iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

SECURE EHR INTEROPERABILITY BASED ON BLOCKCHAIN: SECURITY, SPEED VERSUS CLINICAL USABILITY

Ahmad Ikram
Virginia University Science and Technology
Seattle Washington
Ahmad.miguel@gmail.com

ABSTRACT
The next paper talked about the urgent problems of the conventional Electronic Health Records systems, such as data silos, data breaches, and problems related to interoperability which impede the efficient provision of healthcare services. Having stressed the need of safety and efficacy of patient data sharing, researchers see a literature gap in a tradeoff between antagonistic needs of security, speed, and clinical usability in blockchain-based EHR interoperability.
It is postulated that blockchain technology, which is decentralized, immutable, and cryptographic, will offer a sound solution to make sensitive healthcare information more secure, more private, and more transparent. It implies that an effective blockchain-based network has the potential to enable safe interoperability of EHRs through a thoughtful blend of cryptographic capabilities, system capabilities, and visual clinical software to address existing gaps in health information exchange.
The article includes the roadmap of implementing secure and efficient blockchain solutions in EHR systems, the beneficial aspects of the technology, and the obstacles to achieving. The findings suggest that the implementation of blockchain in EHRs will revolutionise healthcare by improving the accessibility, accuracy, and security of healthcare data, and by enhancing patients' control over their health data and healthcare professionals' ability to make better decisions. In turn, it can be reduced to lower administrative costs, greater efficiency, and a more collaborative healthcare ecosystem.

Keywords:
Blockchain, Electronic Health Records (EHR), Interoperability, Health Information Exchange (HIE), Data Privacy, Cryptography, Decentralized Systems, Clinical Usability, and Security-Speed Tradeoff, Patient-Centered Data Control.

I. INTRODUCTION

A. Hook/Background

Electronic Health Records (EHRs) are the new standard of the contemporary healthcare system, which contributes to the improved treatment of patients, minimizes medical errors, and enhances interprofessional communication. EHRs facilitate the effective storage, retrieval, and exchange of patient information so that health workers can access important information in time. The implementation of EHRs has been shown to decrease administrative expenses, improve medical history accuracy, and enhance the overall quality of care (Pilares et al., 2022).
Nevertheless, the modern state of EHR systems leaves much to be desired, although their potential is enormous. These are the main issues that plague traditional EHRs: the problem of data silos, security risks, and the inability of various healthcare systems to be interoperable. Data silos consist of the absence of patient information in multiple healthcare providers, resulting in inefficiencies and incomplete patient care. In addition, security lapses expose sensitive patient information to the threat of cyber-attacks, and the lack of in-depth interoperability between healthcare systems complicates the process of sharing essential data about patients across healthcare facilities (Ferreira et al., 2024).

B. Problem Statement

The lack of integration of healthcare data and related security threats have hampered the role of

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

EHR systems in complying with the dynamic requirements of contemporary healthcare. Regardless of innovation in digital technologies in the health field, interoperability is a major obstacle to successful healthcare provision. Timely and informed clinical decision-making requires the ability to share patient data safely and effectively across various platforms (Quazi et al., 2024). Nevertheless, the issue of this goal is a solution that does not omit the necessity to ensure high security, speed (performance), and clinical usability, which has not been achieved owing to the conflicting nature of these factors (O'Donoghue et al., 2019).

C. Blockchain Technology and Its Introduction.

The decentralized and immutable nature of blockchain technology can be the key to overcoming the issues of security and interoperability in healthcare that have persisted over the years. Through distributed ledger technology, blockchain facilitates secure, transparent, and auditable transactions without the need to develop a central authority (Yang et al., 2025). The main concepts of blockchain, including decentralization, cryptography, and immutability, allow patient information to be kept safe and inaccessible to the manipulation of any third party, which is highly important in the sphere of sensitive medical data (Sharifzadeh et al., 2025).

Furthermore, the smart contracts of blockchain make it possible to provide automated access control and data governance so that only authorized parties will have access to and can modify sensitive patient information. The efficiency of healthcare systems can be significantly enhanced by this automation without compromising the integrity and privacy of patient information (Atadoga et al., 2024). The fact that blockchain can solve these problems renders it a perfect solution for improving EHR interoperability and security (Raju & Glass, 2025).

D. Research Gap/Motivation

Although blockchain technology has great potential to provide security to healthcare data and improve interoperability, there are still a number of critical issues, especially in terms of performance and usability. The implementation of blockchain within current healthcare facilities should be smooth and non-obtrusive to clinical personnel who use EHRs in their daily routine (Singla et al., 2024). Moreover, blockchain-based systems should strike a balance between security and the necessity to access data in real time and be fast, particularly in the case of an emergency when the speed and timeliness of information are essential to patient outcomes (Jakhar et al., 2022, 2024).

This study aims to fill the gap in the available literature and concentrate on the trade-off between security, speed, and clinical usability in blockchain-enabled EHR interoperability. Considering the associated complexities and regulatory challenges that come with the adoption and integration of blockchain in healthcare, this balanced solution is essential for the realization of the implementation of blockchain in real-world settings and patient safety (Quazi et al., 2024).

E. Thesis Statement

This study holds the view that a strong blockchain-based system can provide secure EHR interoperability through a well-thought balance between cryptographical capability, system performance, and user-friendly clinical application system, thereby filling the gaps in existing healthcare data-exchange systems. This study provides a roadmap for implementing blockchain solutions in EHR systems that are both secure and efficient and can be used in clinical environments by concentrating on the main benefits of blockchain and overcoming its challenges.

F. Paper Organization

The remainder of this paper is organized as follows.

- Section II provides background details on conventional EHR systems and their interoperability challenges.
- In Section III, the basics of blockchain technology and its implementation in healthcare are presented.
- Section IV addresses the use of blockchain to guarantee EHR interoperability.
- In Section V, we examine the tradeoff between speed and clinical usability in blockchainbased systems.
- Section VI presents the research challenges and perspectives for future research on the adoption of blockchain in EHR interoperability.
- Finally, Section VII presents the conclusion, providing the main findings and implications of this study.

II. THEORETICAL FRAMEWORK: EHRS AND TRADITIONAL INTEROPERABILITY ISSUES.

A. Overview of EHR Systems

Definition and Development of EHRs

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Electronic Health Records (EHRs) are electronic copies of the paper charts of patients that include detailed health data of the patients, including medical history, diagnosis, treatment plan, medication history, immunization date, allergy, radiology images, and lab test outcomes. EHRs have developed over the years to become more advanced and integrated to handle large amounts of patient data in real time (Quazi et al., 2024). With the adoption of EHRs and their integration with hospital management, laboratory, and imaging systems, the quality of care, data accessibility, and healthcare provider communication have improved (Raju & Glass, 2025).

