR, Woźniak M. Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network. Electronics. 2021;10(12):1437.
13. Javed AR, Hassan MA, Shahzad F, Ahmed W, Singh S, Baker T, et al. Integration of blockchain technology and federated learning in vehicular (IoT) networks: a comprehensive survey. Sensors. 2022;22(12):4394. doi:10.3390/s22124394.
14. Peng S, Cai Z, Liu W, Wang W, Li G, Sun Y, et al. Blockchain data secure transmission method based on homomorphic encryption. Comput Intell Neurosci. 2022;2022(1):3406228.
15. Wang J, Ling X, Le Y, Huang Y, You X. Blockchain-enabled wireless communications: a new paradigm towards 6G. Natl Sci Rev. 2021;8(9):nwab069. doi:10.1093/nsr/nwab069.
16. Wu M, Wang K, Cai X, Guo S, Guo M, Rong C. A comprehensive survey of blockchain: from theory to IoT applications and beyond. IEEE Internet Things J. 2019;6(5):8114–54.
17. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for 5G and beyond networks: a state of the art survey. J Netw Comput Appl. 2020;166:102693.
18. Yue K, Zhang Y, Chen Y, Li Y, Zhao L, Rong C, et al. A survey of decentralizing applications via blockchain: the 5G and beyond perspective. IEEE Commun Surv Tutor. 2021;23(4):2191–217.
19. Shafay M, Ahmad RW, Salah K, Yaqoob I, Jayaraman R, Omar M. Blockchain for deep learning: review and open challenges. Cluster Comput. 2023;26(1):197–221. doi:10.36227/techrxiv.16823140.v1.

20. Wang R, Luo M, Wen Y, Wang L, Raymond Choo KK, He D. The applications of blockchain in artificial intelligence. Secur Commun Netw. 2021;2021(1):6126247.
21. Pandl KD, Thiebes S, Schmidt-Kraepelin M, Sunyaev A. On the convergence of artificial intelligence and distributed ledger technology: a scoping review and future research agenda. IEEE Access. 2020;8:57075–95. doi:10.1109/access.2020.2981447.
22. Liu Y, Yu FR, Li X, Ji H, Leung VC. Blockchain and machine learning for communications and networking systems. IEEE Commun Surv Tutor. 2020;22(2):1392–431.
23. Jameel F, Javaid U, Khan WU, Aman MN, Pervaiz H, Jäntti R. Reinforcement learning in blockchain-enabled IIoT networks: a survey of recent advances and open challenges. Sustainability. 2020;12(12):5161.
24. Kuznetsov O, Sernani P, Romeo L, Frontoni E, Mancini A. On the integration of artificial intelligence and blockchain technology: a perspective about security. IEEE Access. 2024;12:3881–97. doi:10.1109/access.2023.3349019.
25. Hussain I. AI in healthcare, data analytics, block chain, cybersecurity, and machinelLearning. Glob Trends Sci Technol. 2026;2(1):75–93.
26. Pablo RGJ, Roberto DP, Victor SU, Isabel GR, Paul C, Elizabeth OR. Big data in the healthcare system: a synergy with artificial intelligence and blockchain technology. J Integr Bioinform. 2022;19(1):20200035. doi:10.1515/jib-2020-0035.
27. Pilozzi A, Huang X. Overcoming Alzheimer's disease stigma by leveraging artificial intelligence and blockchain technologies. Brain Sci. 2020;10(3):183. doi:10.3390/brainsci10030183.
28. Verma P, Rao CM, Chapalamadugu PK, Tiwari R, Upadhyay S. Future of electronic healthcare management: blockchain and artificial intelligence integration. In: Next-generation cybersecurity: AI, ML, and blockchain. Cham, Switzerland: Springer; 2024. p. 179–218.
29. Vetrivel S, Mohanasundaram T. Blockchain-empowered metaverse healthcare systems and applications. In: Malviya R, Sundram S, Dhanaraj RK, Kadry S, editors. Digital transformation in healthcare 50: volume 2: metaverse, nanorobots and machine learning. Berlin, Germany: De Gruyter; 2024. p. 61–88.
30. Rajeswari P, Gobinath A, Suresh Kumar N, Anandan M. The impact of 5G and 6G on healthcare. In: Smart hospitals: 5G, 6G and moving beyond connectivity. Hoboken, NJ, USA: John Wiley & Sons; 2024. p. 107–24.
31. Garg H, Somkuwar VU. AR/VR telehealth platforms for remote procedural training. In: Extended reality for healthcare systems. Amsterdam, The Netherlands: Elsevier; 2023. p. 127–43.
