Vol.3, No.1, Page 577- 586, 2025 https://doi.org/10.59628/jast.v3i1.1297 ISSN 2958-9568 JAST

SUN PUBLISHER

مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا

Sana'a University Journal of Applied Sciences and Technology

https://journals.su.edu.ye/index.php/jast/

Blockchain-IoT Healthcare Applications and Trends: Review

Ammar T. Zahary * and Wafaa A. N. A. AL-Nbhany

Department of Information Technology, Faculty of Computer and Information Technology, University of Sana'a, Sana'a, Yemen

*Corresponding author: Zahary@su.edu.ye

Abstract

The combination of IoT (Internet of Things) and blockchain technology in healthcare has garnered significant interest due to its potential to improve data security, privacy, and overall efficiency within the sector. IoT facilitates continuous patient monitoring through interconnected medical devices that gather and transmit health data in real-time. Given the sensitivity of this data, robust security measures are crucial to prevent unauthorized access and maintain data integrity. Blockchain technology provides a decentralized and unalterable ledger system that can effectively mitigate these security concerns by ensuring that all data transactions are encrypted, time-stamped, and accessible only to authorized users. This paper examines the complementary advantages of integrating IoT and blockchain in healthcare, addressing the challenges and proposing solutions for their implementation. The discussion includes a review of existing frameworks and case studies that highlight the practical application with these contributions.

Article Info

Keywords:
IOT, BIOT, IOMT, IOT healthcare Methodology, Blockchain-IOT Trends

Article History:
Received: 1-October-2024,
Revised: 13-December-2024,
Accepted: 20-January-2025,
Available online: 28 February 2025.

1. INTRODUCTION

IoT-based healthcare offers significant advantages such as lowering the costs associated with hospital visits, transportation, and human resources [1]. In recent years, sensors and Internet of Things (IoT) technology have enabled the collection of diverse data for various purposes. Individuals now use wearable devices to track personal health and behavioral data, and are increasingly taking steps to personalize their healthcare services using smart sensors and devices. [2]. With the growing popularity of IoT technology, ensuring the security and privacy of the diverse data produced by IoT devices has become increasingly important. This is because IoT devices often generate extremely sensitive information such as video and audio from smart surveillance systems, location and activity patterns, medical data from fitness devices, and even daily routines of family members at home [3]. The growing use of IoT devices has resulted in larger volumes of data, thereby raising concerns regarding confidentiality and privacy. To address these challenges, the authors integrated blockchain with the IoT to ensure data confidentiality and security. Blockchain is employed with IoT to safeguard confidentiality and trust through its inherent features such as decentralization, distribution, and encryption. [4]. Most IoT solutions are typically centralized, depending on cloud computing for data storage and services. By contrast, blockchain offers a decentralized distributed ledger that ensures secure data sharing and decentralized network governance, making it resistant to tampering [5]. Blockchain is a technology that facilitates transparency and secures data storage and transmission without requiring central authority. It also serves as a platform for executing smart contracts; that is, automated procedures are triggered when specific conditions are met. Owing to its key features, such as decentralization, security, and distribution, blockchain has gained significant popularity across many sectors. The decentralized nature of the blockchain eliminates the need for a central governing authority. The data were stored and verified using a consensus process, and the ledger was shared and maintained by all nodes in the network. Blockchain security relies on several principles, including cryptography, consensus algorithms, immutability, data replication, and traceability [6]. In information technology, encryption involves transforming data and