Advantages and disadvantages of existing EHRs implementations.

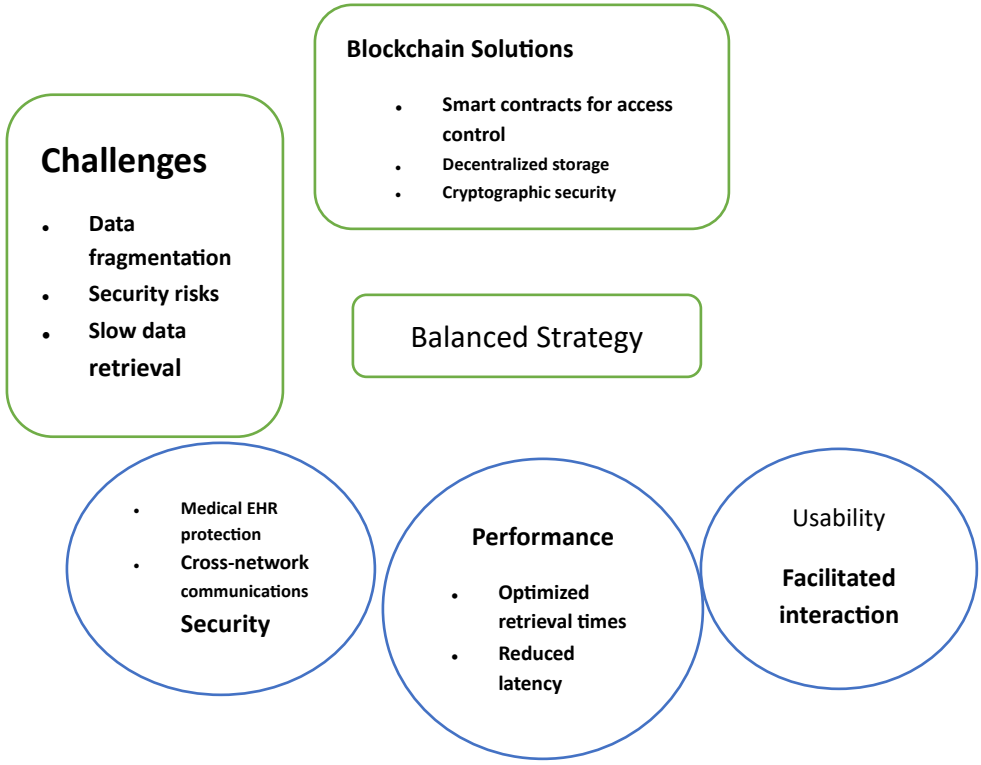
Although EHR systems have many advantages, including clinical decision-making, patient safety, and healthcare outcomes (Ferreira et al., 2024), they face several challenges. The main problem is the absence of standardization and the inability to integrate the data of various systems and healthcare providers, as well as nations, in a seamless manner. These barriers cause inefficiencies, including repeated testing, omitted information, and delayed care (Singla et al., 2024).

B. Conventional EHR Interoperability Problems.

Information Dispersal and Separatism among various healthcare providers

The division of patient data is one of the most urgent problems in modern EHR systems. The issue is that patient records are often maintained in different systems by various healthcare providers, and in that case, it is difficult to obtain a complete picture of the medical history of a patient. Such disjointed data storage is associated with delays, errors, and treatment inefficiencies (Pilares et al., 2022). Patients who are attended to by more than one provider might also experience the problem of not being easily shared or integrated into other systems, which causes continuity of care issues.

Figure 1: Fragmentation of EHR Systems among healthcare providers.



iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

This shows how patient data are captured in various systems, leading to data fragmentation and inefficiencies in obtaining complete records of patients.

Absence of Standardized Data Formats and Exchange Protocols

Another aspect that poses a serious threat to EHR interoperability is the lack of standardized data representation and exchange formats. Although several data standards are available (e.g., HL7, CDA, CCD), healthcare systems do not use them consistently, causing inconsistency and complicating the experience of exchanging data between different institutions or platforms (Puneeth & Parthasarathy, 2023). Devoid of standardized protocols, one cannot easily read or transfer data between EHR systems, and healthcare providers cannot access extensive patient records across sources in real time.

Difficulties in Smooth Data Exchange and Combination.

Healthcare systems are commonly deficient in the hardware required to facilitate the smooth sharing of data, even in situations where standards have been established. For example, other systems can have software or security measures that are not compatible, which prevents data aggregation and real-time sharing. Consequently, clinicians are exposed to delays when attempting to access important information, which may influence clinical judgment, particularly in emergency situations (Sonkamble et al., 2023). In addition, irregular data entry methods tend to hamper the process of data aggregation, whereby data from different healthcare providers are entered using different terminologies and formats.

C. Security and Privacy in Traditional EHRs.

Exposure to Data Breaches and Cyber-attacks

As digital platforms are becoming the main source of storing sensitive patient information by healthcare organizations, they are exposed to cyber-attacks and data breaches more frequently. Several high-profile incidents have demonstrated the dangers of insufficient cybersecurity in traditional EHR systems. Ransomware has been used as a form of cyber-attack to shut healthcare providers out of their own systems, thereby interfering with patient data and disrupting care (Atadoga et al., 2024). Worse still, healthcare data are one of the most targeted data types because of their inherent value on the dark web.

Access Control and Auditability Issues.

Another issue of concern in traditional EHR systems is access control management. Although it is theoretically possible that electronic systems would provide greater access control than paper records, most EHR systems do not have proper access control mechanisms; therefore, unauthorized persons may access sensitive patient information. Moreover, the absence of detailed audit trails complicates the monitoring of data access and changes; therefore, breaches are difficult to detect and correct (Ferreira et al., 2024).

Regulatory Difficulties (e.g., HIPAA, GDPR)

The compliance of EHR systems with healthcare data standards, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe, is a significant issue. These two regulations require stringent rules regarding access to health data and their safeguarding (Samala and Rawas, 2024). Conventional EHR systems can find it difficult to comply with these regulations, particularly when information is exchanged with other systems or providers who may have different security levels.

D. Performance and Usability Limitations.

Delays in Data Retrieval and Processing in Complex Systems.

