

Article

blockHealthSecure: Integrating Blockchain and Cybersecurity in Post-Pandemic Healthcare Systems

Bishwo Prakash Pokharel ¹, Naresh Kshetri ^{2,*} , Suresh Raj Sharma ³  and Sobaraj Paudel ³ 

¹ Sault College of Applied Arts and Technology, Sault Ste. Marie, ON P6B 4J3, Canada; bishwoprakash.pokharel@triosstudent.com

² Department of Cybersecurity, Rochester Institute of Technology, Rochester, NY 14623, USA

³ Tribhuvan University, Birendra Multiple Campus, Bharatpur 44200, Chitwan, Nepal; sr.sharma119@gmail.com (S.R.S.); paudel.sobaraj123@gmail.com (S.P.)

* Correspondence: naresh.kshetri@rit.edu

Abstract: The COVID-19 pandemic exposed critical vulnerabilities in global healthcare systems, particularly in data security and interoperability. This paper introduces the blockHealthSecure Framework, which integrates blockchain technology with advanced cybersecurity measures to address these weaknesses and build resilient post-pandemic healthcare systems. Blockchain's decentralized and immutable architecture enhances the accuracy, transparency, and protection of electronic medical records (EMRs) and sensitive healthcare data. Additionally, it facilitates seamless and secure data sharing among healthcare providers, addressing long-standing interoperability challenges. This study explores the challenges and benefits of blockchain integration in healthcare, with a focus on regulatory and ethical considerations such as HIPAA and GDPR compliance. Key contributions include detailed case studies and examples that demonstrate blockchain's ability to mitigate risks like ransomware, insider threats, and data breaches. This framework's design leverages smart contracts, cryptographic hashing, and zero-trust architecture to ensure secure data management and proactive threat mitigation. The findings emphasize the framework's potential to enhance data security, improve system adaptability, and support regulatory compliance in the face of evolving healthcare challenges. By bridging existing gaps in healthcare cybersecurity, the blockHealthSecure Framework offers a scalable, future-proof solution for safeguarding health outcomes and preparing for global health crises.

Keywords: blockchain; data security; post-pandemic healthcare; interoperability; COVID-19



Academic Editor: Eric Pardede

Received: 3 January 2025

Revised: 2 February 2025

Accepted: 7 February 2025

Published: 11 February 2025

Citation: Pokharel, B.P.; Kshetri, N.; Sharma, S.R.; Paudel, S.

blockHealthSecure: Integrating Blockchain and Cybersecurity in Post-Pandemic Healthcare Systems. *Information* **2025**, *16*, 133. <https://doi.org/10.3390/info16020133>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

As a distributed database and decentralized ledger, and with its other powerful features, blockchain technology is gaining more ground. The use of cybersecurity with several other emerging technologies like metaverse, blockchain technology, and many more are increasing as global weaknesses, ethical concerns, and legal automation in healthcare systems increase, with blockchain used as a part of secure algorithms like LGE-HES [1,2]. The development and advancement of blockchain emphasize the ability to protect sensitive information (including personally identifiable information or PII) in healthcare systems.

Healthcare systems are the most attacked critical infrastructures as compared to other critical infrastructures, with a significant rise in cyberattacks in the post-pandemic period. As blockchain has emerged as a ground-breaking technology, although it started as a digital currency (cryptocurrency), blockchain can be a perfect match for cybersecurity and cyber

defense [3]. Blockchain technology offers various countermeasures for healthcare systems, including preventing data tampering, addressing security vulnerabilities, detecting malicious actors, authenticating containers in smart systems, mitigating DoS attacks, securing IoT devices, and enabling robust communication within critical healthcare infrastructure.

In addition to enhancing security, blockchain technology can foster greater transparency and accountability in healthcare operations. By providing immutable records and decentralized control, blockchain enables a robust framework for auditing and compliance with regulatory standards such as HIPAA [4] and GDPR [5]. Furthermore, its applications in the secure sharing of medical records, streamlined clinical trials, and efficient supply chain management demonstrate its potential to revolutionize healthcare systems by improving efficiency and fostering trust among stakeholders.

Blockchain technology, combined with advanced cybersecurity measures, is a game-changer for addressing the vulnerabilities in healthcare systems exposed during the pandemic. Its decentralized architecture enables secure data sharing, while its cryptographic underpinnings ensure patient data integrity and privacy. Furthermore, blockchain supports real-time monitoring and tamper-proof auditing, providing healthcare providers and patients with unparalleled transparency and trust. The synergy of blockchain with emerging technologies like AI and IoT further enhances its potential, creating a robust foundation for future healthcare innovations.

The COVID-19 pandemic has not only highlighted the importance of secure healthcare systems but also underscored the challenges of maintaining data integrity and privacy during a global crisis. Contact tracing initiatives, for example, exposed the difficulty of balancing public health measures with the need to protect sensitive patient information. Blockchain technology provides an effective solution to these challenges by enabling decentralized storage and sharing of data, where patients retain control over their personal information. This approach aligns with the principles of privacy protection mandated by regulations such as GDPR, emphasizing its applicability to future healthcare crises.

Despite its potential, the adoption of blockchain technology in healthcare faces significant challenges, including interoperability issues, scalability concerns, and the integration of blockchain systems with existing healthcare infrastructures. The blockHealthSecure Framework addresses these limitations by incorporating a multi-layered design that ensures seamless data exchange through standardized formats and decentralized identity systems. Moreover, its reliance on smart contracts and cryptographic security measures mitigates risks such as data breaches and insider threats, which were identified as prevalent issues in reports like IBM's X-Force Threat Intelligence Index 2024 [6].

The rise in ransomware attacks and credential harvesting in healthcare further justifies the integration of blockchain with advanced cybersecurity tools. Recent findings from Verizon's DBIR 2024 [7] show that insider threats account for a substantial portion of healthcare breaches, highlighting the need for robust access controls and real-time monitoring. The blockHealthSecure Framework leverages zero-trust architecture and AI-driven anomaly detection to safeguard patient records and ensure compliance with federal standards like HIPAA. These features make the framework a scalable and adaptable solution capable of addressing the evolving cyber threat landscape in healthcare.

By providing tamper-proof audit trails and enabling transparent operations, blockchain technology empowers healthcare providers to build trust among patients and other stakeholders. When combined with cybersecurity, blockchain becomes a transformative tool for securing electronic medical records, improving clinical trial transparency, and enhancing pharmaceutical supply chain traceability. As healthcare systems increasingly rely on digital solutions, the integration of blockchain and cybersecurity emerges as a crucial step in creating resilient infrastructures capable of withstanding future challenges.

2. Background Study

Integrating blockchain technology into healthcare systems has become a promising approach to overcoming several ongoing issues, especially following the COVID-19 pandemic. As healthcare organizations continue to embrace digital transformation, ensuring the security and confidentiality of patient data have become paramount. Blockchain technology offers a decentralized and secure approach to managing, storing, and sharing medical information, enhancing data integrity, and safeguarding patient privacy within healthcare systems. Blockchain technology has diverse applications in the healthcare sector, including electronic health records (EHRs) and pharmaceutical supply chain management. Its core attributes—decentralization, immutability, and cryptographic protection—make it a perfect choice for managing sensitive health information. For example, researchers have suggested using blockchain to improve supply chain management for medical devices and pharmaceuticals, ensuring product authenticity and minimizing fraud.

Despite significant advancements in healthcare innovation and management, security concerns such as data breaches and cybersecurity have yet to receive sufficient attention. Effective healthcare data management is crucial for healthcare authorities to deliver optimal services in daily operations and during pandemics like COVID-19. Blockchain (BC) technology can enhance the security of healthcare data management. Smart contract code development and testing were performed on the Remix IDE platform. We have combined Hyperledger Fabric (HLF) and the InterPlanetary File System (IPFS) to provide decentralized storage [8]. Besides assessing various safety concerns, we also compared our method with current blockchain-based systems and estimated the transaction costs it proposes. We illustrated the advantages of utilizing blockchain to create a secure and reliable healthcare system. Additionally, we highlighted the existing challenges in integrating blockchain technology into healthcare information management and identified potential future research directions for its implementation and practical applications. A key aspect of blockchain technology is its use of cryptographic hash functions for various operations [9].