files from their original readable formats into different encoded formats. [7]. A blockchain system can be viewed as a distributed network managed by multiple nodes in a peer-to-peer setup. Its primary function is to achieve state-machine replication of valid data (typically transactions) across participating nodes, using a designated consensus mechanism [8]. Blockchain is a straightforward, transformative technology. Platforms such as Bitcoin and Ethereum have the potential to revolutionize healthcare by distributing records across multiple computers globally, rather than relying on a single, vulnerable server. This decentralized ledger reduces single points of failure and enhances privacy protection for sensitive medical data such as electronic health records (EHRs). Consequently, blockchains can enhance healthcare by improving security, transparency, and efficiency. However, despite its many benefits, the incorporation of blockchain into the existing infrastructure remains challenging.[9] Multiple blockchain frameworks have emerged that offer flexible and adaptable platforms to support a wide range of applications. These include Hyperledger Fabric, Ethereum, Corda, Omni, Ripple, MultiChain, Open Chain, and Chain Core [10]. A blockchain is an integrated system that combines multiple technologies. It has been enhanced from various perspectives, such as the use of lightning network technology to boost blockchain performance, cross-chain technology to enable interactions between different blockchains, and zero-knowledge proof technology to safeguard privacy. These innovations are designed to strengthen the key features of blockchain, including decentralization, traceability, tamper resistance, high reliability, and availability. [11] Blockchain can be categorized into two types: permissionless and permissioned. Permissionless or public blockchains such as Bitcoin and Ethereum allow anyone to join and participate in the consensus process without the need for permission. On the other hand, permissioned blockchains, also known as private or consortium blockchains, such as Hyperledger and Quorum, require prior authorization to join the network and participate in the consensus process. Permissioned blockchains are particularly useful when limiting access and participation, particularly for handling sensitive data, as is often the case in the medical and healthcare sectors [12]. To modernize traditional healthcare practices, blockchain technology offers a promising model for tackling critical challenges. Its immutability and structure make it a potential solution, as each block contains a specific summary of the previous block, secured by a hash value, sequence, timestamp, and trade details that cannot be tampered with or modified [13]. Blockchain technology serves as the core mechanism for securely storing and transferring data, making it a reliable foundation for creating trusted and intelligent healthcare systems. [14]. Blockchain technology has various applications, including asset transfers such as money, securities, and stocks; enhancing supply chain processes with improved traceability of goods and products; and securing sensitive data, such as in voting, healthcare, and academic credentials [15]. Numerous studies have explored the integration of the blockchain technology into the IoT context. Notably, many of these focus on its application in healthcare, whether for public health management, medical research utilizing patient data, or ensuring quality control in drug production. [16]. Internet of Medical Things (IoMT) refers to a connected network of smart medical devices integrated with applications, healthcare services, and systems. These devices and applications are connected to healthcare systems via the internet. Key challenges in IoT, particularly in IoMT, include ensuring patient data privacy and security, scalability, and data accessibility. Blockchain has the potential to revolutionize how patient data are accessed, exchanged, stored, managed, and shared [17]. The Internet of Medical Things (IoMT) is an expanding field within IoT applications, where medical devices are utilized to deliver various healthcare services [18]. As the Internet of Things (IoT) continues to advance, medical sensors are increasingly being used for health monitoring. The vast amount of data generated by these sensors must be securely recorded and transmitted to ensure timely actions in critical patient situations. Moreover, the privacy of users' personal information must be protected and health records must be stored securely. The ownership details of IoT devices should be electronically stored to prevent counterfeit activities. Blockchain, an emerging distributed and transparent technology, offers a trusted and immutable transaction record [19]. IoT devices used in healthcare handle sensitive data that require the protection of confidentiality and privacy. The centralized architecture of the IoT poses significant challenges to the security and confidentiality of these data. Traditional cryptographic methods to safeguard healthcare information introduce certain risks. Therefore, a decentralized approach for ensuring security is necessary. Blockchain offers a potential solution by encrypting the stored data and digitally signing each block, thereby providing an important level of authenticity. It is particularly suitable for the healthcare sector, where numerous participants are involved and trust is crucial. Blockchain is ideal for highly distributed applications because tracking activities and ensuring data reliability are essential [20]. The General Data Protection Regulation (GDPR) establishes a universal framework for protecting personal data, which is defined as any information that can identify an individual. Applicable to entities handling such data, regardless of location, GDPR governs data privacy within the European Union (EU) and the European Economic Area (EEA) and oversees data transfers beyond these regions. It outlines principles such as consent, transparency, purpose limitation, data minimization, privacy-by-design, accountability, and data breach protection, with relevance to healthcare organizations handling sensitive information. The Health

Insurance Portability and Accountability Act (HIPAA), enacted in 1996, sets national standards for safeguarding Protected Health Information (PHI) in the U.S. It ensures secure data handling, restricts unauthorized access, and prevents the misuse of health information. HIPAA also guarantees continuity of healthcare access by preserving insurance coverage during employment transitions. Title II of HIPAA focuses on enhancing healthcare system efficiency, protecting sensitive health data, and reinforcing patient privacy, security, and ethical accountability in healthcare practices.[21]. This paper reviews blockchain-IoT healthcare applications, and analyze them in terms of blockchain IOT healthcare applications, contributions, challenges, and solutions.

2. METHODOLOGY

The blockchain-IoT has the potential to revolutionize applications owing to its key features, such as enhanced security, elimination of third-party involvement, and transparency. In this paper, our approach involves reviewing and gathering recent studies on blockchain-IoT in healthcare applications and then summarizing the contributions, challenges, and solutions to provide a comprehensive understanding of blockchain-IoT in the healthcare sector.

3. IOT

The Internet of Things (IoT) has undergone significant expansion, with applications in smart cities, self-driving vehicles, wearable technologies, online commerce, and healthcare. This evolution has brought transformative changes to healthcare, particularly through Remote Patient Monitoring (RPM). RPM leverages wearable devices to remotely monitor patients' health, enhance the quality of care, reduce appointment costs and frequency, and enable prompt diagnosis and treatment.

Devices used in RPM are categorized as follows: Stationary Devices: Fixed-location systems, such as those used for remote chemotherapy. Embedded Devices: Devices implanted within the body, such as deep brain stimulators. Wearable Devices: Body-worn portable technologies such as insulin pumps. These advancements in the IoT have streamlined healthcare delivery, making them more efficient and widely accessible [19]. IoT devices such as wearable sensors and implantable medical devices enable Remote Patient Monitoring (RPM), real-time health data collection, and disease prediction [4, 12, 15]. IoMT systems improve healthcare delivery by providing secure data transmission and enhancing the interoperability among devices and systems [5, 16, 17]. These advancements have led to applications in drug traceability, patient tracking, and telemedicine [9, 12, 14].

4. BLOCKCHAIN

Blockchain, a decentralized Distributed Ledger Technology (DLT), ensures secure and reliable record keeping. Introduced in 2008, it has expanded beyond Bitcoin to revolutionize industries, such as supply chains, healthcare, energy, and public services. Its key advantage is that a publicly distributed ledger replicates across all network nodes, enabling secure, anonymous transactions verified through cryptographic algorithms without central authorities. Various adaptable blockchain platforms, including Hyperledger Fabric, Ethereum, and Ripple, support diverse applications [10]. Blockchain technology offers decentralized, immutable, and secure data management systems. Hyperledger Fabric and Ethereum are widely used to store and manage Electronic Health Records (EHR) and facilitate secure access to patient data [1, 9, 13]. Smart contracts provide automated and auditable access control, enhance data privacy, and reduce reliance on intermediaries [2, 8, 16]. Hybrid storage models, such as combining interplanetary file systems (IPFS) for off-chain storage with blockchain for metadata, have addressed scalability issues in managing large datasets [6, 7, 14].