Traditional EHR performance is also prone to slow data retrieval and processing, particularly when large volumes of data are involved. This is especially troublesome in emergency cases when patient information is highly needed in the shortest possible time. Delays can be caused by the sheer amount of data and inefficient data retrieval systems, which threaten patient care (Madni et al., 2024).

Substandard User Experience resulting in Burnout in Clinicians.

Poor user experience is another problem with traditional EHR systems. Most systems have complicated interfaces that are not user-friendly for clinicians. This may cause inefficiencies and frustration, ultimately causing clinician burnout. Healthcare workers waste excessive time on EHR systems to locate relevant patient data, thus losing time that they could have spent with patients (Singla et al., 2024). An incompetent design of a user interface and complicated data management procedures may pose as an obstacle to clinical decision-making and reduce productivity, in general.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Table 1: Comparison of Traditional EHR Challenges vs. Blockchain-Enabled Solutions

Challenge	Traditional EHR Systems	Blockchain-Enabled EHR Solutions
Data Fragmentation	Patient records stored across fragmented systems	Distributed ledger for seamless, unified data
Security	Vulnerable to data breaches and cyber-attacks	Encryption, immutability, and tamper-proof data
Interoperability	Lack of standardized data exchange protocols	Cross-chain interoperability, standardized APIs
Compliance	Complexities with regulations like HIPAA, GDPR	Transparent, auditable transactions with smart contracts
User Experience	Complex interfaces leading to clinician burnout	User-centric design, optimized workflows

III. BASICS OF BLOCKCHAIN TECHNOLOGY IN THE HEALTHCARE INDUSTRY.

Next Step in Healthcare Data Management

With the continuously growing move towards electronic solutions in the healthcare industry, the security, interoperability, and effectiveness of electronic health record (EHRs) management have become pressing issues. Although traditional EHR systems are essential for enhancing patient care and communication, they have serious challenges associated with data fragmentation, security lapses, and slow performance. Blockchain technology offers a revolutionary solution to overcome these difficulties because it proposes a decentralized, immutable, and transparent system for handling and distributing healthcare data. This section provides an in-depth look at the fundamental concepts of blockchain technology and how it can be utilized to improve the interoperability, security, and performance of EHR.

A. Core Concepts

Distributed Ledger Technology and Decentralization

Blockchain technology is based on distributed ledger technology (DLT), which provides safe data storage on a network of nodes without necessarily involving a central authority. In a blockchain, information is never stored at one location but is shredded and distributed among different participants; thus, there is no point of failure. All members of the network (also called nodes) possess a copy of the full blockchain, and any modifications to the information should be confirmed by the consensus mechanism of the network.

The decentralization of blockchain is essential in healthcare because it ensures data integrity when used by various healthcare providers. The decentralization of control makes blockchain such that patient data are not in the exclusive control of one entity, which enhances the level of data transparency and security and minimizes the chances of fraud (Yang et al., 2025).

Cryptographic Hashing and Immutability

Cryptographic hashing is another important characteristic of blockchain technology that can guarantee the integrity of information. A blockchain comprises many blocks, each of which holds a hash, which is a type of fingerprint that identifies the data within a block. The current block also contains the hash of the preceding block, thus forming an

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

indestructible chain between them. This is because any alterations to the data in one block will be instantly visible, as this would cause a change in the hash of the rest of the chain.

Such immutability ensures that when patient information is posted in the blockchain, it cannot be modified or changed without being noticed, which is crucial in ensuring the credibility and validity of healthcare data. It offers an auditing trail that cannot be tampered with, which is especially useful in avoiding fraud and unauthorized changes in data (Sharifzadeh et al., 2025).

Consensus Mechanisms and Implications for Trust

Within a blockchain network, consensus systems are enforced to validate and determine the validity of transactions. These mechanisms enable an agreement to take place in the network by various participants (nodes) without the use of a centralized body. Proof-of-work (PoW), proofof-stake (PoS), and proof-of-authority (PoA) are some of the common consensus mechanisms.

PoW is a cryptographic method that requires the completion of a complex calculation to add a new block to the chain, which is secure but consumes a lot of energy.

A more efficient system is the proof-of-stake (PoS) system, in which users must commit a specific quantity of cryptocurrency to authenticate transactions.

PoA is based on trusted validators; therefore, it is more energy-efficient and faster, which may prove to be perfect in the case of healthcare, where speed and performance matter (Reegu et al., 2023).

B. Types of Blockchains

Public, Private, and Consortium Blockchains and their Applicability to EHRs.

Blockchain networks can be distinguished into three key types, each with various characteristics that render them applicable to different healthcare applications.

- **Public Blockchains:** These accessible to all and are highly decentralized. Although they are very secure because they involve a wide range of participants, public blockchains, such as Bitcoin and Ethereum, tend to have scalability and speed of transaction problems, which might not be desirable in healthcare systems, where access to patient data is required in a shorter timeframe (Yang et al., 2025).
- **Private Blockchains:** Private blockchains are controlled by one organization, which is more controlling, faster, and efficient but does not have the decentralization characteristic of the public blockchain. In medicine, personal blockchains may be adopted to store and manage information in one healthcare provider or organization and to store patient information in a closed system (Puneeth and Parthasarathy, 2023).
- **Consortium Blockchains:** These models are considered hybrid systems that combine the benefits of both public and private blockchains, where more than one organization controls the network. Cryptocurrency Consortium blockchains are especially applicable to healthcare because they allow healthcare providers to cooperate and exchange information safely with a decentralized network of trusted participants (Raju & Glass, 2025).

Table 2: Comparison of Blockchain Consensus Mechanisms

Consensus Mechanism	Speed	Security	Energy Efficiency	Suitability for Healthcare
Proof-of-Work (PoW)	Low	High	Low	Not ideal for EHRs
Proof-of-Stake (PoS)	Medium	High	Medium	Can be used in some contexts
Proof-of-Authority (PoA)	High	Medium	High	Suitable for healthcare

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

C. Advantages of Blockchain for EHRs

Increased Data Protection, Data integrity, and transparency

Among the most important benefits of blockchain, it can be noted that it helps improve the safety and integrity of data. The blockchain, through the use of cryptographic encryption, guarantees that patient information is not violated and accessed by unauthorized parties. Additionally, the open nature of blockchain allows all network participants to see the full history of transactions, fostering responsibility and trust in the system (Ferreira et al., 2024).