2.1. Blockchain Technology in Healthcare

Blockchain technology in healthcare involves applying blockchain concepts and frameworks to improve the management and security of medical information. Initially created for cryptocurrency, blockchain's decentralized and unchangeable characteristics provide solutions to numerous issues in healthcare, such as data security, interoperability, and patient privacy. The growing digitalization of healthcare has heightened concerns over managing sensitive patient information, making blockchain a notable and promising tool in the industry. Blockchain's importance in healthcare stems from its ability to transform data sharing and security practices. By ensuring secure and transparent transactions between stakeholders like patients, providers, and insurers, blockchain can enhance access to electronic health records (EHRs) and help address challenges such as data breaches and counterfeit medications.

Integrating blockchain into healthcare cybersecurity frameworks can offer significant advantages in defending against cyberattacks. Studies indicate that blockchain-based models can significantly improve patient data security, making it more resistant to unauthorized access and breaches. Unlike traditional security methods, which are typically centralized and vulnerable to attacks, blockchain's decentralized structure offers a more robust defense against data tampering and cyber threats. However, challenges still exist; for instance, hashing alone is not enough to eliminate all risks of data tampering by enabling secure and transparent transactions among various stakeholders—including patients, providers, and insurers—but blockchain can facilitate improved access to electronic health records (EHRs) and mitigate issues such as data breaches and counterfeit medications.

Key applications of blockchain in healthcare include increasing transparency in clinical trials, optimizing pharmaceutical supply chain management, and giving patients more control over their health data. Various initiatives and pilot projects have demonstrated its efficacy in these areas, sparking interest and investment across the sector. Although blockchain technology holds great promise, its integration into healthcare faces challenges and controversies. Concerns over scalability, regulatory compliance, and data privacy have emerged as significant barriers to adoption. Moreover, the requirement for strong frameworks to handle patient consent and access control brings up ethical and legal concerns. As the technology progresses, continuous research and collaboration among stakeholders are crucial to address these challenges and fully realize the potential of blockchain in enhancing healthcare delivery and patient outcomes.

2.2. Cybersecurity Challenges in Healthcare

As healthcare organizations increasingly rely on digital technologies like electronic health records (EHRs) and interconnected medical devices, they are becoming prime targets for cybercriminals employing advanced tactics such as ransomware, phishing, and distributed denial-of-service (DDoS) attacks.

The rise in cyberattacks has resulted in substantial financial damage, disrupted patient care, and triggered urgent questions regarding the adequacy of existing security measures to safeguard sensitive patient information.

Ransomware attacks, specifically, represent a major danger, as they can paralyze essential systems and jeopardize patient care by making access to crucial medical records and services unfeasible. Moreover, insider threats, along with the utilization of weaknesses in third-party vendors, intensify the security environment, requiring extensive strategies for risk management and reaction. Regulatory compliance plays a vital role in the cybersecurity framework for healthcare organizations. Federal laws like the HIPAA mandate stringent protections for patient health data, and non-compliance can lead to hefty fines and reputational damage. With the changing regulatory landscape, healthcare providers must stay alert and flexible, integrating best practices and frameworks to enhance their cybersecurity stance in response to increasing threats. Tackling cybersecurity issues in healthcare demands a comprehensive strategy that harmonizes technological progress with proactive risk management tactics, continuous employee training, and strong compliance practices. These issues are crucial due to their profound effect on patient trust and the future of healthcare services, emphasizing the need for a cohesive and informed approach to address the growing cyber threat landscape. Table 1 demonstrates the cybersecurity challenges in healthcare and blockchain-based solutions.

Table 1. Cybersecurity challenges in healthcare and blockchain-based solutions.

Cybersecurity Challenges	Description	Blockchain-Based Solution
Data Breaches	Frequent cyberattacks exposing sensitive health records and patient data.	Blockchain's cryptographic security and decentralized storage ensure tamper-proof and secure data management
Unauthorized Access to Health Records	Insider threats and lack of access control lead to misuse of patient data.	Permissioned blockchain networks enforce strict access controls and transparent access logs.
Interoperability Risks	Fragmented healthcare systems hinder secure data exchange between institutions	Standardized data formats on blockchain enable seamless and secure data sharing across healthcare entities

Table 1. Cont.

Cybersecurity Challenges	Description	Blockchain-Based Solution
Ransomware Attacks	Cybercriminals encrypt data, demanding payment to release it.	Decentralized and immutable data storage on blockchain prevents unauthorized encryption or manipulation of data.
Lack of Auditability and Transparency	Limited visibility into who accesses or modifies healthcare data.	Blockchain's immutable ledger ensures transparent, tamper-proof audit trails for data usage and modifications.
Fraudulent Activities in Clinical Trials	Manipulated data reduces trust and increases operational risks.	Blockchain provides verifiable and transparent records, preventing data manipulation in clinical trials.
Supply Chain Security	Counterfeit drugs and inefficiencies in pharmaceutical tracking.	Blockchain enhances traceability and authenticity, ensuring secure pharmaceutical supply chains.

3. Methodology

This study adopts a mixed-method approach to integrate blockchain technology and cybersecurity, addressing the critical need for secure and efficient systems in the healthcare sector. Blockchain's decentralized, immutable, and transparent nature forms the foundation for the proposed blockHealthSecure Framework, enabling robust protection against healthcare-specific cyber threats such as data breaches and ransomware attacks. To support this study, an extensive literature review was conducted, drawing insights from key sources, including peer-reviewed journals, regulatory frameworks, and industry reports [4–7]. The review also highlighted existing gaps in the healthcare cybersecurity landscape, reinforcing the necessity of an innovative, research-driven framework.

Secondary data collection was pivotal to this methodology, utilizing credible resources such as the Health Insurance Portability and Accountability Act (HIPAA) regulations, the NIST standards mentioned in Figure 1, and industry reports like IBM's X-Force Threat Intelligence and Verizon's Data Breach Investigations Report (DBIR). According to the X-Force report, the healthcare industry rose to the sixth most attacked sector in 2023, accounting for 6.3% of total cyberattacks. Similarly, Verizon's 2024 DBIR report which is presented in Table 2, revealed that healthcare experienced 1378 incidents, of which 1220 involved confirmed data disclosures. The report identified that internal actors were responsible for 70% of breaches, highlighting the need for robust internal security measures.



Figure 1. NIST cybersecurity framework 2.0 [10].

Table 2. Key insights from the Verizon 2024 DBIR [7].

Category	Details
Frequency	1378 incidents, 1220 with confirmed data disclosure
Top Patterns	Miscellaneous Errors, Privilege Misuse, and System Intrusion (83% of breaches)
Threat Actors	Internal (70%), External (30%) (breaches)
Actor Motives	Financial (98%), Espionage (1%) (breaches)
Data Compromised	Personal (75%), Internal (51%), Other (25%), Credentials (13%) (breaches)
Consistent Trends	System Intrusion breaches remain in the top three attack patterns

Interestingly, personal data have overtaken medical data as the primary target for threat actors, further underscoring the urgency of integrating blockchain to ensure data integrity and confidentiality. Insights from federal mandates such as HIPAA and GDPR informed the design of the framework, ensuring its alignment with critical compliance requirements [4,5].

The methodology culminates in the development of the blockHealthSecure Framework, designed to mitigate cybersecurity risks in the healthcare ecosystem through a holistic, integrated solution. By combining blockchain's decentralized and tamper-proof architecture with advanced cybersecurity strategies such as zero-trust models, AI-driven threat detection, and real-time monitoring, the framework ensures data integrity, confidentiality, and availability. This approach not only bridges the gaps identified in the literature but also offers a scalable and adaptive model for addressing the evolving cyber threat landscape in healthcare. The research methodology ensures the framework is grounded in theoretical insights, regulatory standards, and practical applicability, enabling its seamless adoption across healthcare organizations.