5. INTEGRATION BLOCKCHAIN WITH IOT

The integration of blockchain technology with the Internet of Things (IoT) has the potential to bring transformative changes across various sectors, introducing new operational models and needing a reevaluation of existing systems and processes. Blockchain can enhance IoT adoption by providing robust security for user data and ensuring privacy protection [16]. The integration of blockchain with the IoT enhances healthcare data security, scalability, and accessibility. For example, Attribute-Based Access Control (ABAC) integrated with Hyperledger Fabric eliminates the need for centralized access lists and provides fine-grained, decentralized access control [3, 5, 7]. Lightweight consensus mechanisms, such as Proof of Authority (PoA) and RAFT, reduce computational overhead for IoT devices, enabling real-time healthcare applications [1, 18].

The integration of Blockchain and the Internet of Things (IoT) in healthcare has garnered substantial attention in recent years, leading to advancements in secure data management, decentralized access control, and enhanced scalability. This review outlines the key contributions, applications, challenges, and solutions.

6. BIOT HEALTHCARE APPLICATIONS, CONTRIBUTIONS, CHALLENGES, AND SOLUTIONS

In [1], the authors designed a distributed user authentication and access control scheme for IoT-based healthcare utilizing local gateways integrated with Ethereum blockchain smart contracts. These gateways manage multiple IoT devices, enhancing scalability by offloading resource-intensive tasks, such as authentication and blockchain communication. This study contributes a decentralized access control framework that manages both static and dynamic access rights validation, and addresses challenges such as scalability and computational limitations through token-based access control and a hybrid on-chain/off-chain model.

Similarly, [2] proposed the Individual-Initiated Auditable Access Control (IIAAC) model, which integrates blockchain, Ciphertext-Policy Attribute-Based Encryption (CP-ABE), and Interplanetary File System (IPFS). This model allows individuals to control access to their personal health data (PHD), ensuring privacy preservation through encryption and blockchain immutability. The key contributions include individual-initiated control and auditable access control, addressing challenges such as fine-grained access control and data privacy during sharing using CP-ABE and robust audit mechanisms.

In [3], an Attribute-Based Access Control model using a Hyperledger Fabric blockchain (ABAC-HLFBC) was introduced. By adopting ABAC, the need for access control lists (ACLs) and role assignments is eliminated, thus granting access based on user attributes. This study contributes to securing sensitive data from healthcare IoT devices and enhances performance using the Raft consensus mechanism. Challenges, such as managing access control for numerous IoT devices and ensuring data security, are addressed through decentralized access management and the ABAC model for flexible, scalable access control.

The review paper in [4] examined various healthcare applications utilizing blockchain and IoT, such as Remote Patient Monitoring (RPM), patient tracking, disease prediction, and fighting COVID-19. This study highlights key contributions, such as improving data security, privacy, and decentralized access control for sensitive healthcare data. It discusses challenges such as maintaining data privacy and scalability limitations, proposing solutions such as decentralized data storage using hybrid models, and the use of permission blockchains to restrict access to sensitive data.

In [5], the authors integrated a Hyperledger Fabric blockchain with IoT devices to demonstrate access control and establish a root of trust. Using Raspberry Pi 4 Model B as an IoT device, they implemented an attribute-based access control (ABAC) mechanism to manage permissions. This study contributes by showing how blockchain can secure data management in healthcare settings and address challenges such as performance constraints of IoT devices through programmatic access control in chain code and lightweight blockchain protocols.

The work in [6] focused on enhancing security and privacy in healthcare systems for remote monitoring of chronic diseases. By utilizing proxy re-encryption combined with blockchain and storing health data off-chain in an IPFS, this study addresses challenges related to data privacy and scalability. The Proof of Authority (PoA) consensus mechanism is adopted to improve the processing speed, contributing to faster data processing for real-time healthcare applications.

In [8], a framework for access control was presented, allowing the exploration of new blockchain-based solutions to address security and performance issues. This study highlights applications such as IoT-based healthcare, where blockchain manages access control for devices that monitor patient health. These contributions include blockchain-enabled access control systems and the integration of ABAC for fine-grained control, addressing challenges such as scalability and privacy concerns through solutions such as sharding and smart contracts.

The authors of [9] reviewed popular blockchain networks such as Ethereum and Hyperledger Fabric for data exchange in healthcare. This study explored applications such as secure health data exchange, patient consent management, and drug supply chain oversight. It highlights the blockchain's ability to manage sensitive health data securely and addresses challenges such as scalability and patient data privacy by proposing solutions such as off-chain storage systems and efficient consensus mechanisms.

In [12], a review categorized healthcare applications integrating IoT and blockchain technologies, focusing on RPM, electronic medical record management, disease prediction, patient tracking, drug traceability, and fighting infectious diseases. This study contributes by showing how combining IoT and blockchain enhances security and transparency, addressing challenges such as the resource limitations of IoT devices and scalability issues with solutions such as permissioned blockchains and energy-efficient consensus mechanisms.