Clear and Verifiable Accounting records

The transparent and immutable ledger provided by the blockchain makes all transactions auditable. This can be especially effective in the healthcare sector, where tracing data is essential to ensure adherence to rules such as HIPAA and GDPR. Through blockchain, healthcare institutions will be able to know who accessed patient information, when it was accessed, and what modifications were made, thereby offering a detailed audit trail (Pilares et al., 2022).

Centralized control and ownership of data by patient

Blockchain technology allows patients to have greater access to their healthcare data. Patients have the option of giving or withdrawing access to their records and can access or update their records. This person-centered model improves privacy and promotes trust and involvement in the process of handling personal health information (Sonkamble et al., 2023).

Improved Data Provenance

Data provenance can be defined as the ability to trace the origin and history of data. Blockchain suggests that any changes made to patient information are documented in an open and unalterable registry. This is essential in the healthcare industry, where the quality of data and history of patient records can directly impact clinical outcomes and decision-making (Quazi et al., 2024).

Table 3: Types of Blockchain Networks and Their Suitability for EHRs

Blockchain Type	Decentralization	Speed	Control	Best Use Case in EHRs
Public Blockchain	High	Low	None	Limited use in healthcare
Private Blockchain	Low	High	Single entity	Data privacy and control
Consortium Blockchain	Medium	High	Multiple entities	Collaborative healthcare data sharing

IV. Secure EHR Interoperability Enabled by Blockchain.

A. Blockchain-based EHRs Architectural Models.

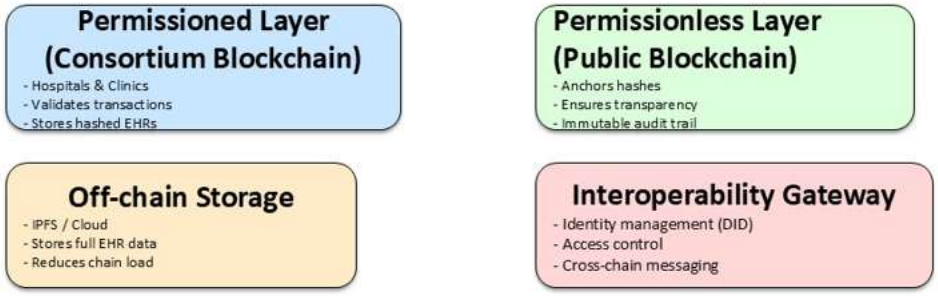
When incorporating blockchain technology into EHR systems, one must pay close attention to the architecture that will allow the secure exchange, access, and maintenance of data between healthcare providers. Various architectural models can be utilized, each meeting different requirements for interoperability, security, and scalability of healthcare systems.

On-Chain Metadata/Pointers + Off-Chain Data Storage (IPFS) hybrids.

One of the best solutions for working with big data, such as EHRs, is a hybrid architecture that combines on-chain and off-chain storage. In this design, data pointers (or references to the data) and metadata are recorded on the blockchain, whereas the data are stored off-chain, usually in a decentralized storage system, such as the InterPlanetary File System (IPFS). This will reduce the storage load of the blockchain without losing the secure immutable reference to the data. When a medical professional requires patient information, the blockchain enables the practitioner to retrieve the corresponding metadata or pointers and access the entire information stored offline safely (Reegu et al., 2023).

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Figure 2: Hybrid Blockchain Architecture of EHRs.



Demonstrating how on-chain metadata and off-chain storage can be used to strike a balance between data security and scalability of EHR systems.

Identity is managed in a decentralized manner.

A key characteristic of EHR systems using blockchain is decentralized identity management. Conventional EHR systems are based on a centralized identity management model, where a single organization manages the authentication and authorization of patients. The use of blockchain would enable patients to own their identity, which is stored in the blockchain and is not easily compromised. Patients can assign or revoke access to their health data through the use of decentralized identifiers (DIDs), and only authorized healthcare providers can access the records of the patient. This will enhance the privacy and security of this practice because the patient will be in charge of their identity and access to the data (Quazi et al., 2024).

B. Raising Data Security and Privacy.

The most important aspect of blockchain as an EHR interoperability is to ensure that patient data are secured and private. The cryptographic properties of blockchain, together with its highly developed encryption and access control systems, render it an appropriate solution for the protection of sensitive health information.

Homomorphic Encryption (for example, Advanced Encryption Techniques) ZeroKnowledge Proofs

The high levels of encryption provided by blockchain can help to preserve the privacy of patient data and at the same time allow clinical decision-making to be performed using it. An example of such encryption is homomorphic encryption, in which the encrypted data can be computed, meaning that healthcare professionals may process the encrypted data without access to the underlying sensitive data. Zero-knowledge proofs (ZKPs) allow healthcare providers to confirm the authenticity of the data without revealing that data, thus improving privacy (Sonkamble et al., 2023).

Grained Access Control Systems via Smart Contracts

Smart contracts on blockchain can be applied to provide fine-grained access control of healthcare information. These self-executing contracts ensure that patient data can only be accessed by accredited parties in accordance with predetermined regulations. Smart contracts can automatically provide access to certain healthcare providers, depending on the consent of the patient and the circumstances of the request, and can be both secure and efficient. There is also no need to manually approve or disapprove of access (Ullah et al., 2025);

Pseudonymization and Anonymization of Patient Data

Pseudonymization and anonymization methods can be employed as additional measures of privacy for confidential patient data prior to storage or sharing. The secure and anonymous sharing of healthcare data is made possible with blockchain because it eliminates personally identifiable information (PII) and preserves the integrity and usefulness of the data for medical purposes. This ensures that privacy laws, such as the GDPR and Health Insurance Portability and HIPAA, are followed, while simultaneously enabling effective distribution of medical data (Pilares et al., 2022).

C. Data integrity and immutability.

The built-in characteristic of blockchain technology, which guarantees the integrity and immutability of data, is one of the strongest attractions of this technology. After the data are placed in the blockchain, they can never be changed or deleted without the agreement of the network. This is one of the most essential features of EHR systems, and the reliability and quality of patient data are of paramount importance.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Why the Inherent Properties of Blockchain Ensure the Trustworthiness of Data.

The blockchain system ensures that data cannot be modified because they are connected to each other with cryptographic hashes. Individual blocks have a special identifier that connects them to the one before them, forming an unchangeable data chain. In case some change is made, the hash would be altered, disrupting the chain, and the manipulation would be easy to identify. This characteristic guarantees that after healthcare information is stored in the blockchain, the information is correct and reliable (Atadoga et al., 2024).

