IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

Blockchain-Based Cybersecurity and Data Privacy in Healthcare Systems Review of Challenges and Emerging Trends

Mr. Kapil Ahir
Assistant Professor, Department of Computer Sciences and Applications
Mandsaur University, Mandsaur
kapil.ahir@meu.edu.in

Abstract: *The increasing reliance on Electronic Health Records (EHRs), telemedicine, and interconnected medical devices has introduced significant cybersecurity and privacy challenges in modern healthcare systems. Centralized data architectures are particularly vulnerable to breaches, system failures, and interoperability issues. Blockchain technology offers a promising alternative by providing a decentralized, secure, and tamper-resistant framework for managing sensitive health data. This review explores how blockchain enhances cybersecurity in healthcare through features such as transparent audit trails, data immutability, decentralized trust, and patient-centric control. It categorizes blockchain types public, private, and consortium and examines their relevance to healthcare use cases. The paper also identifies key cybersecurity threats facing the sector, including vulnerabilities in remote operations, weak incident response mechanisms, and governance gaps. Blockchain's potential to enable secure data sharing, ensure data provenance, detect fraud, and automate regulatory compliance is critically assessed. Furthermore, the integration of blockchain with emerging technologies such as artificial intelligence (AI), federated learning, and token-based incentive models is explored. Despite its transformative potential, widespread adoption remains limited due to technical, organizational, and regulatory barriers. This paper advocates for a strategic and cautious approach to blockchain adoption in healthcare, aiming to build more secure, interoperable, and resilient digital health ecosystems.*

Keywords: *Blockchain, cybersecurity, data privacy, healthcare systems, Decentralized Systems, Smart Contracts, Federated Learning*

I. INTRODUCTION

Digital technologies have transformed the healthcare industry by enabling the development of modern information systems and the integration of smart devices, which have enhanced communication with patients and improved access to treatments[1]. Key advancements such as electronic health records (EHR) have replaced traditional paper records, significantly increasing the efficiency of health services. Telecommunication networks and services have facilitated better communication and collaboration between patients and healthcare professionals. Additionally, innovations like mHealth, telehealth, and telemedicine have streamlined patient management processes and elevated the overall quality of healthcare services[2]. While these innovations have improved efficiency and patient care outcomes, they have also introduced critical challenges related to data security, privacy, interoperability, and trustworthiness of healthcare information systems.

Cybersecurity is a growing concern in the healthcare system. Due to the sensitive and confidential nature of the information that is stored and transmitted within this system[3]. Healthcare organization faces numerous modern threats to their systems and networks [4]. Cyber threats affect healthcare more than other industries because they are highly specialized. Most healthcare companies possess and store substantive personal information, finances, and health

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

records. The amount and type of information that healthcare databases store make it possible for hackers who seek vulnerabilities in information systems to consider the healthcare databases utterly irresistible[5][6].

Traditional healthcare systems often rely on centralized architectures, which create single points of failure and increase vulnerability to internal and external attacks[7]. Additionally, these systems struggle with interoperability and access control, particularly in multi-institutional or cross-border healthcare settings. As a result, there is a pressing need for novel approaches that can decentralize trust, improve auditability, and ensure secure and seamless data exchange.

Blockchain technology offers a promising solution to these security challenges. It creates a tamper-proof record of transactions, ensuring data integrity and preventing unauthorized alterations[8]. This technology not only safeguards patient information but also facilitates secure, transparent sharing among authorized providers, enhancing patient privacy and trust[9]. Thus, incorporating blockchain into healthcare infrastructure marks a pivotal step toward achieving secure, interoperable, and trustworthy data management.

Blockchain offers a secure and decentralized solution to the growing cybersecurity and privacy challenges in healthcare. Ensuring data integrity, transparency, and trust, it enhances patient care and system reliability. Integrating blockchain into healthcare systems marks a vital step toward safer and more efficient data management.

1.1 Structured of the paper

The structure of this paper is as follows: Section II provides an explanation of blockchain fundamentals. Section III discusses key cybersecurity and privacy issues in healthcare. Section IV presents blockchain-based solutions, emerging trends, and limitations. Section V reviews related literature and existing frameworks. Section VI concludes with insights and future research directions.