The literature review and secondary data collection revealed several critical vulnerabilities in the healthcare sector, including the widespread prevalence of phishing, ransomware attacks, and insider threats. Reports such as IBM's X-Force Threat Intelligence Index 2024 noted that credential harvesting accounted for half of the reported cases in healthcare, while reconnaissance, data leaks, and extortion collectively represented 25% of incidents. These findings underscore the necessity of designing a framework that incorporates advanced cybersecurity mechanisms, such as cryptographic hashing, multi-factor authentication (MFA), and role-based access control (RBAC), to mitigate these risks effectively.

The framework development process involved mapping identified vulnerabilities to specific blockchain features and cybersecurity measures. For example, smart contracts were integrated to automate patient consent and data-sharing protocols, addressing concerns about data misuse and non-compliance with regulations like HIPAA. Permissioned blockchain networks were selected to ensure that only authorized entities could access sensitive medical records, significantly reducing the likelihood of insider threats and unauthorized access. Furthermore, decentralized identity (DID) systems were incorporated to enhance patient control over their data, aligning with the principles of GDPR and ensuring transparency in data transactions.

The methodology emphasized compliance with global standards and best practices. The framework was designed to align with the NIST Cybersecurity Framework 2.0, leveraging its guidelines to establish risk management practices and enhance the resilience of healthcare systems. This alignment ensures that the proposed solution meets the highest standards of security and interoperability, paving the way for its widespread adoption across diverse healthcare settings.

3.1. Structure of the Proposed Blockchain System

The blockHealthSecure Framework is designed to enhance healthcare cybersecurity by integrating blockchain technology, cryptographic security mechanisms, and smart contracts. This multi-layered framework and its functionality are presented in Table 3, which ensures data integrity, interoperability, access control, and regulatory compliance while mitigating cyber threats such as data breaches, ransomware, and insider threats.

Table 3. Multi-layered architecture of blockHealthSecure.

Layer	Functionality
Data Integrity and Security Layer	Uses cryptographic hashing and decentralized storage to prevent data tampering and unauthorized modifications.
Interoperability Enhancement Layer	Implements FHIR/HL7 standards and permissioned blockchain networks to facilitate secure medical data exchange between healthcare providers.
Cybersecurity Integration Layer	Incorporates Intrusion Detection Systems (IDS), Zero Trust Architecture (ZTA), and AI-driven threat analysis to monitor and mitigate cyber threats.
Regulatory Compliance and Governance Layer	Ensure compliance with HIPAA, GDPR, and NIST standards through blockchain-based audit trails and automated access controls.
Future-Proofing and Innovation Layer	Focuses on AI-driven analytics, IoT integration, and scalability features to ensure adaptability to emerging healthcare challenges.

3.2. Consensus Mechanism

The blockHealthSecure Framework employs Proof of Authority (PoA) as its consensus mechanism, which offers:

- High security: Only verified and trusted healthcare providers participate in the validation process.
- Low latency: Faster transaction validation compared to Proof of Work (PoW).
- Energy efficiency: Requires significantly less computational power, making it scalable for healthcare operations.

This multi-layered structure ensures robust security, seamless interoperability, and compliance with healthcare regulations, making the system resilient against cyber threats and unauthorized access.

3.3. Detail Explanation of the Proposed Method

The blockHealthSecure Framework integrates blockchain technology, smart contracts, AI-driven intrusion detection systems (IDS), and Zero Trust Architecture (ZTA) to enhance healthcare security, compliance, and threat mitigation. The following are detailed explanations of how each of these components contributes to secure, interoperable, and resilient healthcare systems.

3.3.1. How Blockchain Enhances Healthcare Security

Blockchain technology strengthens healthcare security through data immutability, cryptographic verification, and decentralized control.

Data Immutability and Integrity

Blockchain's distributed ledger ensures that once medical records are recorded, they cannot be altered or deleted, preventing data tampering by malicious insiders or external attackers [11]. Each medical record is hashed and stored as a cryptographic digest, ensuring integrity and non-repudiation [12]. Any modification in patient data creates a new

version while maintaining a full historical audit trail, ensuring transparency and regulatory compliance (e.g., HIPAA, GDPR) [13].

Cryptographic Verification

Elliptic Curve Cryptography (ECC) and SHA-256 hashing provide strong encryption to secure patient records against unauthorized access [14]. Decentralized Identity (DID) mechanisms enable secure authentication, reducing risks associated with stolen credentials or identity fraud [15]. Multi-signature (multi-sig) verification ensures that critical actions (such as modifying access permissions) require approvals from multiple authorized entities (e.g., patient and healthcare provider). By leveraging these features, blockchain provides a secure, tamper-proof, and transparent healthcare data management system [16].

3.3.2. How Smart Contracts Automate Access Control, Auditing, and Compliance Enforcement

Smart contracts are self-executing blockchain programs that enforce security policies and automate compliance mechanisms [17].

Automated Access Control

Patients have sovereignty over their Electronic Health Records (EHRs) and can grant or revoke access using blockchain-based smart contracts [18]. Healthcare providers must request access, and the smart contract verifies the request based on predefined rules before granting temporary or permanent access. Access logs are immutably recorded, preventing unauthorized access and ensuring an audit trail for compliance.

Smart Contracts for Auditing

Every data request, modification, or sharing event triggers a smart contract, which logs the action on the blockchain. These logs create a real-time, immutable audit trail, ensuring compliance with healthcare regulations (HIPAA, GDPR, and NIST standards). Smart contracts can automatically flag suspicious activities, such as unauthorized data access attempts.

Compliance Enforcement

Regulatory policies are encoded into smart contracts to ensure automatic compliance enforcement. If a healthcare provider or insurer violates predefined security policies, the contract can revoke permissions or trigger an alert for human review. Time-sensitive permissions allow temporary access to patient data (e.g., emergency room scenarios) and expire automatically after the designated period.

By eliminating manual intervention, smart contracts reduce human error, prevent fraud, and streamline compliance monitoring in healthcare systems.

3.3.3. How AI-Driven IDS Systems Detect and Mitigate Cyber Threats in Real-Time

AI-driven Intrusion Detection Systems (IDS) continuously monitor network traffic, blockchain transactions, and system logs to identify and neutralize cyber threats before they escalate [19].

Threat Detection with Machine Learning

AI-based IDS analyzes behavioral patterns to detect anomalous activities, such as unauthorized logins, data exfiltration, or abnormal transaction requests. Supervised and unsupervised machine learning models classify threats and predict potential attack vectors (e.g., ransomware or phishing attempts). IDS continuously learns from past cyberattacks and updates its detection algorithms to counter emerging threats.

Automated Threat Mitigation

If any anomaly is detected, the AI-IDS system can automatically trigger a response, such as:

- Revoking blockchain access tokens for compromised accounts.
- Blocking malicious IP addresses attempting unauthorized blockchain transactions.
- Alerting cybersecurity teams for manual intervention.

AI-powered systems can also correlate multiple attack indicators (e.g., abnormal network traffic + failed authentication attempts) to prevent multistage cyberattacks.

By integrating real-time AI-based IDS, the blockHealthSecure Framework detects, prevents, and mitigates cyber threats before they cause damage.

3.3.4. Integration of Zero Trust Architecture (ZTA) for Access Control

Zero Trust Architecture (ZTA) eliminates implicit trust and enforces strict identity verification at every access request [20].