The study in [13] explored advancements in RPM using blockchain technologies, focusing on Ethereum and Hyperledger Fabric. This contributes to the system architecture for EHR management using Ethereum, addressing challenges such as scalability and latency through optimized consensus mechanisms and hybrid storage systems.

Table 1

Authors	Application for BIOT healthcare	contribution	challenges	solutions
[1]	Remote Patient Monitoring, Data Security in Healthcare, Decentralized User Authentication, Smart Contracts for Healthcare Access	Blockchain-Based Access Control, Off-Chain Mutual Authentication, Dynamic Misbehavior Detection, Scalability Enhancements	Scalability Issues, Computational Limitations of IoT Devices, Security Concerns	Local Gateways for IoT Devices, Token-Based Access Control, Smart Contract-Based Misbehavior Handling, Hybrid On-Chain and Off-Chain Model
[2]	Personal Health Data (PHD) Management, Privacy-Preserved Data Sharing, Secure IoT-Based Health Monitoring	Individual-Initiated Control, Auditable Access Control, Integration of Blockchain, CP-ABE, and IPFS, Privacy Preservation	Fine-Grained Access Control, Data Privacy, Data Ownership and Management, Scalability	Use of CP-ABE for Access Control, Off-Chain Data Storage, Audit Mechanism, Individual Control over Data
[3]	Data Privacy in IoT-Healthcare, Secure IoT Healthcare Data Sharing, IoT Device Management in Healthcare.	Integration of ABAC with Hyperledger Fabric, Smart Contracts for IoT Devices, Performance Optimization with Raft Consensus,	Access Control Complexity, Latency and Scalability, Data Security and Privacy	Attribute-Based Access Control (ABAC), Raft Ordering Service, Decentralized Access Management
[4]	Remote Patient Monitoring (RPM), Patient Tracking, Disease Prediction, Fighting COVID-19, Security of Medical Records, Security of Medical Records, Securing the Internet of Medical Things (IoMT)	Integration of Blockchain and IoT, Decentralized Access Control, Improved Data Integrity, Enhanced Scalability and Efficiency	Data Privacy and Security, Scalability, Interoperability, High Computational Requirements, Data Storage	Decentralized Data Storage, Use of Permissioned Blockchains, Optimization of Consensus Algorithms, Interoperability Frameworks
[5]	IoT for Remote Health Monitoring, Blockchain for Medical Record Security, Access Control for Medical Devices	Integration of Blockchain and IoT, Dynamic Access Control Mechanism, Custom Chaincode for IoT Devices	Performance Constraints, Data Privacy, Scalability, Interoperability	Programmatic Access Control, Hybrid Storage Solutions, Use of Lightweight Blockchain Protocols, Dynamic Chaincode and Policy Management
[6]	Remote Patient Monitoring for Chronic Diseases, Privacy-Preserved Data Sharing, E-Healthcare Systems	Blockchain for Security and Privacy, Scalability through IPFS, Secure Authentication with Smart Contracts, Consensus Algorithm for Fast Processing	Data Privacy and Security, Scalability, System Integration, Real-Time Data Processing	Proxy Re-Encryption for Privacy, Smart Contracts for Access Control, Decentralized Storage via IPFS, Proof of Authority Consensus:
[8]	IoT-Based Healthcare, Patient Data Management, Privacy and Security of Health Data	Blockchain-Enabled Access Control, Decentralized Storage Solutions, Fine-Grained Access Control, Consensus Mechanism Exploration	Scalability of Blockchain Systems, Latency in Access Control Systems, Privacy Preservation	Sharding for Scalability, Smart Contracts for Efficient Access Control, Decentralized Storage Using Blockchain, Combining Blockchain with ABAC