II. BLOCKCHAIN BASICS AND CORE CONCEPTS

Blockchain is a decentralized, unchangeable database that simplifies the tracking of assets and recording of transactions in a corporate network. A blockchain is composed of an expanding collection of documents, known as blocks, that are securely linked to one another using encryption. Each block includes transaction information, a timestamp, and a cryptographic hash of the preceding block. The timestamp indicates that the transaction data was present at the time the block was produced. The blocks effectively create a chain since each block holds information about the one before it, making them interconnected. Thus, once a transaction has been recorded, it cannot be undone without also undoing all following blocks, rendering blockchain transactions irreversible[10].

A. Key Features of blockchain in healthcare

The use of blockchain in healthcare helps ensure data security, improve the accuracy of information, increase transparency, and allow systems to work more seamlessly together[11]. It enables smart contracts to manage consent and execute automated processes, while ensuring the security of data exchange in clinical trials [12]. These points, as shown in fig. 1, are further discussed below to demonstrate how they contribute to better healthcare practices.

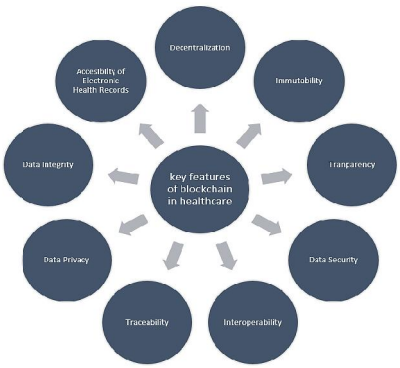

Figure 1: Key features of blockchain in healthcare

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

Here are the key features of blockchain in healthcare are as follows:

- Decentralization: Blockchain eliminates the need for a central authority, distributing the ledger across a network, making it more resilient to single points of failure and enhancing data security[13].
- Immutability: Once data is recorded on the blockchain, it cannot be altered or deleted, ensuring data integrity and traceability.
- Transparency: Blockchain allows for transparent and verifiable data sharing, facilitating better collaboration and accountability among stakeholders in the healthcare ecosystem.
- Data Security: Cryptographic principles and distributed ledger technology enhance data security, making it difficult for unauthorized individuals to access or modify patient records.
- Interoperability: Blockchain can help standardize data formats and protocols, improving data exchange and interoperability between different systems and organizations.
- Traceability: Blockchain allows for the creation of a complete audit trail, enabling the tracking of medications and medical devices throughout the supply chain, reducing counterfeiting and improving patient safety.
- Data Privacy: While blockchain enhances transparency, it can also be used to protect patient data privacy by implementing access control mechanisms and pseudonymization techniques.
- Data Integrity: Blockchain ensures the integrity of data by preventing modifications and providing a verifiable record of transactions and events.
- Accessibility of Electronic Health Records: Blockchain can improve access to electronic health records by providing secure and decentralized storage and sharing mechanisms[14].

B. Types of Blockchain

Blockchain technology can be broadly classified into different types based on access permissions and decentralization levels. Common blockchain kinds are public, private, consortium, and hybrid[15]. The following categories, along with their primary characteristics, are described below:

1. Public Blockchain: A disruptive, permissionless, and open-source technology based on the Proof of Work (PoW) consensus algorithm, where anyone can join the network, perform transactions, and audit the blockchain. Transactions are transparent and visible to all participants. Public blockchains, such as Bitcoin, Ethereum, Litecoin, Monero, Dash, and Dogecoin, utilize this model.
2. Private Blockchain: Private blockchains are permissioned networks where only the owning organization can run full nodes and make transactions. Their security relies on the trustworthiness of the validating entity. They offer greater speed, trust, and control, making them suitable for applications requiring high confidentiality and privacy. Examples include Multichain and Bank Chain.
3. Federated Blockchain: Federated or Consortium blockchains are semi-permissioned networks where a group of selected members run full nodes and handle transactions. They offer greater scalability and transaction privacy, with only authorized participants allowed to audit the ledger. Examples include R3, EWF, B3i, and Corda. A comparison in Table I helps differentiate them shown below:

Parameters	Public	Private	Federated
Type	Permissionless	Permissioned	Semi-permissioned
Network	Decentralized	Partially ecentralized	A hybrid between public and private
Access	Anyone, Anywhere	Single entity control	Set of nodes control
Speed	Slower	Faster	Moderate
Example	Bitcoin, Ethereum	Bankchain, ultichain	R3, Corda

Table I: Differences Between Various Types of Blockchain

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

III. DATA PRIVACY AND CYBERSECURITY CHALLENGES IN HEALTHCARE

Data privacy and cybersecurity present significant challenges for healthcare systems today. Due to the sensitive nature of medical data and the increasing reliance on digital technologies, these organizations are prime targets for cyberattacks and data breaches[16]. Key issues include protecting patient information from unauthorized access, preventing insider threats, managing ransomware and malware attacks, and ensuring compliance with complex regulatory frameworks such as HIPAA and GDPR. As healthcare systems digitize and integrate technologies like EHRs, telehealth, and IoMT, they face growing cybersecurity threats[17]. These developments create new attack surfaces that traditional security models cannot adequately protect. Addressing data privacy and system integrity requires understanding a complex and evolving risk landscape.