The key principles of ZTA in blockHealthSecure are as follows:

- Least-privilege access: Users and devices only receive access to the minimum necessary data to perform their tasks. Even healthcare providers cannot access full medical records unless explicitly authorized.
- Continuous authentication and verification: Every request to access patient data is re-evaluated in real time, ensuring dynamic access control. AI-powered risk scoring assesses whether to allow, deny, or restrict access based on user behavior and device security.
- Micro-segmentation: Network segmentation isolates critical patient records and blocks lateral movement in case of a breach. If one segment is compromised, the attack cannot spread to other parts of the system.
- Multi-factor authentication (MFA): Advanced MFA mechanisms, including biometric authentication and cryptographic tokens, ensure that only authorized personnel gain access. Blockchain-based authentication further eliminates the risk of credential theft.

By integrating ZTA principles, blockHealthSecure ensures secure, dynamic, and context-aware access control, minimizing insider threats and external attacks.

4. blockHealthSecure Framework

4.1. Introduction to the blockHealthSecure Framework

The blockHealthSecure Framework represents an integrated approach to securing healthcare data through the synergy of blockchain technology and cybersecurity practices. In response to the increasing need for secure, interoperable, and flexible healthcare systems, the framework was developed especially after the COVID-19 pandemic highlighted critical weaknesses in data security and healthcare infrastructure. By utilizing blockchain's decentralized structure combined with advanced cybersecurity practices, the framework seeks to protect the integrity, confidentiality, and accessibility of sensitive health data while tackling the ongoing challenges of healthcare delivery.

4.2. Components of the blockHealthSecure Framework

The blockHealthSecure framework consists of five interconnected layers that collaborate to guarantee secure data management, seamless interoperability, and protection against cyber threats. Each layer incorporates specific components and functionalities that contribute to the overall security posture of healthcare systems. Figure 2 demonstrates the different layers of the blockHealthSecure Framework with its connectivity.

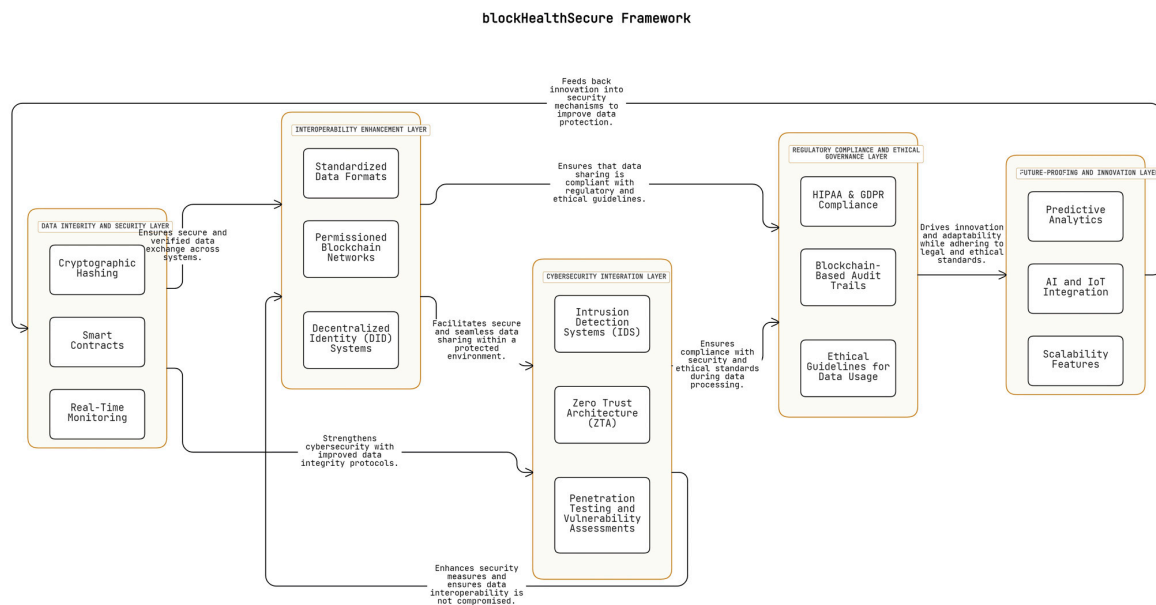


Figure 2. blockHealthSecure Framework.

4.2.1. Data Integrity and Security Layer

The data integrity and security layer serve as the core foundation, which is focused on ensuring that healthcare data remain accurate, secure, and immutable. This layer includes three key components:

- **Cryptographic hashing:** Hashing algorithms are used to verify data integrity by converting sensitive information into a fixed size of characters, ensuring that any alteration in the data can be detected.
- **Smart contracts:** Smart contracts are self-executing agreements where the terms are embedded directly in the code. They automate data access and exchange, ensuring transactions are secure and resistant to tampering.
- **Real-time monitoring:** This component enables continuous monitoring of healthcare systems to identify unauthorized access or potential security breaches, delivering real-time alerts and ensuring a swift response.

4.2.2. Interoperability Enhancement Layer

The Interoperability Enhancement Layer guarantees the secure and efficient sharing of data among various healthcare providers, fostering collaboration and enhancing patient outcomes. This layer includes the following components:

- **Standardized data formats:** Standardized data formats like HL7 and FHIR (Fast Healthcare Interoperability Resources) enable the seamless transfer of medical information between different systems.
- **Permissioned blockchain networks:** These are blockchain networks in which participants are verified, ensuring that only authorized entities can access and share data, thereby promoting trust within healthcare networks.
- **Decentralized Identity (DID) systems:** DID systems empower patients and healthcare providers to manage their identities securely, ensuring privacy while allowing for effective data sharing.

4.2.3. Cybersecurity Integration Layer

The cybersecurity integration layer protects the system from potential cyber threats. It incorporates several advanced cybersecurity measures:

- Intrusion Detection Systems (IDS): IDS track network traffic for any suspicious activity and potential threats, offering early alerts for unauthorized access attempts.
- Zero Trust Architecture (ZTA): ZTA ensures that no device or user is automatically trusted, necessitating ongoing authentication and validation to reduce vulnerabilities.
- Penetration testing and vulnerability assessments: These proactive measures identify and assess system vulnerabilities, allowing for timely patching and hardening of the healthcare infrastructure.

4.2.4. Regulatory Compliance and Ethical Governance Layer

This layer guarantees that the system meets regulatory standards and follows ethical guidelines in handling healthcare data:

- HIPAA/GDPR compliance: Healthcare systems must adhere to stringent data protection laws, such as HIPAA in the U.S. and the GDPR in Europe, to ensure patient data privacy and security.
- Blockchain-based audit trails: Blockchain offers an unchangeable and transparent record of data transactions, ensuring accountability and providing a clear trace of all interactions with healthcare data.
- Ethical guidelines for data usage: Ethical guidelines govern the appropriate use of patient data, ensuring that patient rights and privacy are respected throughout the data lifecycle.

4.2.5. Future-Proofing and Innovation Layer

The future-proofing and innovation layer focuses on ensuring that the healthcare system remains adaptable and resilient to future technological changes and health crises. Key components include:

- Predictive analysis: Predictive models can forecast health trends and patient needs, enabling healthcare providers to respond proactively to potential public health emergencies.
- AI and IoT integration: Combining AI with the IoT enhances patient monitoring, enables personalized healthcare services, and supports better decision-making.
- Scalability features: The framework is built to scale as healthcare data volume grows, ensuring it can manage large datasets while preserving performance and security.

4.3. Connectivity and Feedback Loops

The blockHealthSecure Framework emphasizes the interconnectedness of its components, with feedback loops to enhance its adaptability. For instance, innovations in the future-proofing and innovation layer can drive improvements in the data integrity and security layer by introducing more robust encryption techniques. Similarly, cybersecurity measures such as Zero Trust Architecture in the cybersecurity integration layer can inform data-sharing protocols in the interoperability enhancement layer, ensuring that security does not hinder effective collaboration.

The regulatory compliance and ethical governance layer ensure that as the framework evolves, it does so within the confines of legal and ethical standards. This feedback loop ensures that new technologies and practices, such as AI and blockchain, remain in compliance with data protection laws, thus reinforcing patient trust and ensuring the long-term sustainability of the healthcare system.