[9]	Electronic Health Records (EHR) Management, Clinical Trials, Drug Supply Chain Management, Health Insurance Claims	Security and Privacy, Improved Data Sharing, Increased Transparency and Accountability	Scalability, Storage Costs, Data Privacy, Consensus Mechanism Performance	Off-Chain Storage Solutions, Efficient Consensus Mechanisms, Sharding and Sidechains, Smart Contracts for Automation
[10]	Electronic Health Records (EHR), Medical Data Sharing, IoT Device Data Management	Scalability Analysis, Performance Improvements, Use of Docker, and AWS EC2 for Deployment	Latency and Throughput Limits, Managing Simultaneous Transactions, Complexity of Smart Contracts,	Optimizing Transaction Types, Scalable Hardware Configurations, Adjusting Transaction Rates and Block Size
[12]	Remote Patient Monitoring (RPM), Electronic Medical Records (EMR) Management, Disease Prediction, Patient Tracking, Drug Traceability, Fighting Infectious Diseases	Combining IoT and Blockchain, Addressing Security and Privacy, Survey of Existing Applications	Resource Limitations of IoT Devices, Scalability, Interoperability, Interoperability, Bandwidth and Energy Consumption	Permissioned Blockchains, Energy-Efficient Consensus Mechanisms, Scalable Blockchain Solutions, Data Encryption, Cross-Blockchain
[13]	Remote Patient Monitoring (RPM), Electronic Health Record (EHR) Management, Telehealth and Telemedicine	Blockchain as a Secure Data Management Tool, System Architecture for Secure Data, Decentralized Access Control	Scalability, Latency, Interoperability, Cost	Ethereum-Based Prototype for RPM, Optimizing Consensus Mechanisms, Hybrid Systems for Storage, Collaboration with Health IT Standards
[14]	Electronic Health Record (EHR) Management, Remote Patient Monitoring (RPM), Data Privacy and Security	Blockchain-Integrated RPM System, Decentralized Data Management, Proof of Authority (PoA) Consensus Mechanism	Data Privacy and Security, Interoperability, High Costs	Decentralized Storage Using Blockchain, Smart Contracts for Access Control, Proof of Authority for Improved Security
[15]	Remote Patient Monitoring, EHR Management, Medical Data Sharing	Blockchain Integration for Data Security, Low-Cost and Efficient Platform, Two-Layer Security Approach	Data Privacy and Confidentiality, Power and Resource, Scalability Issues	Permissioned Blockchain for Security, Hybrid Storage System, Efficient Energy Use via FPGA
[16]	Remote Patient Monitoring, Medical Data Sharing, Wearable Medical Devices	Blockchain for Security, Decentralized Data Management, Two-Blockchain Approach, NDN Paradigm Integration	Scalability, Privacy and Confidentiality, Processing and Power Constraints, Data Storage	Use of Hyperledger Fabric, Smart Contracts for Data Processing, Hybrid Blockchain Architecture, NDN-Based Data Communication
[17]	Remote Patient Monitoring (RPM), Electronic Health Records (EHR) Management, Implantable Medical Devices	Blockchain-Based Secure Data Management Framework (BSDMF), Enhanced Data Accessibility and Security, Improved Accuracy and Trust	Data Privacy and Security, Scalability Issues, Latency and Response Time	Use of Blockchain for Security, Hybrid Storage Approach, Smart Contracts for Data Management

[18]	Medical Data Security, Remote Patient Monitoring, Medical Device Management	Blockchain-Based IoMT Security, Decentralized Network Architecture, Elliptic Curve Cryptography (ECC) Integration, Privacy-Preserving Techniques	Resource Constraints of IoMT Devices, Scalability Issues, Network Latency	Hierarchical Blockchain Architecture, Threshold-Based Data Communication, Use of Bolsters, Enhanced Security Mechanisms
[21]	electronic health record (EHR)	blockchain-based interoperable EHR framework combining GDPR and HIPAA standards, Proposes a patient-centric approach to data management with verifiable credentials and secure digital wallets	Scalability, Integration challenges, Privacy concerns with public ledger accessibility and immutability conflicting with GDPR's right to data erasure, Immutability Conflicts with Regulatory Compliance, Access Inequality, Ethical Use of Decentralized Data, Governmental Resistance	Employs hybrid on-chain/off-chain data storage to enhance scalability, uses advanced cryptographic, Implements hash-lock mechanisms