The following subsections outline the primary cybersecurity and data privacy challenges faced by healthcare systems today, categorized according to technical, organizational, and human factors:

a) Remote Working Risks

Remote desktop protocols (RDP) and virtual private networks (VPNs) are commonly used carry known vulnerabilities. Attackers exploit exposed RDP ports and VPN flaws. The growing number of wireless and IoT devices, combined with DDoS attacks, poses an additional risk to remote work environments.

b) Endpoint Device Vulnerabilities

Many medical and patient-monitoring devices are unpatched or outdated, particularly those adopted rapidly. Increased use of personal devices and integration of new equipment with legacy systems elevate risks such as phishing, ransomware, and data breaches due to endpoint complexity.

c) Human Error

Most security incidents result from human error, especially under stressful conditions or rapid changes in work environments. Healthcare staff may fall victim to phishing or social engineering, particularly during crises, and the sector lacks proper root cause analysis to prevent recurring mistakes.

d) Low Cybersecurity Awareness

Healthcare personnel often lack awareness of cybersecurity risks and their consequences[18]. Training is minimal, and guidance for identifying threats like phishing is insufficient. This gap became more critical due to increased misinformation and targeted scams.

e) Board-Level and Strategic Gaps

Executives in healthcare organizations often lack a clear understanding of cyber risks and their impact on clinical outcomes. A lack of a clear matrix connecting strategic healthcare goals to cybersecurity priorities results in weak governance and underprioritized security investments.

f) Inadequate Business Continuity Planning

Many healthcare institutions have weak data protection mechanisms and rely heavily on insecure third-party vendors. There is minimal encryption control, poor health information exchange protocols, and little consideration of cybersecurity from the outset of projects, compromising resilience and recovery.

g) Fragmented Incident Response

Cyberattacks are often detected late, giving attackers more time to explore systems. Responses are reactive, coordination across teams is weak, and backup mechanisms are frequently inadequate, all of which worsen the impact of breaches.

h) Budget Constraints and Skill Shortages

Limited funding and a lack of qualified cybersecurity experts hinder proactive defense. Security is often overlooked in favor of uninterrupted service delivery, preventing healthcare organizations from adapting securely at the necessary pace.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 10, April 2026 Impact Factor: 8.2

i) Insecure Medical Cyber-Physical Systems

Medical devices, especially IoT-enabled ones, often lack built-in cybersecurity capabilities like patch management[19]. Their integration into hospital networks makes the entire infrastructure more vulnerable, and security measures are often dependent on external manufacturers[20].

IV. BLOCKCHAIN-ENABLED APPROACHES: EMERGING TRENDS, TECHNICAL CHALLENGES, AND LIMITATIONS

Blockchain-based solutions are bringing changes to financial, healthcare and supply chain industries by making information management decentralized, secure and transparent. With these systems, trust is higher, intermediaries are needed less and records cannot be changed[21]. New trends are emerging, including DeFi, digital health records on blockchain, and self-managed identity governance. Nevertheless, technical difficulties and limits make it hard for the technology to be used by everyone. Important challenges include the weak ability to scale, the high energy consumption of Proof of Work, gaps in how platforms can communicate with one another, and weak security in smart contracts. To provide a thorough understanding, the following subsections examine these emerging trends, technical issues, and challenges closely.