4.4. Roles of Different Participants in the blockHealthSecure Framework

The blockHealthSecure Framework includes multiple stakeholders, each with specific roles and responsibilities in maintaining data security, access control, and compliance. Key participants and their roles are represented in Table 4.

Table 4. Key participants and their roles.

Participant	Role in the Blockchain System
Patients	Own and control access to their health records using Decentralized Identity (DID) mechanisms.
Healthcare Providers	Upload medical data securely using cryptographic hashing and interact with smart contracts for automated data verification.
Regulatory Authorities	Monitor compliance, conduct audits, and verify transactions on the blockchain to ensure regulatory adherence.
Insurance Companies	Access patient-approved medical records for claims processing, reducing fraud and ensuring faster approvals.
Cybersecurity Teams	Oversee intrusion detection, malware analysis, and system monitoring, ensuring security across all layers.

Following are the roles of different participants in Data Access and Permission Management

- Patients retain full control over their personal health records (PHR) via blockchain-based access control.
- Healthcare providers must request data access, which is authorized via smart contracts and validated through blockchain authentication mechanisms.
- Regulatory bodies can audit blockchain logs but cannot modify patient records, ensuring transparency and compliance.

This decentralized participant structure enhances data privacy, operational efficiency, and transparency in healthcare ecosystems.

4.5. Operation and Control Mechanisms of Smart Contracts

Smart contracts play a critical role in automating, securing, and enforcing healthcare processes within the blockHealthSecure Framework. These self-executing contracts handle data sharing, consent management, and compliance enforcement without human intervention. Table 5 represents the different functions and its description that appears on control mechanism of Smart contracts.

Table 5. Smart contract functionalities.

Function	Description
Patient Consent Management	Automates patient approval and revocation of medical data access requests.
Medical Record Validation	Ensures that only verified healthcare providers can update patient records.
Insurance Claims Processing	Automates claim verification, reducing fraudulent transactions and improving efficiency.

Governance and Security of Smart Contracts are executed as follows:

- Deployment: Smart contracts are initiated by healthcare providers and reviewed by regulatory bodies before activation.
- Modification control: Any updates require multi-signature approval from at least two regulatory bodies, preventing unauthorized tampering.
- Auditing mechanisms: Regular blockchain audits and automated alerts detect anomalies and security breaches.

The following is an example of the workflow of smart contract execution:

Scenario: A patient grants a specialist access to their medical records.

Step 1:

- The patient authorizes access through the Decentralized Identity (DID) system.
- A smart contract logs the request and encrypts the patient's approval on the blockchain.

Step 2:

- The healthcare provider submits a request to retrieve the medical record.
- The smart contract verifies authorization and grants time-limited access.

Step 3:

- The provider accesses the record securely, and the blockchain logs the transaction, ensuring immutability and auditability.
- If the provider attempts unauthorized access, the Intrusion Detection System (IDS) triggers an alert, revoking access.

This smart contract execution model ensures secure, traceable, and automated medical data exchange, reducing the risk of unauthorized access and compliance violations.

5. Blockchain and Cybersecurity Integration in Post-Pandemic Healthcare Systems

The COVID-19 pandemic highlighted weaknesses in healthcare systems, especially regarding data security, interoperability, and patient privacy. Blockchain technology, with its decentralized and immutable nature, offers a solution to these issues when paired with strong cybersecurity practices. This section examines how the integration of blockchain and cybersecurity can transform healthcare systems, focusing on how this convergence helps protect sensitive health information and supports secure, efficient healthcare delivery in the post-pandemic era.

5.1. The Role of Blockchain in Healthcare

Blockchain technology provides several benefits for healthcare systems. Table 6 outlines the key functions of blockchain in healthcare with its benefits and examples.

Table 6. The role of blockchain in healthcare.

Role	Description	Benefits	Example	Ref.
Data Integrity	Blockchain's immutable ledger ensures that any alterations to data are permanently recorded, providing a transparent and secure audit trail.	Reduces fraud and unauthorized modifications.	Tracking changes in Electronic Medical Records (EMRs).	[21]
Decentralized Data Management	Eliminate the need for a central authority by distributing data across various nodes in the blockchain network.	Remove single points of failure, improving system resilience	Decentralized access for hospital networks.	[15]
Secure Data Sharing	Facilitates encrypted and efficient data exchange among healthcare providers while maintaining authenticity.	Enhances interoperability and reduces data silos.	Sharing lab results between hospitals.	[16]
Patient Empowerment	Decentralized Identity (DID) systems empower patients to control their personal health data, allowing them to decide who can access it.	Builds trust, improves data transparency, and supports privacy.	Patients managing their digital health records.	[15]
Data Provenance	It monitors the source and changes to data, ensuring accountability and verifying the authenticity of data usage.	Ensures reliability and reduces data tampering.	Maintaining an accurate supply chain for medical devices	[22]
Compliance and Reporting	Automates compliance tracking for regulations like HIPAA and GDPR through smart contracts and immutable records.	Reduces administrative burden, ensures regulatory adherence.	Automating GDPR-compliant data access logs.	[13]

Table 6. Cont.

Role	Description	Benefits	Example	Ref.
Fraud Detection	Blockchains' transparency enables real-time fraud detection and accountability in medical billing and insurance claims.	Minimizes financial losses from fraudulent activities.	Verifying insurance claims against treatment records.	[16]
Scalable Research Collaboration	Provides a secure, shared database for researchers to store and share anonymized data without compromising patient privacy.	Facilitates global research collaboration.	Sharing anonymized genomic data for medical research.	[23]
Supply Chain Integrity	Tracks the journey of pharmaceuticals and medical supplies from production to delivery, ensuring authenticity.	Reduces counterfeit medicines and improves supply chain efficiency.	Monitoring vaccine distribution.	[22,24]

5.2. Cybersecurity Measures in Post-Pandemic Healthcare Systems

The swift digital transformation of healthcare systems during the COVID-19 pandemic has revealed several cybersecurity challenges. As healthcare providers increasingly adopt technologies such as telemedicine, electronic health records (EHRs), and Internet of Things (IoT) devices, the demand for advanced cybersecurity solutions has become critical. The following subsections outline various cybersecurity strategies that can bolster healthcare systems' resilience in the post-pandemic era.

5.2.1. Strengthening Perimeter Security

The surge in digital health services during the pandemic has made perimeter security a critical concern. Healthcare organizations must protect their network infrastructure from external threats, ensuring that unauthorized entities cannot gain access to sensitive data. Technologies such as firewalls, VPNs, and advanced Intrusion Detection Systems (IDS) are foundational in protecting healthcare systems from cyber threats. Moreover, healthcare providers must continually monitor network traffic and establish real-time alerts for suspicious activities [25].

5.2.2. Implementing Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) is a robust security model gaining popularity in healthcare. It operates on the principle that no user, device, or application should be trusted by default, even if they are inside the network perimeter. ZTA mandates continuous verification for every user and device accessing vital healthcare systems. By implementing ZTA, healthcare organizations can greatly minimize the risk of insider threats and data breaches. This architecture ensures that access is granted based on identity and behavior, enhancing security at multiple layers [20].

5.2.3. Adopting Endpoint Security Solutions

As IoT devices and other connected technologies become ubiquitous in healthcare, security endpoints are crucial. Medical devices such as pacemakers, smart monitoring systems, and wearable health trackers provide multiple entry points for cybercriminals. Protecting these devices requires multi-layered security approaches, including encryption, secure firmware, and anomaly detection. Endpoint protection solutions, including antivirus software, behavioral analysis tools, and network segmentation, play a critical role in defending these devices from malware and other attacks [26].