32. Rana SK, Rana SK, Rana AK, Nisar K, Soomro TR, Nisar S. A survey on blockchain technology supported approaches for healthcare system, open issues and challenges. In: 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS). Piscataway, NJ, USA: IEEE; 2022. p. 1–7.
33. Indumathi J, Shankar A, Ghalib MR, Gitanjali J, Hua Q, Wen Z, et al. Block chain based internet of medical things for uninterrupted, ubiquitous, user-friendly, unflappable, unblemished, unlimited health care services (BC IoMT U 6 HCS). IEEE Access. 2020;8:216856–72. doi:10.1109/access.2020.3040240.
34. Rane N, Choudhary S, Rane J. Enhanced product design and development using artificial intelligence (AI), virtual reality (VR), augmented reality (AR), 4D/5D/6D printing, internet of things (IoT), and blockchain: a review. SSRN Electron J. 2023;2021(7):1–24. doi:10.2139/ssrn.4644059.
35. Gadekallu TR, Wang W, Yenduri G, Ranaweera P, Pham QV, da Costa DB, et al. Blockchain for the metaverse: a review. Future Gener Comput Syst. 2023;143(9):401–19. doi:10.1016/j.future.2023.02.008.
36. Chaudhary U, Ali MF, Rajkumar S, Jayakody DNK. Sensing and secure NOMA-assisted mMTC wireless networks. Electronics. 2023;12(10):2322. doi:10.3390/electronics12102322.
37. Bodkhe U, Verma A, Saraswat D, Bhattacharya P, Tanwar S. Adoption of blockchain for data privacy in 6G-envisioned augmented reality: opportunities and challenges. In: Emerging Technologies for Computing, Communication and Smart Cities: Proceedings of ETCCS 2021. Singapore: Springer Nature; 2022. p. 519–32.
38. Zhu HY, Hieu NQ, Hoang DT, Nguyen DN, Lin CT. A human-centric metaverse enabled by brain-computer interface: a survey. IEEE Commun Surv Tutor. 2024;26(3):2120–45. doi:10.1109/comst.2024.3387124.

39. Javeed D, Saeed MS, Ahmad I, Adil M, Kumar P, Islam AN. Quantum-empowered federated learning and 6G wireless networks for IoT security: concept, challenges and future directions. Future Gener Comput Syst. 2024;160(1):577–97. doi:10.1016/j.future.2024.06.023.
40. Quy VK, Nguyen DC, Van Anh D, Quy NM. Federated learning for green and sustainable 6G IIoT applications. Internet Things. 2024;25(2):101061. doi:10.1016/j.iot.2024.101061.
41. Alotaibi A, Barnawi A. Securing massive IoT in 6G: recent solutions, architectures, future directions. Internet Things. 2023;22:100715.
42. Yu H, Taleb T, Samdanis K, Song J. Toward supporting holographic services over deterministic 6G integrated terrestrial and non-terrestrial networks. IEEE Network. 2023;38(1):262–71. doi:10.1109/mnet.133.2200509.
43. Ahmad HF, Rafique W, Rasool RU, Alhumam A, Anwar Z, Qadir J. Leveraging 6G, extended reality, and IoT big data analytics for healthcare: a review. Comput Sci Rev. 2023;48(3):100558. doi:10.1016/j.cosrev.2023.100558.
44. Tyagi AK, Tiwari S. Blockchain-enabled smart healthcare applications in 6G networks. In: Digital twin and blockchain for smart cities. Hoboken, NJ, USA: John Wiley & Sons, Inc.; 2024. p. 459–94.
45. Jahid A, Alsharif MH, Hall TJ. The convergence of blockchain, IoT and 6G: potential, opportunities, challenges and research roadmap. J Netw Comput Appl. 2023;217(3):103677. doi:10.1016/j.jnca.2023.103677.
46. Abiodun KM, Adeniyi EA, Awotunde JB, Chakraborty C, Aremu DR, Adebiyi AA, et al. Blockchain and internet of things in healthcare systems: prospects, issues, and challenges. In: Digital health transformation with blockchain and artificial intelligence. Boca Raton, FL, USA: CRC Press; 2022. p. 1–22.
47. Munjal K, Bhatia R. A systematic review of homomorphic encryption and its contributions in healthcare industry. Complex Intell Syst. 2023;9(4):3759–86. doi:10.1007/s40747-022-00756-z.
48. Kumar R, Kumar J, Khan AA, Ali H, Bernard CM, Khan RU, et al. Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images. Comput Med Imaging Graph. 2022;102(5):102139. doi:10.1016/j.compmedimag.2022.102139.
49. Chen J, Li K, Philip SY. Privacy-preserving deep learning model for decentralized VANETs using fully homomorphic encryption and blockchain. IEEE Trans Intell Transp Syst. 2021;23(8):11633–42. doi:10.1109/tits.2021.3105682.