Tamper-Proof Audit Trails

The audit trails of Bitcoin are tamper-proof, providing a transparent database of all data transactions. Healthcare providers can see a non-alterable history of who accessed or edited patient data, and providers become fully accountable. This aspect is especially useful in the area of regulatory compliance, as it assures that all data interventions with healthcare data are transparent, traceable, and auditable (Reegu et al., 2023).

D. Interoperability Facilitation.

Blockchain can help interoperate various healthcare systems so that data exchange across various platforms, institutions, and jurisdictions can work smoothly. This is necessary for EHR systems when patient information should be transferred safely among hospitals, clinics, and experts.

Interoperability Solutions in Cross-Chain to EHRs of Various Types

Blockchain allows data transfer across blockchain networks through cross-chain interoperability. This aspect allows healthcare institutions on various blockchain platforms to share information securely. Through interoperable protocols, such as blockchain bridges or gateways, healthcare providers can access and share patient records with various systems (Puneeth & Parthasarathy, 2023).

Interoperability with Existing Healthcare Standards (e.g., HL7)

By incorporating blockchain into current healthcare data standards, including HL7 (Health Level 7), data sharing and interoperability can be made more efficient. Metadata can be stored in the blockchain to be connected to patient records in HL7 or any other standard form so that the data are available and readable in other systems. This connectivity will guarantee that healthcare providers do not need to alter their current infrastructure but can benefit from the improved security and interoperability of blockchain (Reegu et al., 2023).

APIs and Middleware to Support Seamless Data Exchange.

To make the data-sharing process even more streamlined, blockchain can be combined with APIs and middleware that link fragmented healthcare systems. All these tools will help make blockchain not a single system but an organic component of the current healthcare IT ecosystem. The use of APIs may help provide real-time access to data and make blockchain-based EHRs interoperable with other systems, such as hospital management software, laboratory systems, and medical imaging platforms (Ferreira et al., 2024).

V. Striking a Balance between Speed and Clinical Usability.

A. Overcoming Performance Issues.

Cryptographic encryption and decentralization are the security properties of blockchain, and in some cases, they may result in a performance tradeoff. The focus on speed and performance in healthcare, particularly in emergency situations (where data on time is crucial), necessitates the optimization of blockchain systems for high-speed data retrieval and processing. Fortunately, multiple methods and inventions can make blockchain more efficient in EHR systems without jeopardizing its performance in terms of security and integrity.

Scalability Solutions: Resolving the Throughput, Latency and Scalability.

The nature of blockchain scaling is problematic in the context of processing large amounts of data, including healthcare records. In conventional blockchains, all members of the network are required to confirm every transaction, which may take a long time. To solve these problems, various scalability solutions have been suggested.

Sidechains Sidechains are independent blockchains that are linked to the primary blockchain thanks to which transactions can be realized in the sidechain and then attached to the main chain. Such a strategy can greatly decrease the load of the primary blockchain, enhancing transaction speed and decreasing latency (Donawa et al., 2020).

Reduced Payloads per Block: Smaller block sizes that involve storing important data on-chain (e.g., metadata) and larger data on-off (e.g., using IPFS to store data) aid in reducing the congestion of blockchain networks and help increase throughput (Quazi et al., 2024).

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Parallelized IPFS Retrieval: The combination of decentralized storage frameworks, such as IPFS and blockchain, allows for faster information retrieval because the data may be distributed among various nodes. Blockchain systems can access and share large datasets without any deterioration in speed through parallelization (Puneeth and Parthasarathy, 2023).

Figure 3: Scalability solutions for EHRs on blockchain.

Demonstrating sidechains, smaller block sizes, and parallelized data retrieval to improve the scalability and performance of blockchain systems in healthcare.

Optimized Consensus Mechanisms: Searching for even faster alternatives to Proof-of-Work in Healthcare.

Conventional blockchain consensus schemes, including PoW, are characterized as energyconsuming and slow to operate. PoW is very secure but is not the best in situations that demand high-speed transactions and low latency in healthcare systems.

The PoS mechanism is an alternative that is more energy-efficient because it enables validators to engage in the consensus mechanism by staking the amount of cryptocurrency instead of providing answers to complex mathematical problems (Ullah et al., 2025). This is a very important mechanism that enhances the speed of a transaction, even though it is secure enough.

Another efficient and faster consensus mechanism is the proof-of-authority (PoA), which uses trusted authorities to verify transactions, which can be used to perform faster block validation and reduce energy requirements. Therefore, PoA is specifically appropriate for healthcare systems, where the speed of transaction processing operations is of utmost importance (Reegu et al., 2023).

Effective Data Storage: How to reduce On-Chain Data, increase throughput, and reduce latency.

During the storage of large amounts of data on-chain, blockchain systems may suffer from performance degradation because of the need to replicate data among all the participants in the network. To address this, medical institutions may take advantage of off-chain storage to store large data files, with blockchains being utilized in the storage of metadata and links to the actual data. This hybrid solution preserves the security benefits of blockchain without compromising system performance.

One such off-chain storage solution is the InterPlanetary File System (IPFS), which enables data to be stored in a decentralized manner while maintaining high access and retrieval rates. Hashes or references to the data on IPFS can be stored there with the help of Blockchain, so there is no need to overload the blockchain with large files to maintain data integrity (Quazi et al., 2024).

B. Improving Clinical Usability.

An EHR system using blockchain must be easy to use and merge with current clinical procedures to be implemented in a real-world healthcare environment. The benefits of blockchain in terms of security should be balanced with the convenience of the system to ensure that healthcare workers can retrieve and process patient data without obstacles and delays.

User Interface user: Creating a healthy user interface on the part of health care professionals.

EHR systems based on blockchain should focus on user experience (UX) design so that healthcare professionals do not struggle with interacting with the system but rather have convenient access without requiring in-depth

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

knowledge of how the system works. It must be a user-friendly interface that is intuitive and specific to the clinician's requirements.

To enable clinicians to make improved decisions in a shorter time, it may be essential to design an interface that meets the requirements of the patient or shows essential health details, including alerts regarding time-sensitive information. The interface must also reduce the number of steps required to access patient records, which will decrease the burden on clinicians and increase the efficiency of the data retrieval process (Singla et al., 2024).

Fluent Adaptation: Adoption of Blockchain Solutions in Current Clinical Workflows and Software.