5.2.4. Enhancing Data Encryption

Data encryption is a highly effective way to protect patient information, both while being transmitted and when stored. Healthcare systems must adopt robust encryption standards, such as Advanced Encryption Standard (AES) and RSA encryption, to safeguard sensitive data from unauthorized access. Furthermore, blockchain-based encryption offers additional layers of protection, ensuring that patient data are immutable and verifiable, thus minimizing the risks of data tempering. This dual approach of encryption and blockchain ensures that data remain secure and accessible only to authorized individuals.

5.2.5. Leveraging AI for Threat Detection

AI is transforming cybersecurity in healthcare by improving the speed and accuracy of threat detection. Machine learning algorithms can process vast amounts of data to identify unusual behaviors and forecast potential security risks. These AI-driven systems can identify patterns of unauthorized access, phishing attacks, and other forms of cyber intrusion, enabling faster response times. AI also assists in automating threat hunting, reducing the workload of cybersecurity professionals, and improving overall efficiency.

5.2.6. Compliance with Regulatory Standards

In the healthcare industry, cybersecurity must comply with regulatory standards like HIPAA and GDPR. These standards mandate specific cybersecurity practices, including data access control, audit trails, and breach notification procedures. Compliance with these regulations not only ensures data protection but also mitigates legal risks and penalties for data breaches. Moreover, integrating blockchain technology can further enhance compliance by providing transparent and immutable audit trails for every transaction involving patient data [27].

5.2.7. Improving Incident Response Mechanisms

Cybersecurity incidents in healthcare need to be handled promptly to avoid large-scale data breaches. A thorough incident response plan, with clear protocols for detecting, containing, and mitigating cyber threats, is crucial for reducing the impact of attacks. The integration of blockchain for real-time logging and tracking of access events enhances the transparency and accountability of the incident response process [28]. Moreover, AI can assist in automating incident detection, significantly reducing response time and improving the efficiency of healthcare cybersecurity teams.

5.2.8. Fostering Cybersecurity Awareness

Human error continues to be a major vulnerability in healthcare cybersecurity. Training healthcare professionals and patients on secure practices—such as identifying phishing attempts, using strong passwords, and protecting personal information—is essential for minimizing the risk of cyberattacks. Ongoing training programs and cybersecurity awareness campaigns help staff recognize potential threats and act swiftly to mitigate risks [29].

5.2.9. Resilience Through Redundancy

Redundancy in cybersecurity involves setting up backup systems and disaster recovery procedures to ensure that essential healthcare operations can continue during a cyberattack. Healthcare providers must establish redundant systems for data storage, server infrastructure, and application services. By distributing healthcare data across multiple locations and utilizing blockchain for decentralized storage, healthcare organizations can increase their resilience against data loss and system downtime.

6. Challenges and Potential Benefits

Integrating blockchain technology and cybersecurity measures into healthcare systems presents both challenges and opportunities. The blockHealthSecure framework aims to address healthcare's evolving needs by enhancing data integrity, interoperability, cybersecurity, and regulatory compliance. However, there are several hurdles to its widespread adoption and implementation.

6.1. Challenges

Although the blockHealthSecure framework offers a comprehensive solution for security healthcare systems, several challenges remain in its practical implementation.

6.1.1. Technical and Scalability Issues

The data integrity and security layer of the blockHealthSecure framework leverages blockchain technology, which provides decentralization and cryptographic techniques to enhance data protection. However, the scalability of blockchain networks remains a concern. Healthcare systems generate large volumes of data, and blockchain platforms, especially public ones, struggle to handle these data flows without compromising performance. The process of storing vast amounts of medical records across a decentralized network may lead to increased latency, creating difficulties in accessing real-time data, which is essential in healthcare environments. Addressing scalability issues requires developing more efficient blockchain solutions with higher transaction throughput and lower processing times [30].

6.1.2. Regulatory and Compliance Issues

Blockchain's ability to provide immutable records, while valuable in many applications, presents a challenge in healthcare, particularly when it comes to compliance with privacy regulations. Healthcare data are governed by stringent regulations like the HIPAA and the GDPR, which safeguard patient privacy and provide the right to delete personal data upon request. Blockchain's immutability complicates these requirements, as it makes deleting or altering data challenging once they are stored on the ledger [31]. This conflict between blockchain's inherent characteristics and regulatory requirements calls for innovative solutions to reconcile the two. It is essential to develop strategies that allow for data modification while maintaining blockchain's decentralized and secure nature [32].

6.1.3. Adoption Barriers

A major obstacle to integrating blockchain and cybersecurity solutions in healthcare systems is the lack of technological preparedness and resistance to change. Healthcare organizations, particularly small and medium-sized ones, may find the costs of implementing blockchain technology prohibitive. Furthermore, healthcare professionals need extensive training to understand blockchain and its implications for data security and privacy. Resistance to change poses another challenge, as many healthcare providers are familiar with traditional data management systems and may hesitate to embrace new technologies. These factors slow adoption rates and prevent the healthcare sector from fully realizing the potential of blockchain.

6.1.4. Interoperability Challenges

A key objective of the Interoperability Enhancement Layer in the blockHealthSecure framework is to enhance data exchange across various healthcare systems. However, many existing healthcare systems are not designed to interact with blockchain-based networks, creating significant interoperability challenges. Current medical records management systems may not support blockchain integration or may require significant modifications

to do so. A major challenge in integrating blockchain into healthcare systems is the need for standardized protocols that enable smooth data exchange across different platforms.

6.1.5. Ethical and Privacy Concerns

Blockchain technology's ability to provide transparency and traceability in healthcare transactions is a double-edged sword. While transparency is essential for ensuring data integrity and preventing fraud, it also raises privacy concerns. Healthcare data are highly sensitive, and the idea of publicly accessible transaction records can be alarming to patients. Although blockchain can provide secure, permissioned access to healthcare data, ethical concerns related to data ownership, patient consent, and control over personal health information persist. These concerns must be resolved to ensure that blockchain systems are implemented in a manner that upholds patient autonomy and privacy.

6.2. Potential Benefits

Despite these challenges, the blockHealthSecure framework offers numerous potential advantages that could transform healthcare systems by enhancing data security, interoperability, and overall efficiency.

6.2.1. Improved Data Security and Privacy

The data integrity and security layer of the blockHealthSecure framework strengthens the security and privacy of healthcare data through blockchain's cryptographic features. Blockchain's decentralized design minimizes the risk of single points of failure, increasing resilience against cyberattacks and unauthorized access. Additionally, healthcare data can be stored in encrypted blocks, ensuring that only authorized individuals can access sensitive information [33]. The ability for patients to control who can access their data further protects privacy, allowing them to grant or revoke access according to their preferences.

6.2.2. Enhanced Interoperability

The interoperability enhancement layer of the blockHealthSecure framework provides the foundation for seamless data sharing between various healthcare institutions. Blockchain provides a standardized, decentralized platform for data exchange, enabling healthcare providers to securely share patient information across various systems. This interoperability enhances care coordination, allowing providers to access real-time data from any institution, which in turn improves diagnostic accuracy and treatment outcomes [34]. Additionally, blockchain's capability to provide a transparent, tamper-resistant record guarantees that data remain accurate and reliable throughout the entire process.

6.2.3. Cost Reduction

Blockchain technology can reduce operational costs within healthcare systems by eliminating intermediaries and reducing administrative overhead. The Cybersecurity Integration Layer of the blockHealthSecure framework utilizes smart contracts to automate administrative tasks like billing and claims processing. By decreasing the dependence on third-party services and reducing the risk of fraud, blockchain helps streamline workflows and enhance the efficiency of healthcare operations [35].

6.2.4. Enhanced Patient Control

Blockchain in healthcare enhances patients to control their personal health information. The regulatory compliance and ethical governance layer in the blockHealthSecure framework emphasize the importance of patient consent management. Blockchain allows patients to grant or revoke access to their health data as needed, giving them control over

who views their information and when. This increased control builds trust between patients and healthcare providers, encouraging data sharing and enhancing care.