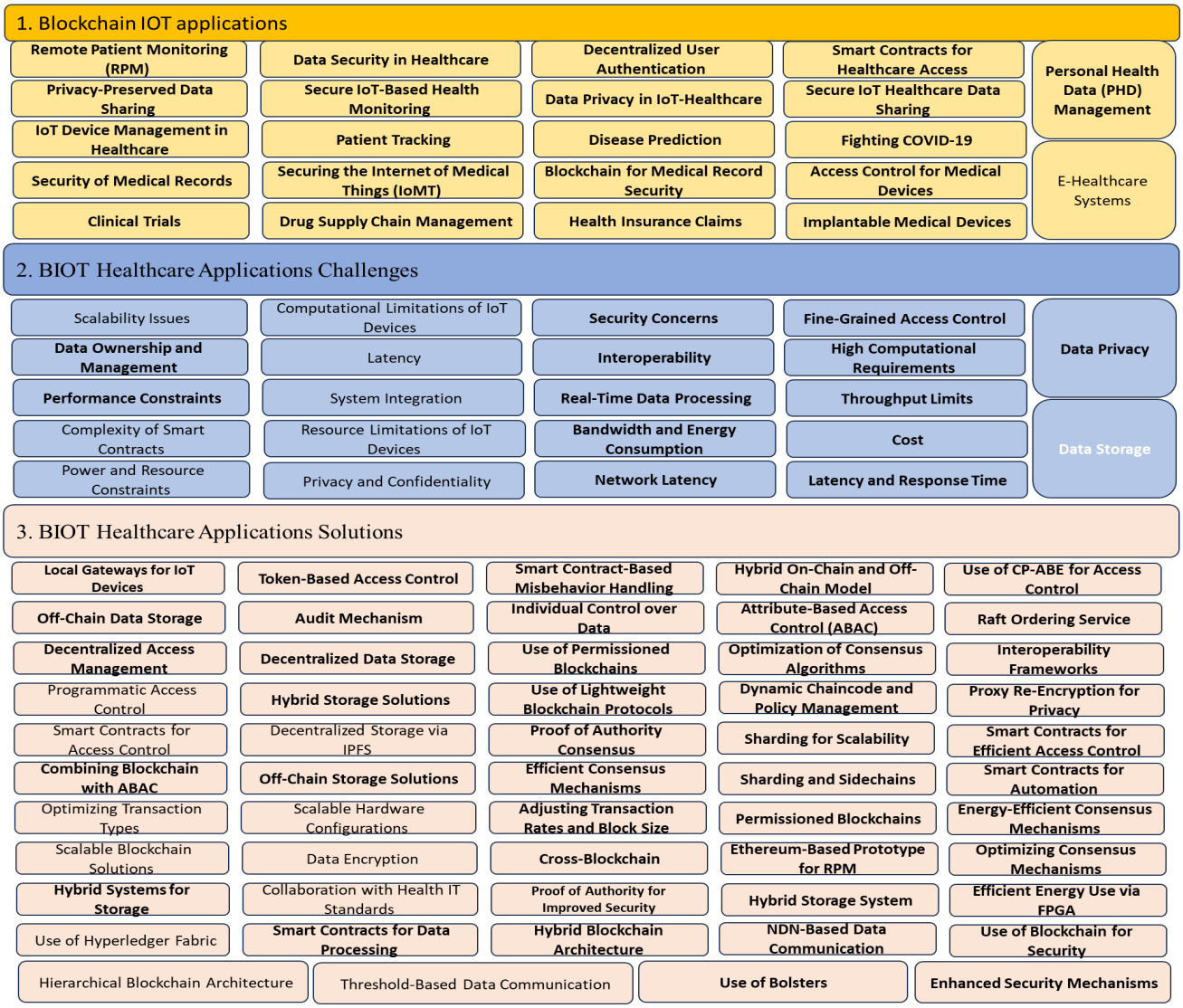

Figure 1. blockchain IOT healthcare applications contributions, challenges and solutionsblockchain IOT healthcare applications contributions, challenges and solutions

In [14], a new framework merged EHR and RPM techniques into a unified system using Django, enabling secure data transfer from IoT devices using Ethereum smart contracts. This study contributes by introducing decentralized data management and improving data security through smart contracts and the PoA consensus algorithm, addressing challenges such as data privacy during transmission and integration complexity.

[15] presents an IoMT-based platform for patient health monitoring, ensuring medical confidentiality and data security through blockchain. These contributions include a low-cost decentralized healthcare data management system using Raspberry Pi and a two-layer security approach. Challenges, such as data privacy and resource limitations, are addressed through permissioned blockchains and hybrid storage systems.

In [16], a security architecture based on Hyperledger Fabric was proposed, validated through design examples, and implemented functionalities. The study contributes by utilizing a two-blockchain approach to improve performance and data management, integrating Named Data Networking (NDN) to enhance communication efficiency. Challenges, such as scalability and privacy, are addressed through smart contracts and hybrid blockchain architectures.

The authors of [17] proposed a blockchain-assisted secure data management framework (BSDMF) for IoMT that enhances scalability and data accessibility. This study contributes to improving healthcare data security and achieving important levels of accuracy and trust in data management. Challenges, such as data privacy and latency, are addressed through encryption, hybrid storage, and smart contracts.

The study in [18] presented a blockchain-based approach with components, such as cloud servers, network clusters, medical facilities, and smart medical devices. This study contributes a lightweight blockchain scheme optimized for IoMT environments, addressing challenges such as resource constraints and scalability through a hierarchical blockchain architecture and enhanced security mechanisms that combine elliptic curve cryptography and identity-based credentials.

Finally, the study in [21] emphasizes the transformative potential of integrating blockchain and IoT technologies in healthcare, particularly for managing electronic health records (EHRs). This integration seeks to improve data interoperability, security, and scalability, while maintaining strict compliance with the GDPR and HIPAA regulations. Key applications include patient-centric EHR systems that empower individuals to securely manage and share their health data, facilitating real-time access for remote patient monitoring, seamless interhospital communication, and secure data exchange. This study introduces a blockchain-based framework designed to align GDPR and HIPAA standards, incorporating advanced encryption techniques, hashing, and secure digital wallets to safeguard data privacy, manage patient consent, and enforce verifiable access controls.

Despite its promise, this study identifies significant challenges, including scalability limitations posed by the volume of IoT-generated data, integration difficulties with existing healthcare infrastructure, and the inherent conflict between blockchain's immutability and GDPR's requirement for data erasure. To address these issues, this study proposes solutions, such as hybrid on-chain/off-chain data storage to improve scalability, advanced cryptographic methods to secure data sharing, and lightweight blockchain protocols tailored for IoT systems to enhance performance. This framework exemplifies a patient-focused approach to healthcare data management, effectively combining the strengths of blockchain's decentralized architecture with international data protection standards.

However, this study also highlights the critical ethical challenges inherent in the implementation of blockchain technology in healthcare, particularly concerning the sensitivity of medical data. Privacy and confidentiality have emerged as key concerns, as the distributed nature of permissionless blockchains exposes patient information to unauthorized access via techniques such as graph analysis, phishing, and transaction linkage. This decentralized model amplifies the potential for privacy breaches in an industry in which data confidentiality is paramount. Additionally, blockchain's immutability presents regulatory conflicts, as it clashes with legal frameworks such as GDPR and HIPAA that grant individuals the right to delete or modify their personal data. This tension underscores the fundamental incompatibility between blockchain's design principles and patient rights to data management.

Further complicating matter is the issue of access inequality. Implementing blockchain systems requires technical expertise, financial resources, and advanced hardware that may not be equally accessible to all healthcare providers or patients. This disparity risks widening the gap in health care delivery, particularly between resource-rich and resource-constrained environments. Although blockchain offers robust security, it remains vulnerable to sophisticated attacks, such as 51% attacks, Sybil attacks, and wallet hacking, which could undermine system integrity and erode patient trust. The decentralized nature of blockchain also raises accountability concerns, particularly in instances of data misuse or breaches, because there is no central authority responsible for oversight.