A. Blockchain-based solution for enhancing cybersecurity in healthcare systems

Traditional security methods often fall short in protecting sensitive health data. Blockchain offers decentralized and tamper-resistant solutions that enhance privacy, integrity, and resilience[22]. Table II below highlights key applications in healthcare cybersecurity:

Blockchain-Based Solution	Role in Healthcare Cybersecurity	Impact on Data Security and Privacy	Healthcare-Specific Use Case
Data Integrity Solution	Provides an immutable ledger where every medical data transaction is permanently recorded, ensuring traceability and auditability.	Prevents tampering, reinforces trust in clinical documentation.	Tracking historical updates in Electronic Medical Records (EMRs).
Decentralized Data Management Solution	Distributes health data across blockchain nodes, removing reliance on centralized servers.	Increases system resilience, reduces centralized attack risks.	Shared, decentralized access to patient records across hospitals.
Secure Data Sharing Solution	Facilitates encrypted, authenticated exchange of health data among authorized stakeholders via blockchain protocols.	Enhances interoperability and safeguards against data interception.	Secure sharing of radiology or pathology reports.
Patient-Controlled Access Solution	Uses Decentralized Identity (DID) systems to let patients grant or revoke access to their health data.	Empowers patients and ensures privacy compliance.	Patients managing access to their digital health wallets.
Data Provenance Solution	Tracks the origin and all modifications to health data, creating a transparent and verifiable data lineage.	Prevents data forgery and ensures accountability in clinical data usage.	Verifying source and integrity of clinical trial data.
Compliance Automation Solution	Leverages smart contracts and immutable records to automate compliance with HIPAA, GDPR, and similar regulations.	Streamlines audits and reduces regulatory violations.	Automated GDPR-compliant access logging and reporting.
Fraud Detection Solution	Uses blockchain transparency to detect inconsistencies and	Reduces financial fraud and improves billing	Validating insurance claims against blockchain-logged

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

	unauthorized transactions in healthcare billing and insurance claims.	transparency.	treatments.
Research Collaboration Solution	Offers a secure, blockchain-based environment for sharing anonymized datasets for research without breaching patient confidentiality.	Supports secure global research without violating privacy laws.	Sharing anonymized patient genomes for collaborative research.

Table II: Blockchain-Based Solution for Enhancing Cybersecurity in Healthcare Systems

B. Emerging Trends in Blockchain

As healthcare adopts digital advancements, blockchain is discovering new applications beyond securing data. Emerging trends, as shown in fig.2, indicate the integration of blockchain with related technologies to address various security, privacy, and interoperability challenges.

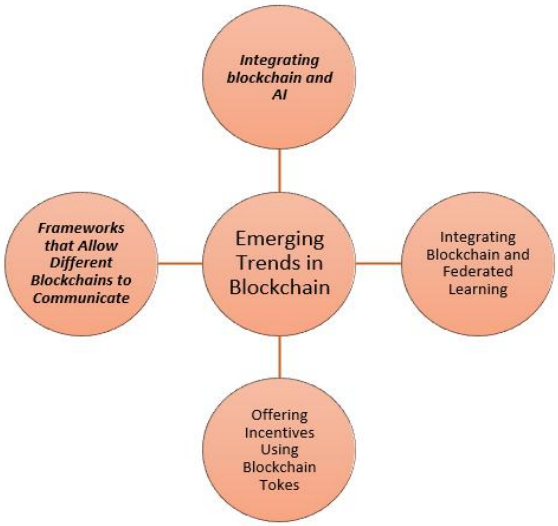

Figure 2: Emerging Trends in Blockchain

Here are the key emerging trends in blockchain are as follows:

Integrating blockchain and AI: By connecting blockchain and AI, the healthcare system can rely more on safe and interpretable AI-powered decision-making. With the use of blockchain, it is possible to review how AI comes to its treatment or diagnosis decisions, ensuring others can view, check and comply with the necessary rules.

Integrating Blockchain and Federated Learning: Federated learning allows institutions to teach models together, without disclosing patient information. Combining FL and blockchain lets it be coordinated more transparently and without the chance of changes[23]. By using this technology, it is possible to support secure and legal analytics, plus safeguard data even when shared between several parties.

Offering Incentives Using Blockchain Tokens: WITH blockchain, patients and healthcare providers are motivated to provide their health data for clinical or research purposes. It helps make the health data economy more decentralized and based on patients' priorities, so people feel trusted with their personal health information.

Frameworks that Allow Different Blockchains to Communicate: Companies are currently working on aligning and linking various blockchain platforms, using Hyperledger Fabric, MedBloc and Ethereum-based protocols to lead innovation. Their purpose is to make electronic health records (EHRs) usable worldwide, allow for their growth and promote regulations like HIPAA and GDPR.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 10, April 2026 Impact Factor: 8.2

C. Challenges and Limitations of Blockchain Implementation

D. Blockchain technology has already spread its roots in various industries and
E. domains including asset management, retail, monetary-use cases, digital currencies,
F. e-contracts, decentralized exchanges, and more. However, like every other technology,
G. Blockchain isn't perfect. There are certain implementational, operational, and
H. maintenance-related barriers that limit the effectiveness of blockchain technology.
I. 144
J. Blockchain Technology
K. Here are some current issues that clearly point to blockchain limitations:

Blockchain technology has already established a foothold in various industries and domains. However, like any technological innovation, blockchain has inherent limitations [24]. There are certain implementational, operational, and maintenance-related barriers that limit the effectiveness of blockchain technology[25]. Here are some current issues that clearly point to blockchain limitations:

1. Weak Performance: Blockchain is inherently slower than centralized systems due to additional cryptographic and consensus processes.
2. Signature Verification: Every transaction requires complex digital signature verification, increasing computational load.
3. Redundancy: Each node processes data independently, leading to inefficiencies compared to parallel processing in centralized systems.
4. High Energy Consumption: Mining and validation require powerful hardware and substantial energy, raising sustainability concerns.
5. Human Error: The accuracy of data input relies on users, and incorrect data can compromise the entire blockchain network.
6. Consensus Delays: Achieving agreement among distributed nodes takes time and resources, especially as network size grows.
7. Scalability and Storage Issues: Blockchain networks have limited transaction throughput and accumulate data rapidly, leading to storage constraints.
8. Lack of Technical Knowledge: Many users and stakeholders lack the technical understanding needed for effective implementation and oversight.
9. Manual Data Entry Errors: Mistakes during data entry can cause mismatches or outdated records, affecting system reliability.
10. Energy-Intensive Computation: Solving complex algorithms demands powerful computing, which consumes excessive energy.

V. LITERATURE REVIEW

This section provides an extensive review of the existing literature on blockchain-based cybersecurity and Data Privacy within healthcare systems. Following this review, Table III provides a concise summary of the examined studies, highlighting their primary focus areas, the challenges they address, and the significant findings that emerge from their analyses.

B. Kumar et al. (2025) explore the use of blockchain in healthcare, emphasizing its potential to improve data privacy, improve communication, and simplify the management of electronic health records (EHRs). Key features of the blockchain such as decentralization, immutability and cryptographic security have been analyzed in the context of healthcare. The review looks at notable developments, including blockchain-based frameworks for secure data shares, smart contracts for automated processes, and parallel healthcare systems combining it with artificial intelligence, as well as enabling efficiencies within the supply chain. This work provides a comprehensive analysis of blockchain's transformative potential and identifies areas for further research to ensure that it has been widely accepted[26].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

Singh et al. (2024) examine several cybersecurity risks facing healthcare systems, including data breaches, ransomware, insider threats, and regulatory compliance challenges. Insider threats whether intentional or accidental pose significant risks, as employees, contractors, and vendors with system access can compromise security. Compliance with stringent regulations like HIPAA further complicates cybersecurity management. The consequences of cyber incidents go beyond financial loss, affecting both reputation and patient safety. To address these challenges, healthcare organizations must implement proactive strategies such as strong risk management frameworks, secure system design, encryption, and continuous monitoring[27].

Sharma et al. (2024) provide an effective mechanism based on blockchain that can be utilized in the healthcare sector to overcome these issues. The key objective of the proposed model is to enable patients to use the data in order to support their care and to provide a strong consent mechanism for the creation and sharing of data between different organizations and applications. The proposed model is based on the principle that this combination of event-driven smart contracts, medical record data, and off-chain data storage is important for the adoption of blockchain-based solutions for healthcare. The results evaluated exhibit that the proposed blockchain-enabled model has shown satisfactory performance in the field of healthcare[28].

A. Kumar et al. (2024) suggest using Multichain blockchain technology as a strong approach to improve security in IoT healthcare contexts, to address these concerns. Multichain blockchain provides a distributed, unchangeable, and resistant-to-tampering method of storing data, guaranteeing the privacy, accuracy, and accessibility of patient information while reducing the dangers linked to centralized data repositories. Using a Multichain blockchain architecture in IoT healthcare systems enables the establishment of trust among many stakeholders, mitigates the risk of illegal access, and enhances the security of data exchange across diverse devices and platforms. This presents a comprehensive summary of the suggested methodology and its possible ramifications for augmenting security in healthcare environments provided by the Internet of Things[29].

Pawar et al. (2024) provide depth of coverage on the investments made by Federated Learning in healthcare and go on to detail clearly the underlying concepts, model aggregation methodologies, and implementation with privacy-preserving research protocols. Putting forward the central advantages, such as strong data privacy preservation, the possibility of personalization in model training, and model development scalability with efficiency, the present paper marks Federated Learning as an unparalleled tool for healthcare data analysis. This study has conclusively identified the potential of federated learning to transform healthcare: secure, collaborative, and data-driven medical research with supreme improvement potential for patient outcomes[30].