6.2.5. Transparency and Accountability

The blockHealthSecure framework fosters transparency and accountability by leveraging blockchain's immutable ledger. Every transaction recorded on the blockchain is permanent and unchangeable, offering a clear and verifiable audit trail. This transparency makes it easier to track data access and usage, allowing healthcare providers and regulators to identify unauthorized actions and hold individuals accountable for breaches [36]. Such transparency can help build trust in healthcare systems, as patients can be assured that their data are being handled responsibly.

6.2.6. Future Innovation and Scalability

The future-proofing and innovation layer of the blockHealthSecure framework guarantees the system remains adaptable and scalable. Blockchain supports the integration of emerging technologies like AI and the IoT, which will improve the real-time monitoring and analysis of healthcare data. For example, AI algorithms can analyze patient data stored on the blockchain to predict health outcomes or identify potential risks, enabling proactive care management [37]. By supporting emerging technologies, blockchain enables healthcare systems to remain flexible and responsive to new challenges and innovations.

Figure 3 illustrates how the layered structure of the framework addresses critical challenges in the post-pandemic healthcare system and translates them into tangible benefits. Each identified challenge, including technical and scalability issues, regulatory compliance hurdles, adoption barriers, interoperability challenges, and ethical and privacy concerns, is mapped to specific framework layers. For instance, the interoperability enhancement layer resolves compatibility issues among healthcare systems, while the cybersecurity integration layer mitigates privacy and ethical risks through robust intrusion detection systems. The regulatory compliance and ethical governance layer ensure adherence to legal frameworks and ethical practices, addressing regulatory complexities. These layers, in turn, deliver essential benefits, such as enhanced interoperability, improved data security, transparency, patient control, and future scalability. The connections in the figure highlight the interplay between challenges and solutions, emphasizing the framework's holistic approach to creating a secure, interoperable, and future-ready healthcare ecosystem.

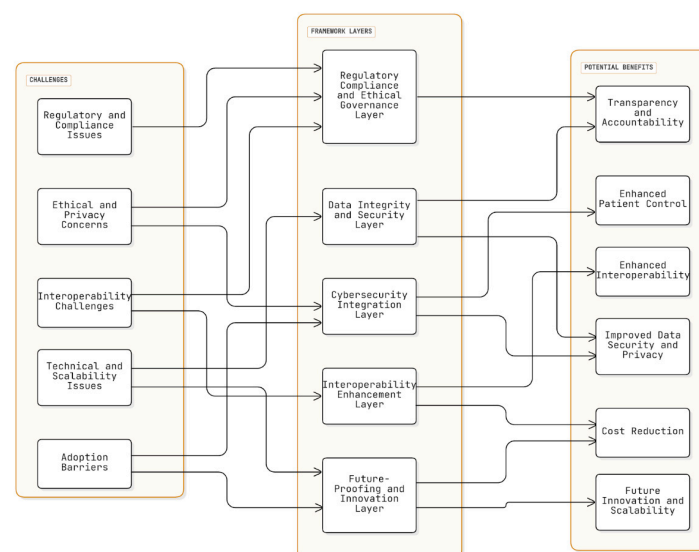


Figure 3. Mapping challenges to potential benefits in the blockHealthSecure Framework.

7. Future Prospects and Innovations

Blockchain technology has garnered significant interest across various industries due to its disruptive features. Its potential for global adoption is evident, as numerous studies have explored its applications. As a secure and immutable digital ledger, blockchain records transactions in a variable and permanent way, making it resistant to tampering [38]. Cryptography is employed to encrypt data, safeguarding them against security risks like unauthorized manipulation. The main risks associated with centralized systems are human error, hacking, and data loss. Cloud storage security and resilience to hackers can be improved with blockchain technology. Blockchain does not address some of the most significant challenges in the digital transformation of the healthcare sector, such as the lack of data interoperability, nor does it provide any additional benefits in these areas.

8. Conclusions

This research emphasizes the transformative potential of blockchain technology and cybersecurity in tackling key challenges within the healthcare system in the post-pandemic era. The integration of blockchain's immutable, decentralized nature with advanced cyber defense mechanisms effectively mitigates vulnerabilities in healthcare data security and interoperability. By leveraging the strengths of these technologies, the blockHealthSecure framework provides a comprehensive approach to enhancing the resilience and robustness of healthcare systems, particularly in the face of global health crises and pandemics. This study also underscores the importance of proactive advancements in blockchain and cybersecurity to prepare healthcare systems for emerging threats. The framework's layered approach ensures adaptability, scalability, and compliance with regulatory and ethical standards, providing a robust foundation for future healthcare innovations. Additionally, the research has explored the potential of predictive analytics, AI, and IoT integration to further enhance healthcare operations and security.

The findings of the study also highlight the role of blockchain technology in fostering patient trust and collaboration across the healthcare ecosystem. By ensuring secure, tamper-proof data sharing and offering patients greater control over their personal information, the blockHealthSecure Framework addresses key concerns around data privacy and ownership. These attributes are particularly critical in rebuilding confidence among stakeholders, especially in light of the data breaches and privacy violations that became more prevalent during the pandemic. The framework not only strengthens the technical infrastructure of healthcare systems but also aligns with ethical principles, creating a more transparent and patient-centric approach to healthcare operations.

Furthermore, the research underscores the necessity of continuous innovation to adapt to the ever-changing cybersecurity landscape. The integration of predictive analytics and AI-driven threat detection into the blockHealthSecure Framework is a critical step toward proactive risk management. These integrations enable healthcare systems to anticipate potential vulnerabilities and respond swiftly to emerging threats, reducing the likelihood of operational disruptions. The inclusion of IoT integration further enhances system efficiency, particularly in managing connected medical devices and ensuring their secure operation within healthcare networks.

Future research can extend this approach to domains beyond healthcare, such as autonomous vehicles, metaverse applications, and the broader medical industry. These domains require secure, transparent, and interoperable systems to address their unique challenges. With the rising frequency and complexity of cyberattacks, integrating blockchain technology with cybersecurity measures presents a promising approach to combat emerging threats across different industries. The findings reaffirm that the blockHealthSecure framework is not only a viable solution for contemporary healthcare challenges but also

a stepping stone for broader applications in a rapidly digitizing world. By consistently evolving and responding to emerging threats and opportunities, this integrated approach will be crucial in maintaining the security, integrity, and efficiency of digital ecosystems.

Author Contributions: Conceptualization, B.P.P. and N.K.; methodology, B.P.P. and N.K.; formal analysis, B.P.P.; investigation, B.P.P. and N.K.; resources, N.K.; data curation, B.P.P., N.K. and S.R.S.; writing—original draft preparation, B.P.P., N.K., S.R.S. and S.P.; writing—review and editing, B.P.P. and N.K.; visualization, B.P.P.; supervision, N.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Acknowledgments: We acknowledge all helping brains in their direct and indirect support for this study.