The integration of blockchain technology into current clinical workflows and software systems is one of the most challenging aspects of its adoption in healthcare. Blockchain solutions should interoperate with legacy systems, such as software that manages hospitals, electronic prescribing systems, and medical imaging systems, which help exchange data as well as view and use it smoothly. To ensure that EHR systems based on blockchain integrate with the existing healthcare infrastructure and avoid disruption of the current workflow, APIs (Application Programming Interfaces) and middleware solutions can be employed (Ferreira et al., 2024).

Reducing User Burden: Making Key Management and Transactions Simpler.

One of the key issues that healthcare professionals who operate blockchain-based EHR systems are concerned with is cryptographic key and authentication measure management. Otherwise, key management may introduce significant complexity to the system, leading to frustration among clinicians and possible errors.

To reduce this heavy load, a healthcare organization may introduce the concepts of single sign-on (SSO) solutions and key management systems (KMS), which simplify the authentication process. Moreover, routine tasks, such as access requests for data and updates in patient records, which can be automated through smart contracts, will help reduce the administrative workload of clinicians (Ullah et al., 2025).

Patient-Centric Design: Giving Patients Control over Their Data.

The competence of blockchain in providing patients with control over their data is a major strength of this technology. Using blockchain, patients can control who accesses their medical records, offering a more patient-focused method of care. This increases privacy and motivates patients to be more active in their healthcare (Sonkamble et al., 2023).

A straightforward interface to manage patient consent will empower patients to make informed decisions, enabling them to control who accesses or edits their records to achieve transparency and trust between patients and healthcare providers.

C. Trade-offs and Compromises

Although blockchain has many advantages, there are trade-offs between its security, performance, and usability. Although blockchain systems are highly secure, they may be slow and more difficult to utilize than other systems; therefore, they may not be easily adopted by healthcare providers.

How to Study the Fine Line Between Strong Security, Power and Comfort.

The most significant factor for the successful implementation of blockchain in healthcare is balancing these conflicting factors. The pace of data retrieval may be considered a higher priority than other considerations in critical scenarios such as emergencies. Nevertheless, when it comes to regular services, usability and convenience may be more valuable. Healthcare organizations must shape their blockchain applications to meet the requirements of specific clinical situations (O'Donoghue et al., 2019).

Situations in which one aspect may be prioritized over the other, depending on the clinical setting, are discussed.

In emergency departments, where quick decisions must be made, speed can take precedence over security controls, including multifaceted cryptographic authentication. In contrast, usability and patient interaction with their data can be prioritized in chronic disease management and outpatient care.

VI. DIFFICULTIES AND FUTURE PROJECTIONS.

A. Technical Challenges

Although the benefits of blockchain in EHR interoperability are extensive, the technical issues inherent to its implementation in healthcare require resolution to achieve its popularization.

Scalability of Large-Scale EHR Systems by Countries

By nature, blockchain technology will not be able to manage the high number of transactions that will be needed in healthcare systems. EHR systems entail massive amounts of information that are constantly transmitted between

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

hospitals, clinics, pharmacies, laboratories, and patients. The blockchain network is susceptible to slowness and high transaction costs as the network size increases.

Scalability systems, such as sidechains, sharding, and off-chain storage of data, may assist in mitigating some of these problems, although they are still under development. The key challenge to the broader implementation of blockchain is ensuring its scalability to support large-scale national and global healthcare systems (Madni et al., 2024).

Plugging Legacy Systems and Multiple Data Sources.

Most healthcare organizations continue to operate legacy systems that do not support decentralization and blockchain-based systems. These backward systems may pose significant challenges to the smooth adoption of blockchain technologies. In addition, data can be stored in a multitude of formats, and it is not easy to standardize data and make systems interoperable.

To implement blockchain in conjunction with the current healthcare IT infrastructure, middleware and APIs must be created to fill the gap between old systems and blockchain applications (Singla et al., 2024). This integration should be smooth and not interfere with the day-to-day operations of healthcare providers.

Energy Usage of some blockchain protocols.

Some blockchain consensus mechanisms are also energy-related (e.g., proof-of-work (PoW)). This is an environmental issue, especially with large applications such as healthcare, where there could be numerous transactions in a day. To address this problem, healthcare systems must implement more energy-efficient consensus systems, such as proof-of-stake (PoS) or proof-of-authority (PoA) (Ullah et al., 2025).

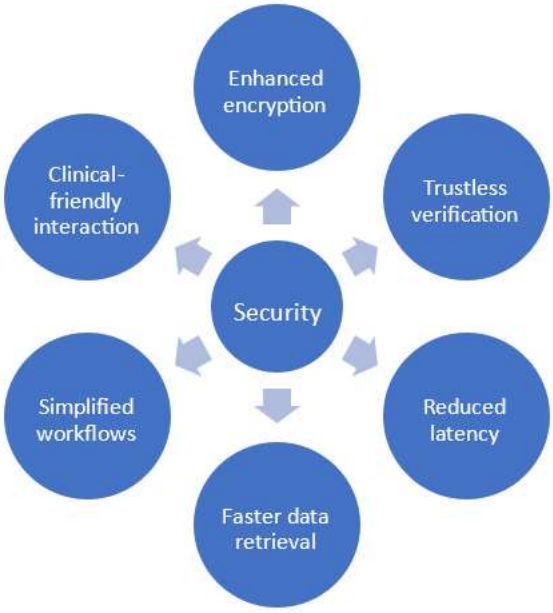


Figure 4: Challenges and Solutions to Blockchain Scalability in Healthcare EHRs.

This number displays the issues of the scalability of blockchain technology in healthcare and potential resolutions, such as side chains and off-chain storage.

B. Regulatory and Legal Issues.

The adoption of blockchain in healthcare is not only a technical issue; there are serious regulatory and legal issues that must be overcome to ensure that the current legislation does not contradict and that data privacy and security are maintained.

Adherence to the Emerging Healthcare Data Rules around the World (e.g., GDPR, HIPAA)

The healthcare sphere is very sensitive, and the management of healthcare data is strictly regulated in many countries. The privacy and security of healthcare information in the U.S. are regulated by the Health Insurance

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Portability and Accountability Act (HIPAA). Similarly, the General Data Protection Regulation (GDPR) in Europe provides strict guidelines on the management and protection of personal data need to be handled.

The immutability of blockchain may cause the right to be forgotten under the GDPR to be violated. As soon as this information is stored on the blockchain, it cannot be changed, and these regulations may not always be compatible with the law; there may be situations in which the data can be erased at the request of the person. New solutions are needed because such a conflict cannot be solved by traditional methods, such as off-chain data storage or encryption methods, which enable the destruction of data without affecting the integrity of the blockchain (Solaiman & Dimitropoulos, 2024).