Lindbergh and De Morais Barroca Filho (2024) systematically map Blockchain technology's role in healthcare, aiming to summarize the domain and pinpoint future research directions. It assesses blockchain's characteristics, issues, platforms, and challenges within healthcare, analyzing 35 publications from the Scopus database. The findings underscore blockchain's capacity to remodel healthcare through decentralized structures, enhanced data security, and improved interoperability, detailing the platforms and technologies driving blockchain application development. Key challenges are highlighted, such as scalability, interoperability, privacy, and compliance. While acknowledging blockchain's potential to advance healthcare data handling, the study calls for a multi-stakeholder collaborative effort to tackle technical and regulatory hurdles[31].

Arbabi et al. (2023) present a systematic framework for classifying and analyzing blockchain-based healthcare storage systems. The framework covers four main dimensions: interactions among healthcare entities, functional components of storage systems, challenges within the healthcare domain that can be addressed through blockchain, and the benefits derived from the technology’s inherent features. By examining over 40 state-of-the-art solutions, the study identifies the scope of each and maps them to the proposed taxonomy. It also includes a comprehensive discussion on compliance with privacy regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). The analysis reveals key research gaps and outlines future directions for further investigation[32].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

Table III: Literature Review Summary on Cybersecurity and Blockchain In Healthcare

Ref. Focus Area Key Contributions Challenges Addressed Findings/Results

B. Kumar et al. (2025) Blockchain Applications in EHR & Communication Comprehensive review of blockchain for EHR, AI integration, supply chain Data privacy, communication, EHR management Shows blockchain's transformative role; identifies future research directions

Singh et al. (2024) Cybersecurity in Healthcare Examines major cybersecurity risks (data breaches, ransomware, insider threats, compliance) Insider threats, HIPAA compliance, patient safety Emphasizes proactive strategies to mitigate cyber risks

Sharma et al. (2024) Blockchain Consent Mechanism in Healthcare Develops a patient-centric consent model using blockchain Data ownership, secure interoperability Model performs satisfactorily in real healthcare scenarios

A. Kumar et al. (2024) Blockchain in IoT-based Healthcare Suggests Multichain blockchain for IoT healthcare security Centralized data risks, access control, data exchange Enhances trust, privacy, and security in IoT healthcare

Pawar et al. (2024) Federated Learning in Healthcare Detailed analysis of federated learning concepts, model aggregation, and privacy protocols Data privacy preservation, scalability, personalized training Federated learning enables secure, collaborative, and scalable medical research with potential for improved patient outcomes

Lindbergh and de Morais Barroca Filho (2024) Blockchain in Healthcare Systems Mapping Systematically maps blockchain's role in healthcare; analyzes 35 Scopus publications Scalability, interoperability, privacy, compliance Highlights blockchain's potential for decentralization, security, and interoperability, while calling for multi-stakeholder collaboration.

Arbabi et al. (2023) Blockchain-based Healthcare Storage Systems Proposes taxonomy for blockchain storage systems in healthcare Privacy regulations (HIPAA, GDPR), interoperability Maps 40+ solutions; identifies research gaps and future work

VI. CONCLUSION AND FUTURE WORK

As healthcare systems undergo rapid digital transformation, safeguarding data privacy, integrity, and availability has become paramount. This review highlights blockchain as a transformative technology capable of addressing critical cybersecurity challenges in healthcare through its decentralized, transparent, and tamper-resistant features. By enabling secure data sharing, immutable audit trails, and enhanced patient-centric control, blockchain aligns well with the growing demands for trust and accountability in health information systems. Its potential is further amplified when integrated with complementary technologies, such as artificial intelligence, federated learning, and the Internet of Medical Things (IoMT), which collectively support secure, data-driven clinical insights. Despite its promise, blockchain implementation in healthcare faces notable hurdles scalability limitations, interoperability with legacy systems, and adherence to evolving regulatory standards. Overcoming these challenges requires a multidisciplinary approach involving technology developers, healthcare stakeholders, and policymakers.