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

References

1. Miriam, H.; Doreen, D.; Dahiya, D.; Rene Robin, C.R. Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology. *Intell. Autom. Soft Comput.* **2023**, *35*, 1889. [CrossRef]
2. Pokharel, B.P.; Kshetri, N. blockLAW: Blockchain Technology for Legal Automation and Workflow--Cyber Ethics and Cybersecurity Platforms. *arXiv* **2024**, arXiv:2410.06143.
3. Kshetri, N.; Bhushal, C.S.; Pandey, P.S. BCT-CS: Blockchain technology applications for Cyber defense and Cybersecurity: A survey and solutions. *Int. J. Adv. Comput. Sci. Appl.* **2022**, *13*, 364–370. [CrossRef]
4. IBM Security X-Force Threat Intelligence Index 2024. IBM. Available online: <https://www.ibm.com/reports/threat-intelligence> (accessed on 20 December 2024).
5. 2024 Data Breach Investigations Report. Verizon Business. Available online: <https://www.verizon.com/business/resources/reports/dbir/> (accessed on 22 December 2024).
6. Begum, K.; Rashid, M.M.; Mozumder, M.A.I.; Kim, H.-C. Leveraging the Power of Blockchain for Secure Healthcare Data Management System. In Proceedings of the 2023 26th International Conference on Computer and Information Technology (ICCIT), Cox's Bazar, Bangladesh, 13–15 December 2023.
7. Sharma, S.R.; Kshetri, N. Blockchain Technology for Cybersecurity, Cyber Data, and Cyber Communication in Today's Cyber World. In *Blockchain Technology for Cyber Defense, Cybersecurity, and Countermeasures: Techniques, Solutions, and Applications*; CRC Press: Boca Raton, FL, USA, 2025; pp. 94–105.
8. HIPAA Compliance Guidelines. The HIPAA Journal. Available online: <https://www.hipaaajournal.com/hipaa-compliance-guidelines/> (accessed on 14 December 2024).
9. Everything You Need to Know About GDPR Compliance. GDPR.eu. Available online: <https://gdpr.eu/compliance/> (accessed on 14 December 2024).
10. The NIST Cybersecurity Framework (CSF) 2.0. 2024. Available online: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> (accessed on 13 November 2024).
11. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin White Paper. 2008. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 13 November 2024).
12. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
13. Ettaloui, N.; Arezki, S.; Gadi, T. An overview of blockchain-based Electronic Health Records and compliance with GDPR and HIPAA. *Data Metadata* **2023**, *2*, 166. [CrossRef]
14. Zhang, W.; Qamar, F.; Abdali, T.-A.N.; Hassan, R.; Jafri, S.T.; Nguyen, Q.N. Blockchain technology: Security issues, healthcare applications, challenges, and future trends. *Electronics* **2023**, *12*, 546. [CrossRef]
15. Satybaldy, A.; Hasselgren, A.; Nowostawski, M. Decentralized Identity Management for E-Health Applications: State-of-the-Art and Guidance for Future Work. *Blockchain Healthc. Today* **2022**, *5*. [CrossRef] [PubMed]

16. Haleem, A.; Javaid, M.; Singh, R.P.; Suman, R.; Rab, S. Blockchain technology applications in Healthcare: An overview. *Int. J. Intell. Netw.* **2021**, *2*, 130–139. [\[CrossRef\]](#)
17. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper. 2014. Available online: <https://ethereum.org/en/whitepaper/> (accessed on 9 November 2024).
18. Dubovitskaya, A.; Baig, F.; Xu, Z.; Shukla, R.; Zambani, P.S.; Swaminathan, A.; Jahangir, M.M.; Chowdhry, K.; Lachhani, R.; Idnani, N.; et al. Action-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. *J. Med. Internet Res.* **2020**, *22*, e13598. [\[CrossRef\]](#) [\[PubMed\]](#)
19. Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Xu, M. A survey on machine learning techniques for cyber security in the last decade. *IEEE Access* **2020**, *8*, 222310–222354. [\[CrossRef\]](#)
20. Chaturvedi, I.; Pawar, P.M.; Muthalagu, R.; Tamizharasan, P.S. Zero Trust Security Architecture for Digital Privacy in Healthcare. In *Springer Tracts in Electrical and Electronics Engineering*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 1–23. [\[CrossRef\]](#)
21. Ullah, F.; He, J.; Zhu, N.; Wajahat, A.; Nazir, A.; Qureshi, S.; Pathan, M.S.; Dev, S. Blockchain-enabled EHR Access Auditing: Enhancing Healthcare Data Security. *Heliyon* **2024**, *10*, e34407. [\[CrossRef\]](#) [\[PubMed\]](#)
22. Bajwa, J.; Munir, U.; Nori, A.; Williams, B. Artificial Intelligence in healthcare: Transforming the practice of medicine. *Future Healthc. J.* **2021**, *8*, e188–e194. [\[CrossRef\]](#) [\[PubMed\]](#)
23. Satamraju, K.P. Proof of concept of scalable integration of internet of things and blockchain in Healthcare. *Sensors* **2020**, *20*, 1389. [\[CrossRef\]](#)
24. Sarosh, P.; Parah, S.A.; Malik, B.A.; Hijji, M.; Muhammad, K. Real-time medical data security solution for Smart Healthcare. *IEEE Trans. Ind. Inform.* **2023**, *19*, 8137–8147. [\[CrossRef\]](#)
25. Yigzaw, K.Y.; Olabarriaga, S.D.; Michalas, A.; Marco-Ruiz, L.; Hillen, C.; Verginadis, Y.; de Oliveira, M.T.; Krefting, D.; Penzel, T.; Bowden, J.; et al. Health Data Security and Privacy: Challenges and solutions for the future. In *Roadmap to Successful Digital Health Ecosystems*; Academic Press: Cambridge, MA, USA, 2022; pp. 335–362. [\[CrossRef\]](#)
26. Pradhan, B.; Bhattacharyya, S.; Pal, K. IOT-based applications in healthcare devices. *J. Healthc. Eng.* **2021**, *2021*, 1–18. [\[CrossRef\]](#) [\[PubMed\]](#)
27. Adere, E. M Blockchain in healthcare and IOT: A systematic literature review. *Array* **2022**, *14*, 100139. [\[CrossRef\]](#)
28. Liu, H.; Crespo, R.G.; Martínez, O.S. Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts. *Healthcare* **2020**, *8*, 243. [\[CrossRef\]](#)
29. Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors* **2021**, *21*, 5119. [\[CrossRef\]](#)
30. Bodkhe, U.; Tanwar, S.; Parekh, K.; Khanpara, P.; Tyagi, S.; Kumar, N.; Alazab, M. Blockchain for Industry 4.0: A comprehensive review. *IEEE Access* **2020**, *8*, 79764–79800. [\[CrossRef\]](#)
31. Corte-Real, A.; Nunes, T.; da Cunha, P.R. Reflections about Blockchain in health data sharing: Navigating a disruptive technology. *Int. J. Environ. Res. Public Health* **2024**, *21*, 230. [\[CrossRef\]](#)
32. Onik Md, M.; Aich, S.; Yang, J.; Kim, C.-S.; Kim, H.-C. Blockchain in Healthcare: Challenges and solutions. In *Big Data Analytics for Intelligent Healthcare Management*; Academic Press: Cambridge, MA, USA, 2019; pp. 197–226. [\[CrossRef\]](#)
33. Angraal, S.; Krumholz, H.M.; Schulz, W.L. Blockchain technology: Applications in Health Care. *Circ. Cardiovasc. Qual. Outcomes* **2017**, *10*. [\[CrossRef\]](#) [\[PubMed\]](#)
34. Villarreal, E.R.; Garcia-Alonso, J.; Moguel, E.; Alegria, J.A. Blockchain for Healthcare Management Systems: A survey on interoperability and Security. *IEEE Access* **2023**, *11*, 5629–5652. [\[CrossRef\]](#)
35. Nzuva, S. Smart contracts implementation, applications, benefits, and limitations. *J. Inf. Eng. Appl.* **2019**, *9*, 63–75. [\[CrossRef\]](#)
36. Ndayizigamiye, P.; Dube, S. Potential adoption of blockchain technology to enhance transparency and accountability in the public healthcare system in South Africa. In Proceedings of the 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC), Vanderbijlpark, South Africa, 21–22 November 2019; pp. 1–5. [\[CrossRef\]](#)
37. Fatoum, H.; Hanna, S.; Halamka, J.D.; Sicker, D.C.; Spangenberg, P.; Hashmi, S.K. Blockchain integration with digital technology and the future of HealthCare Ecosystems: Systematic Review. *J. Med. Internet Res.* **2021**, *23*, e19846. [\[CrossRef\]](#) [\[PubMed\]](#)
38. Andrew, J.; Isravel, D.P.; Sagayam, K.M.; Bhushan, B.; Sei, Y.; Eunice, J. Blockchain for Healthcare Systems: Architecture, Security Challenges, Trends and Future Directions. *J. Netw. Comput. Appl.* **2023**, *215*, 103633. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.