50. Choi KA. Integrating homomorphic encryption with blockchain for privacy preserving communication on the internet of vehicles. J Mach Comput. 2025;5(1):331–42. doi:10.53759/7669/jmc202505025.
51. Xu G, Zhang J, Cliff UGO, Ma C. An efficient blockchain-based privacy-presrving scheme with attribute and homomorphic encryption. Int J Intell Syst. 2022;37(12):10715–50.
52. Ma Z, Wang J, Gai K, Duan P, Zhang Y, Luo S. Fully homomorphic encryption-based privacy-preserving scheme for cross edge blockchain network. J Syst Archit. 2023;134(2):102782. doi:10.1016/j.sysarc.2022.102782.
53. Vanin FNDS, Policarpo LM, Righi RDR, Heck SM, da Silva VF, Goldim J, et al. A blockchain-based end-to-end data protection model for personal health records sharing: a fully homomorphic encryption approach. Sensors. 2022;23(1):14. doi:10.3390/s23010014.
54. Ali A, Pasha MF, Guerrieri A, Guzzo A, Sun X, Saeed A, et al. A novel homomorphic encryption and consortium blockchain-based hybrid deep learning model for industrial internet of medical things. IEEE Trans Netw Sci Eng. 2023;10(5):2402–18. doi:10.1109/tnse.2023.3285070.
55. Yang X, Xing C. Federated medical learning framework based on blockchain and homomorphic encryption. Wirel Commun Mob Comput. 2024;2024(1):8138644. doi:10.1155/2024/8138644.
56. Wu X, Wang J, Zhang T. Integrating fully homomorphic encryption to enhance the security of blockchain applications. Future Gener Comput Syst. 2024;161(5):467–77. doi:10.1016/j.future.2024.07.015.
57. Jiang Y, Yin S, Li K, Luo H, Kaynak O. Industrial applications of digital twins. Philos Trans R Soc A. 2021;379(2207):20200360. doi:10.1098/rsta.2020.0360.
58. Alazab M, Khan LU, Koppu S, Ramu SP, Iyapparaja M, Boobalan P, et al. Digital twins for healthcare 4.0—recent advances, architecture, and open challenges. IEEE Consum Electron Mag. 2022;12(6):29–37. doi:10.1109/mce.2022.3208986.
59. Kaul R, Ossai C, Forkan ARM, Jayaraman PP, Zelcer J, Vaughan S, et al. The role of AI for developing digital twins in healthcare: the case of cancer care. Wiley Interdiscip Rev: Data Min Knowl Discov. 2023;13(1):e1480.

60. Akash SS, Ferdous MS. A blockchain based system for healthcare digital twin. IEEE Access. 2022;10(6):50523–47. doi:10.1109/access.2022.3173617.
61. Lu Q, Chen L, Xie X, Fang Z, Ye Z, Pitt M. Framing blockchain-integrated digital twins for emergent healthcare: a proof of concept. In: Proceedings of the Institution of Civil Engineers-Engineering Sustainability. Leeds, UK: Emerald Publishing Limited; 2023. Vol. 176, p. 228–43.
62. Hemdan EED, El-Shafai W, Sayed A. Integrating digital twins with IoT-based blockchain: concept, architecture, challenges, and future scope. Wirel Pers Commun. 2023;131(3):2193–216. doi:10.1007/s11277-023-10538-6.
63. Narigina M, Romanovs A, Bruzgiene R. Digital twin technology in healthcare: a literature review. In: 2024 IEEE 11th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE). Piscataway, NJ, USA: IEEE; 2024. p. 1–8.
64. Moztarzadeh O, Jamshidi M, Sargolzaei S, Keikhaee F, Jamshidi A, Shadroo S, et al. Metaverse and medical diagnosis: a blockchain-based digital twinning approach based on MobileNetV2 algorithm for cervical vertebral maturation. Diagnostics. 2023;13(8):1485.
65. Kamel Boulos MN, Zhang P. Digital twins: from personalised medicine to precision public health. J Pers Med. 2021;11(8):745. doi:10.3390/jpm11080745.
66. Dash J, Barekar SS, Borhade RR, Ikhar S, Afaq A, Bendale SP. Next-gen security: leveraging advanced technologies for social medical public healthcare resilience. South East Eur J Public Health. 2024;XXIII(1):35–51.
67. Rangarajan D, Rangarajan A, Reddy CKK, Doss S. Exploring the next-gen transformations in healthcare through the impact of AI and IoT. In: Intelligent systems and IoT applications in clinical health. Hershey, PA, USA: IGI Global; 2025. p. 73–98.