Future research should prioritize the development of lightweight and scalable blockchain architectures suited for resource-constrained environments such as healthcare IoT and edge computing. Emphasis should be placed on real-world pilot implementations to evaluate system performance, operational feasibility, and compliance with healthcare regulations like HIPAA and GDPR. Additionally, integrating advanced privacy-preserving techniques such as zero-knowledge proofs, differential privacy, and homomorphic encryption will be crucial to protect sensitive health data while still enabling secure data analytics and research.

REFERENCES

[1] S. Singamsetty, "Healthcare IOT security: examining security challenges and solutions in the Internet of Medical Things. A bibliometric perspective," JPTCP, vol. 31, no. 8, pp. 1761–1806, 2024.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 10, April 2026 Impact Factor: 8.2

[2] F. M. AbdelSalam, "Blockchain Revolutionizing Healthcare Industry: A Systematic Review of Blockchain Technology Benefits and Threats.," Perspect. Heal. Inf. Manag., vol. 20, no. 3, pp. 1–19, 2023.
[3] A. Mishra, "Ai-Powered Cyber Threat Intelligence System for Predicting and Preventing Cyber Attacks," Int. J. Adv. Eng. Manag., vol. 7, no. 2, pp. 873–892, 2025.
[4] V. Radhakrishnan, "Review Analysis of Cyber Security in Healthcare System: A Systematic Approach of Modern Development," Int. J. Innov. Res. Comput. Sci. Technol., 2023, doi: 10.55524/ijircst. 2023.11.3.7.
[5] M. C. Tayal, "Designing a Secure ETL Architecture for Integrating Multi-Source Healthcare Data," Int. J. Artif. Intell. Data Sci. Mach. Learn., vol. 4, no. 1, March, pp. 98–101, 2023, doi: https://doi.org/10.63282/3050-9262.IJAIDSML-V4I1P111.
[6] M. J. Rahim, M. I. Ibn Rahim, A. Afroz, and O. Akinola, "Cybersecurity Threats in Healthcare IT: Challenges, Risks, and Mitigation Strategies," J. Artif. Intell. Gen. Sci. ISSN3006-4023, vol. 6, no. 1, pp. 438–462, Dec. 2024, doi: 10.60087/jaigs.v6i1.268.
[7] S. Pandya, "Integrating Smart IoT and AI-Enhanced Systems for Predictive Diagnostics Disease in Healthcare," 2024.
[8] V. Prajapati, "Blockchain-Based Decentralized Identity Systems: A Survey of Security, Privacy, and Interoperability," Int. J. Innov. Sci. Res. Technol., vol. 10, no. 3, March, pp. 1011–1020, Mar. 2025, doi: 10.38124/ijisrt/25mar1062.
[9] U. Ullah Tariq et al., "Blockchain-Based Secured Data Sharing in Healthcare: A Systematic Literature Review," IEEE Access, vol. 13, pp. 45415–45435, 2025, doi: 10.1109/ACCESS.2025.3547953.
[10] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique, "Blockchain Application in Healthcare Systems: A Review," 2023. doi: 10.3390/systems11010038.
[11] S. Pandya, "Predicting Diabetes Mellitus in Healthcare : A Comparative Analysis of Machine Learning Algorithms," vol. 13, no. 6, pp. 545–553, 2023.
[12] A. AbuHalimeh and O. Ali, "Comprehensive review for healthcare data quality challenges in blockchain technology," Front. Big Data, vol. 6, May 2023, doi: 10.3389/fdata. 2023.1173620.
[13] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," Int. J. Intell. Networks, vol. 2, pp. 130–139, 2021, doi: 10.1016/j.ijin.2021.09.005.
[14] C. Tayal, "Big Data Pipeline Optimization for Electronic Health Records (EHR)," Int. J. Artif. Intell. Data Sci. Mach. Learn., vol. 5, no. 3, Oct, pp. 121–127, 2024, doi: 10.63282/3050-9262.ijaidsml-v5i3p113.
[15] U. Padmavathi and N. Rajagopalan, "A research on impact of blockchain in healthcare," Int. J. Innov. Technol. Explor. Eng., 2019, doi: 10.35940/ijitee.I1007.0789S219.
[16] R. Q. Majumder, "Designing an Intelligent Fraud Detection System for Healthcare Insurance Claims Using a Machine Learning Approach," in 2025 Global Conference in Emerging Technology (GINOTECH), IEEE, May 2025, pp. 1–6. doi: 10.1109/GINOTECH63460.2025.11076870.
[17] S. S. S. Neeli, "Critical Cybersecurity Strategies for Database Protection against Cyber Attacks," J. Artif. Intell. Mach. Learn. Data Sci., vol. 1, no. 1, p. 5, 2023.
[18] M. A. Mostafiz, "Machine Learning for Early Cancer Detection and Classification : AI- Based Medical Imaging Analysis in Healthcare," Int. J. Curr. Eng. Technol., vol. 15, no. 3, pp. 251–260, 2025, doi: https://doi.org/10.14741/ijcet/v.15.3.7.
[19] S. Radadia, K. Mahendrabhai, N. Shukla, H. Patel, and K. D. Mistry, "CYBER SECURITY DETECTING AND ALERTING DEVICE," 2024
[20] Y. He, A. Aliyu, M. Evans, and C. Luo, "Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review," J. Med. Internet Res., vol. 23, no. 4, p. e21747, Apr. 2021, doi: 10.2196/21747.
[21] G. Modalavalasa, "ADVANCED BLOCKCHAIN MECHANISMS FOR STRENGTHENING DATA SECURITY AND ENSURING PRIVACY IN DECENTRALIZED SYSTEMS," Int. J. Recent Technol. Sci. Manag., vol. 8, no. 6, pp. 89–98, 2023, [Online]. Available: https://ijrtsm.com/wp-content/uploads/2025/05/June-2023-Godavari-89-98.pdf