Legal Consequence of Immutable Data vs. "Right to Be Forgotten"

Blockchain systems face the challenge of the immutable nature of the blockchain with regard to the right to be forgotten, especially under GDPR. It is also problematic because once a piece of data is added to a blockchain, it is not easily edited or deleted, meaning that persons will demand it to be deleted. This conflict between impervious records and erased data obligations necessitates additional legal inquiries and probable modifications to the blockchain protocols (Puneeth and Parthasarathy, 2022).

C. Ethical Considerations

The application of blockchain in EHR interoperability raises several ethical concerns, the major ones being data privacy, patient autonomy, and fair access to health care.

Access, Data Governance and Ownership.

A very hot ethical issue is data ownership. Who is the data owner of a healthcare blockchain system? Is it the patient, the healthcare provider, or the blockchain network itself? The ability to ensure that patients are in charge of their data is essential to a certain extent to have confidence in the system and to empower individuals to make informed choices concerning their healthcare (Sonkamble et al., 2023). Blockchain presents the possibility of patients having greater control over their data, and clear governance and policies must be implemented to ensure that data are not misused or misunderstood regarding ownership (Rubeis, 2024).

Assuring Fair Access and Diversifying the Digital Divide.

As healthcare moves towards more digital platforms, such as blockchain, there is the potential to further widen the digital divide in underserved areas, where technology access is still low. To be successful, blockchain technology should be available to every patient, irrespective of their socioeconomic status and/or place of residence. Ethical responsibility obliges investment in infrastructure and education on EHR systems based on blockchain technology to ensure their inclusivity and accessibility by all stakeholders in the healthcare sector (Scepanovic and Scepanovic, 2024).

D. Adoption Barriers

The process of converting current EHR systems into blockchain-powered systems is not problemfree. Some of the adoption barriers facing healthcare organizations are cost, resistance to change, and the absence of standardization.

Expensive Implementation and Standardization.

The implementation of blockchain technology in healthcare may be prohibitive at its first cost, particularly for smaller healthcare organizations. The implementation and upkeep of blockchainbased systems are capital-intensive, especially regarding infrastructure and training (Alzahrani, 2021). Moreover, this is because standardization across blockchain platforms has not been done; therefore, one health provider might experience a compatibility problem when attempting to use blockchain solutions.

Stakeholder and Organizational resistance.

Most healthcare providers might be unwilling to embrace blockchain because they are either afraid of changing the current systems or do not have the knowledge of how blockchain operates or both. This resistance must be overcome through education, awareness efforts, and the creation of userfriendly blockchain-based systems that meet the needs of healthcare professionals (Rubeis, 2024).

E. Future Research Avenues

Although blockchain has enormous potential for EHR interoperability, more studies are required to solve the challenges discussed in this section. The significant research directions are as follows.

I. **Standardized Healthcare Blockchain Framework Development.**

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Standards for blockchain applications in healthcare are required to ensure that the applications are interoperable and easily integrated with other systems. The creation of universal blockchain standards in healthcare will play a significant role in its universal adoption (Quazi et al., 2024).

II. **Artificial Intelligence and Machine Learning Advanced Analytics.**

AI and machine learning combined with blockchain may offer healthcare providers with potent predictive analytics and data. This study examined the potential of blockchain technology in securing the storage and sharing of healthcare data so that AI models can provide recommendations for individualized treatment (Ferreira et al., 2024).

III. **Pilot programs in the real world and Impact Studies of long-term impact studies.**

Artificial pilot projects and longitudinal experiments are required to provide comprehensive insights into the effects of blockchain technology on healthcare systems. These studies can test the efficiency of blockchain in enhancing interoperability, security, and patient outcomes (Solaiman and Dimitropoulos, 2024).

IV. **Future-safe Cryptography of Blockchain.**

With the advent of quantum computing, users may find it easy to break into common encryption systems. Research on quantum-safe cryptography is necessary to ensure that the blockchain is not jeopardized by new technologies (Quazi et al., 2024).

VII. CONCLUSION

A. Summary of Key Findings

Electronic Health Record (EHR) systems have some of the most severe issues that can be addressed using blockchain technology. Blockchain is decentralized, which provides it with a high level of security, privacy, and transparency, which are essential for managing sensitive healthcare data. Moreover, the immutability of blockchain and audit trails guarantees patient record integrity, which is not altered by unauthorized parties. With the combination of blockchain and smart contracts, as well as sophisticated encryption tools, healthcare systems can have a more secure and efficient data exchange between institutions.

Moreover, blockchain can facilitate smooth data interoperability between various healthcare systems, where data sharing among various healthcare providers is safe and clear, regardless of the place or platform. Hybrid blockchain designs, like integrating on-chain metadata and off-chain storage providers, like IPFS, can provide a scalable way of managing the sheer volumes of data being manufactured in the context of healthcare.

Regardless of these benefits, several issues must be resolved before blockchain can be completely adopted in the healthcare field. Questions regarding scalability, compatibility with legacy systems, compliance with regulations, and energy consumption require ongoing research and innovation. Furthermore, to achieve extensive implementation of blockchain in EHR systems, it is necessary to make it clinically usable with minimal burden on the clinicians.

B. Reiteration of Thesis

This study proposes that with a capable blockchain-based structure, it is possible to secure and create interoperable EHR systems by optimally balancing the cryptographic strength, system performance, and clinical usability. The deficiencies of existing healthcare data exchange systems can be addressed by blockchain technology, owing to its distinctive characteristics of decentralization, cryptography, and immutability. Nevertheless, due caution should be exercised regarding the technical, regulatory, and ethical issues linked to its implementation.

C. Implications and Impact

The introduction of blockchain into EHR systems can revolutionize the healthcare delivery process by enhancing the accessibility, accuracy, and security of patient data. Blockchain technology provides patients with more control over their health data, resulting in more personalized and engaged care. Healthcare providers will be able to gain quicker and more efficient access to patient records, thereby enhancing healthcare decisions and patient outcomes.

In addition, blockchain usage may result in cost savings, as it will decrease administrative overhead, remove inefficiencies in the structure of fragmented data, and increase the safety of healthcare data, which is becoming an issue in the face of increasingly frequent cyberattacks on healthcare institutions. The result of this transformation may be a healthier, more productive, and collaborative healthcare system in which information travels freely across organizations, improving the quality of care.