Moreover, resistance to adopting decentralized technologies in government-owned healthcare systems further impedes equitable access. This reluctance often leads to a divided system in which private institutions advance

with cutting-edge technologies, whereas public institutions lag, exacerbating existing inequalities. To overcome these challenges, this study emphasizes the need for comprehensive governance frameworks and the implementation of advanced privacy-preserving techniques and initiatives to ensure inclusivity and equitable access. Without such measures, the full transformative potential of blockchain in healthcare may remain unattainable, thereby limiting its broader impact on the global healthcare landscape.

In summary, these studies collectively advance the field by proposing innovative applications of blockchain and IoT in healthcare, contributing solutions to challenges, such as scalability, security, data privacy, and interoperability. They offer various models and frameworks that enhance healthcare services through secure data management, decentralized access control, and efficient real-time processing, thus paving the way for future research and implementation in the healthcare industry. In Table.1 we will present the application types, contributions, challenges, and solutions presented in this section. Table 1 presents the authors, applications, contributions, challenges, and solutions

Figure 1. presents a summary of blockchain IOT applications, challenges, and solutions as a summary of related work.

7. CASE STUDY

The case study in [1], involving two laptops and a Raspberry Pi, provides a compelling demonstration of how healthcare providers can effectively implement blockchain-based solutions for IoT systems while overcoming technical barriers. In the framework, Raspberry Pi acted as a local IoT gateway, bridging the gap between resource-constrained IoT devices and the Ethereum blockchain. By delegating computationally intensive tasks such as smart contract execution and user authentication validation to the gateway, the system achieves enhanced scalability and security without burdening IoT devices. The use of Ethereum smart contracts to manage dynamic access policies ensures robust and automated access control, while secure off-chain mutual authentication through socket programming adds an additional layer of protection for sensitive healthcare data.

The setup not only highlights the feasibility of blockchain integration in IoT healthcare, but also underscores its practical utility in resource-constrained environments. By leveraging lightweight blockchain clients on gateways, such as Raspberry Pi, the framework reduces the need for expensive and powerful hardware while maintaining high levels of security and operational efficiency. To make such systems accessible to non-technical users, tools such as Remix IDE for coding and testing smart contracts and JavaScript APIs such as web3.js for blockchain interactions can simplify the deployment and operation of blockchain-based solutions. Preconfigured IoT gateways with user-friendly interfaces further minimize the technical complexities involved, enabling healthcare providers to focus on delivering quality care.

To facilitate the widespread adoption of similar solutions, it is recommended that healthcare providers adopt modular and prebuilt frameworks that include smart contract templates and detailed step-by-step deployment instructions. Such resources can help streamline the implementation process and ensure compliance with health care standards and regulations. Additionally, the use of preconfigured gateways that integrate seamlessly with IoT devices and blockchain networks can further lower entry barriers. This approach not only addresses critical challenges, such as scalability and security, but also paves the way for cost-effective and efficient healthcare systems that harness the full potential of blockchain and IoT technologies. Focusing on accessibility, practicality, and robust security measures, this case study demonstrates how advanced blockchain frameworks can revolutionize healthcare operations, particularly in settings with limited technical expertise and resources.

8. CONCLUSION AND FUTURE WORKS

The integration of blockchain technology into IoT-driven healthcare systems holds immense potential to address critical challenges such as ensuring data security, achieving scalability, and maintaining data integrity. Frameworks, like the one illustrated in the case study, demonstrate how healthcare providers can adopt advanced technologies without requiring significant technical knowledge. By employing local IoT gateways, such as Raspberry Pi devices, these frameworks effectively handle resource-intensive tasks such as smart contract execution and authentication validation. This approach not only secures and scales operations but also alleviates the computational burden on resource-constrained IoT devices. Moreover, the use of intuitive tools, such as Remix IDE and JavaScript APIs (e.g., web3.js), further simplifies the process, making blockchain-based solutions more accessible to non-technical stakeholders.

This review underscores the importance of modular and preconfigured solutions, including reusable smart contract templates, comprehensive deployment instructions, and lightweight blockchain clients specifically designed for healthcare environments. These innovations have enabled healthcare providers to safeguard sensitive patient information, streamline operational processes, and adhere to stringent regulatory requirements. Although challenges such as initial deployment and seamless integration persist, the scalability and robust security demonstrated by these frameworks affirm their viability in resource-limited settings.

The combination of blockchain and IoT represents a transformative approach to modernizing the healthcare infrastructure. By prioritizing user accessibility and practical deployment, these technologies can significantly enhance healthcare delivery, particularly in regions with constrained resources and technical expertise. Moving forward, research and development efforts should focus on further refining these frameworks to enhance simplicity, scalability, and their ability to support larger and more complex healthcare ecosystems and present a review of blockchain IOT healthcare applications, their contributions, challenges, and solutions. We reviewed recent papers published from 2016 to 2024 to provide a full view of blockchain healthcare applications. Figure 1 shows the blockchain IOT healthcare applications, challenges, and solutions. As a result, using Blockchain IOT in healthcare applications can overcome many problems, and there are many disciplines to improve blockchain in healthcare applications. It is especially important to conduct wider research on blockchain IOT healthcare applications to improve healthcare security, availability, integrity, and other services. The reviewed studies highlight the potential of blockchain and IoT integration in healthcare to enhance data security, scalability, and operational efficiency. Although challenges such as scalability, interoperability, and privacy persist, innovative solutions such as hybrid storage, efficient consensus algorithms, and decentralized access control models demonstrate promising progress. Further research is required to standardize the integration processes and optimize these systems for real-world applications.