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

[22] B. P. Pokharel, N. Kshetri, S. R. Sharma, and S. Paudel, "blockHealthSecure: Integrating Blockchain and Cybersecurity in Post-Pandemic Healthcare Systems," Inf., vol. 16, no. 2, pp. 1–21, 2025, doi: 10.3390/info16020133.
[23] D. Patel, "Enhancing Banking Security: A Blockchain and Machine Learning- Based Fraud Prevention Model," Int. J. Curr. Eng. Technol., vol. 13, no. 06, pp. 556–583, Dec. 2023, doi: 10.14741/ijcet/v.13.6.10.
[24] D. Patel, "Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity," TIJER – Int. Res. J., vol. 10, no. 6, pp. 853–858, 2023, [Online]. Available: https://tijer.org/tijer/papers/TIJER2306333.pdf
[25] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing," Futur. Internet, vol. 14, no. 11, p. 341, Nov. 2022, doi: 10.3390/fi14110341.
[26] B. Kumar, V. Garg, K. Ahmed, P. Garg, S. Choudhary, and P. Baniya, "Enhancing Healthcare with Blockchain: Innovations in Data Privacy, Security, and Interoperability," in 2025 3rd International Conference on Disruptive Technologies (ICDT), IEEE, Mar. 2025, pp. 932–938. doi: 10.1109/ICDT63985.2025.10986335.
[27] G. Singh, D. Tiwari, P. Goel, P. Vishwakarma, K. Gupta, and A. Verma, "Cybersecurity Challenges In Healthcare Systems," in 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), IEEE, May 2024, pp. 1–6. doi: 10.1109/IC3SE62002.2024.10593022.
[28] M. Sharma, S. Singh, A. Deep, D. Garg, and A. Kumar, "Blockchain's Frontier: Enhancing Data Security and Collaboration for Healthcare," in 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), IEEE, Mar. 2024, pp. 1–6. doi: 10.1109/ICRITO61523.2024.10522385.
[29] A. Kumar, K. Guleria, I. Sharma, and A. Khan, "Multichain Blockchain Solutions for Ensuring Trust and Transparency in IoT Healthcare Environment," in 2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT), IEEE, Aug. 2024, pp. 1314–1318. doi: 10.1109/ICCPCT61902.2024.10672895.
[30] A. Pawar, S. Jain, A. Dhait, A. Nagbhidkar, and A. Narlawar, "Federated Learning for Privacy Preserving in Healthcare Data Analysis," in 2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA), IEEE, Dec. 2024, pp. 1–6. doi: 10.1109/ICAIQSA64000.2024.10882173.
[31] V. G. Lindbergh and I. De Morais Barroca Filho, "Trends in Blockchain Applied to Healthcare," in 2024 IEEE 12th International Conference on Healthcare Informatics (ICHI), IEEE, Jun. 2024, pp. 531–533. doi: 10.1109/ICHI61247.2024.00078.
[32] M. S. Arbabi, C. Lal, N. R. Veeraragavan, D. Marijan, J. F. Nygard, and R. Vitenberg, "A Survey on Blockchain for Healthcare: Challenges, Benefits, and Future Directions," IEEE Commun. Surv. Tutorials, 2023, doi: 10.1109/COMST.2022.3224644.