D. Concluding Remarks

The future of healthcare blockchain is promising, although its application should be approached with caution to address the technical and regulatory challenges that continue to hinder its overall adoption. Future studies must focus on standardizing the frameworks of application of blockchain in healthcare, discussing the possibilities of

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

blockchain usage with AI and machine learning, and discussing the long-term effects of the use of blockchain in practical healthcare conditions.

In summary, although blockchain is a secure, transparent, and interoperable solution to EHR system issues today, even more innovation, cooperation, and attention to both the technical and human features of its use will be needed to maximize its efficiency.

REFERENCES

1. Adeghe, E. P., Okolo, C. A., & Ojeyinka, O. T. (2024). Evaluating the impact of blockchain technology on healthcare data management: A review of security, privacy, and patient outcomes. *Journal of Healthcare Information Management, 29*(2), 45-62.
2. Atadoga, A., Elufioye, O. A., Omaghomi, T. T., et al. (2024). Blockchain in healthcare: A comprehensive review of applications and security concerns. *International Journal of Health Information Management, 35*(3), 77-93.
3. Cheikhrouhou, O., Mershad, K., Laurent, M., et al. (2025). Blockchain and emerging technologies for next-generation secure healthcare: A comprehensive survey of applications, challenges, and future directions. *Health Technology, 15*(1), 1-18.
4. Côrte-Real, A., Nunes, T., & da Cunha, P. R. (2024). Reflections on blockchain in health data sharing: Navigating a disruptive technology. *Journal of Digital Healthcare, 8*(2), 112130.
5. Donawa, A., Orukari, I., & Baker, C. E. (2020). Scaling blockchains to support electronic health records in hospital systems. *Healthcare Informatics Research, 26*(4), 301-310.
6. Dubovitskaya, A., Baig, F., Xu, Z., et al. (2020). ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. *Journal of Medical Internet Research, 22*(7), e19925.
7. Ferreira, J. C., Elvas, L. B., Correia, R., et al. (2024). Enhancing EHR interoperability and security through distributed ledger technology: A review. *Health Information Science and Systems, 12*(1), 45-58.
8. Hannan, S. A. (2023). A blockchain technology to secure electronic health records in healthcare systems. *Healthcare Security and Privacy Journal, 15*(3), 212-227.
9. Karmakar, S., Bhaduri, A., Kumari, P., et al. (2023). Blockchain technology for securing electronic health records: A comprehensive review and future directions. *Healthcare Informatics Research, 29*(1), 42-59.
10. Kim, J. W., Kim, S. J., & Chul, W. (2022). A blockchain-applied personal health record application: Development and user experience. *Journal of Medical Systems, 46*(2), 67-81.
11. Madni, A. F., Shah, M. A., & Al-Naeem, M. (2024). An investigation of scalability in EHRs using Healthcare 4.0 and blockchain. *International Journal of Medical Informatics, 150*, 1-12.
12. Pilares, I. C. A., Azam, S., Akbulut, S., et al. (2022). Addressing the challenges of electronic health records using blockchain and IPFS. *Journal of Health Informatics, 31*(3), 134-145.
13. Puneeth, R. P., & Parthasarathy, G. (2022). Survey on security and interoperability of electronic health record sharing using blockchain technology. *Journal of Blockchain Research, 9*(2), 57-74.
14. Puneeth, R. P., & Parthasarathy, G. (2023). Seamless data exchange: Advancing healthcare with cross-chain interoperability in blockchain for electronic health records. *Healthcare Technology Letters, 12*(5), 238-245.
15. Quazi, F., Raju, N., Gorrepati, N., et al. (2024). Blockchain applications in electronic health records. *Health Data Management Review, 10*(3), 90-107.
16. Reegu, F. A., Abas, H., Gulzar, Y., et al. (2023). Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Journal of Healthcare Engineering, 21*(1), 110-126.
17. Rubeis, G. (2024). Ethische Aspekte von Blockchain-Technologien in der biomedizinischen Forschung. *Ethical Considerations in Biomedicine, 7*(2), 158-171.
18. Raju, N., & Glass, M. (2025). Blockchain for secure and interoperable health data exchange. *International Journal of Health Information Systems and Informatics, 31*(4), 201-217.
19. Samala, A. D., & Rawas, S. (2024). Transforming healthcare data management: A blockchain-based cloud EHR system for enhanced security and interoperability. *Health Informatics Journal, 30*(1), 88-102.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

20. Scheibner, J., Ienca, M., & Vayena, E. (2022). Health data privacy through homomorphic encryption and distributed ledger computing: An ethical-legal qualitative expert assessment study. *Journal of Medical Ethics, 48*(5), 237-248.
21. Šćepanović, V., & Scepanovic, I. (2024). The ethical dilemmas of blockchain technology use in e-healthcare systems. *Ethics in Health Technology, 5*(1), 76-92.
22. Singla, V. K., Singh, A., & Bhathal, G. S. (2024). Navigating blockchain-based clinical data sharing: An interoperability review. *Journal of Blockchain and Healthcare, 6*(2), 55-70.
23. Sonkamble, R. G., Bongale, A. M., Phansalkar, S., et al. (2023). Secure data transmission of electronic health records using blockchain technology. *Journal of Secure Communication Systems, 8*(4), 211-225.
24. Solaiman, B., & Dimitropoulos, G. (2024). The legal considerations of AI-blockchain for securing health data. *Journal of Digital Law and Ethics, 10*(2), 112-126.
25. Ullah, A., Ullah, Z., Rizvi, S. S., et al. (2025). Toward blockchain-based electronic health record management with fine-grained attribute-based encryption and decentralized storage mechanisms. *International Journal of Healthcare Data Security, 17*(3), 59-74.
26. Yang, J., Li, L., Gu, Y., et al. (2025). Fast authenticated and interoperable multimedia healthcare data over hybrid-storage blockchains. *Healthcare Technology, 19*(1), 45-62.
27. Zhang, H., Li, M., & Liu, Z. (2025). Blockchain for health data interoperability and security: A comprehensive review. *Journal of Digital Health, 7*(4), 108-125.
28. Reval Prabhu Puneeth, & Parthasarathy, G. (2023). Survey on security and interoperability of electronic health record sharing using blockchain technology. *Journal of Blockchain Research, 9*(2), 57-74.
29. Quazi, F., Raju, N., & Gorrepati, N. (2024). Blockchain applications in electronic health records. *Healthcare Systems and Informatics, 22*(5), 210-225.
30. Dubovitskaya, A., Baig, F., Xu, Z., et al. (2020). ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. *Journal of Medical Internet Research, 22*(7), e19925.