REFERENCES

[1] V. Geetha and B. Balakrishnan. “A User Authentication and Access Control Scheme for IoT-Based Healthcare Using Blockchain”. In: *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. Kharagpur, India, 2021, pp. 01–07. DOI: 10.1109/ICCCNT51525.2021.9579992.

[2] R. Cong et al. “Individual-Initiated Auditable Access Control for Privacy-Preserved IoT Data Sharing with Blockchain”. In: *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*. Montreal, QC, Canada, 2021, pp. 1–6. DOI: 10.1109/ICCWorkshops50388.2021.9473508.

[3] E. A. Shammar, A. Zahary, and A. A. Q. Al-Shargabi. “An Attribute-Based Access Control Model for Internet of Things Using Hyperledger Fabric Blockchain”. In: *Wirel. Commun. Mob. Comput.* 2022 (July 2022), pp. 1–25. DOI: 10.1155/2022/6926408.

[4] W. A. N. A. Al-Nbhany, A. T. Zahary, and A. A. Al-Shargabi. “Blockchain-IoT Healthcare Applications and Trends: A Review”. In: *IEEE Access* 12 (2024), pp. 4178–4212. DOI: 10.1109/ACCESS.2023.3349187.

[5] A. Iftekhar et al. “Hyperledger Fabric Access Control System for Internet of Things Layer in Blockchain-Based Applications”. In: *Entropy* 23.8 (Aug. 2021), p. 1054. DOI: 10.3390/e23081054.

[6] K. Azbeg, O. Ouchetto, and S. Jai Andaloussi. “Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management”. In: *IEEE Trans. on Comput. Soc. Syst.* 10.4 (Aug. 2023), pp. 1515–1527. DOI: 10.1109/TCSS.2022.3186945.

[7] W. A. N. A. AL-Nbhany and A. Zahary. “A Comparative Study among Cryptographic Algorithms: Blowfish, AES, and RSA”. In: *International Arab Conference on Information Technology*. 2016, pp. 1–7.

[8] Y. Liu et al. “Blockchain-Based Access Control Approaches”. In: *2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. Washington, DC, USA, 2021, pp. 127–132. DOI: 10.1109/CSCloud-EdgeCom52276.2021.00032.

[9] Meenavolu S. B. Kasyapa and C. Vanmathi. “Blockchain Integration in Healthcare: A Comprehensive Investigation of Use Cases, Performance Issues, and Mitigation Strategies”. In: *Front. Digit. Health* 6 (2024). DOI: 10.3389/fdgth.2024.1359858.

[10] M. Kuzlu et al. “Performance Analysis of a Hyperledger Fabric Blockchain Framework: Throughput, Latency and Scalability”. In: *2019 IEEE International Conference on Blockchain (Blockchain)*. 2019, pp. 536–540. DOI: 10.1109/Blockchain.2019.00003.

[11] G. Gan et al. “Token-Based Access Control”. In: *IEEE Access* 8 (2020), pp. 54189–54199. DOI: 10.1109/ACCESS.2020.2979746.

[12] K. Azbeg et al. “A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications”. In: *IRBM* 43.5 (Oct. 2022), pp. 511–519. DOI: 10.1016/j.irbm.2021.05.003.

[13] M. J. Hossain Faruk et al. “Towards Blockchain-Based Secure Data Management for Remote Patient Monitoring”. In: *2021 IEEE International Conference on Digital Health (ICDH)*. 2021, pp. 299–308. DOI: 10.1109/ICDH52753.2021.00054.

[14] R. Mohammed, R. Alubady, and A. Sherbaz. “Utilizing Blockchain Technology for IoT-Based Healthcare Systems”. In: *J. Physics: Conf. Ser.* 1818.012111 (2021), pp. 1–11.

[15] J. Ktari et al. “IoMT-Based Platform for E-Health Monitoring Based on the Blockchain”. In: *Electronics* 1.15 (2022), pp. 1–17.

[16] O. Attia et al. “An IoT-Blockchain Architecture Based on Hyperledger Framework for Healthcare Monitoring Application”. In: *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. 2019, pp. 1–5. DOI: 10.1109/NTMS.2019.8763849.

[17] A. Abbas et al. “Blockchain-Assisted Secured Data Management Framework for Health Information Analysis Based on Internet of Medical Things”. In: *Pers. Ubiquitous Comput.* (Aug. 2021), pp. 1–14.

[18] M. Seliem and K. Elgazzar. “BIoMT: Blockchain for the Internet of Medical Things”. In: *2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*. 2019, pp. 1–4.

[19] H. S. Z. Kazmi et al. “Trusted Remote Patient Monitoring Using Blockchain-Based Smart Contracts”. In: *Lecture Notes in Networks and Systems*. 2019, pp. 765–776. DOI: 10.1007/978-3-030-33506-9_70.

[20] H. Hasanova et al. “A Novel Blockchain-Enabled Heart Disease Prediction Mechanism Using Machine Learning”. In: *Comput. Electr. Eng.* 101 (2022), p. 108086.

[21] F. A. Reegu et al. “Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System”. In: *Sustainability* 15.8 (Apr. 2023), p. 6337. DOI: 10.3390/su15086337.