Journal of Electrical, Computer and Informatics

E-ISSN: 3090-2444
P-ISSN: 3090-2452

*Research Article*

# Blockchain Implementation to Enhance Medical Data Security in Electronic Health Record Systems

**Gunawan Prayitno[1]*, Syahferi Anwar[2], Syeda Azwa Asif [3]**

[1] Sekolah Tinggi Manajemen Informatika dan Komputer Pesat Nabire, indonesia; e-mail: binaanakpapua@gmail.com
[2] Universitas Haji Sumatera Utara, Indonesia; e-mail: syahferia@gmail.com
[3] NED University of Engineering & Technology, Pakistan; e-mail: syedaazwa@gmail.com
* Corresponding Author: binaanakpapua@gmail.com

**Abstract.** Blockchain technology has emerged as a revolutionary solution for enhancing the security, transparency, and efficiency of Electronic Health Record (EHR) systems. Traditional database-driven EHRs face persistent challenges such as data breaches, unauthorized access, and limited auditability. This study explores the implementation of a private blockchain framework integrated with smart contracts to ensure the confidentiality, integrity, and availability of medical data. Through a comparative analysis between conventional and blockchain-based EHR systems, the research demonstrates that blockchain provides superior data protection by leveraging cryptographic hashing, decentralized validation, and immutable ledgers. Smart contracts further improve automation by securely managing access control, consent authorization, and inter-institutional data sharing without intermediary involvement. The results indicate that while blockchain-based EHRs slightly reduce throughput and increase latency due to distributed consensus mechanisms, they significantly enhance auditability and traceability, achieving up to 98.7% improvement over traditional systems. This ensures that patient data remains tamper-proof and verifiable across multiple healthcare entities. The findings confirm blockchain's potential as a secure and scalable foundation for next-generation health information systems. The study concludes that adopting private or hybrid blockchain models, supported by smart contract automation and regulatory alignment, can transform healthcare data management, promote interoperability, and strengthen patient trust in digital health infrastructures.

**Keywords:** Blockchain; Data Security; Electronic Health Record; Smart Contracts; Transparency.

**Received: May 30, 2025**
**Revised: June 15, 2025**
**Accepted: July 29, 2025**
**Online Available: July 31, 2025**
**Curr. Ver.: July 31, 2025**

## 1. Introduction

Medical data plays a critical role in modern healthcare systems. It forms the foundation for accurate diagnosis, effective treatment, research, and overall patient care management. By providing a comprehensive understanding of a patient's medical history and current health status, medical data assists healthcare professionals in making informed decisions that improve patient outcomes [1], [2]. Furthermore, medical data facilitates medical research by enabling the discovery of patterns and correlations that can lead to innovative therapies and interventions [2].

Despite its importance, medical data is highly vulnerable to manipulation, theft, and privacy breaches. Conventional Electronic Health Record (EHR) systems often face attacks from both external and internal sources, where data can be altered or stolen for financial gain [3]. Breaches in medical data can result in medical identity theft, fraud, and severe violations of patient privacy [4], [5]. Additionally, inadequately protected data may be accessed by unauthorized individuals, leading to misuse of sensitive personal information [6].

Traditional EHR systems encounter several significant security challenges. Unauthorized access is a major concern, as EHR systems are susceptible to attacks by external hackers as well as malicious insiders [3], [7]. Data manipulation within these systems can produce false records or conceal medical errors, potentially endangering patients [8]. Privacy breaches often occur due to insufficient encryption and weak access control mechanisms [9], [10]. Moreover, EHR systems are frequent targets of cyberattacks, including Distributed

Denial of Service (DDoS) attacks, trojans, and Sybil attacks, which can disrupt healthcare services and compromise data integrity [11], [12].

To address these security challenges, various solutions have been proposed, among which blockchain technology has gained significant attention. Blockchain offers a decentralized structure that reduces the risk of single points of failure and provides transparent and immutable transaction records [3], [7], [13]. This technology also empowers patients with greater control over their medical data, enhancing both transparency and trust [14]. Several studies have highlighted the potential of blockchain to secure EHR systems from tampering, insider attacks, and unauthorized access, making it a promising approach for improving healthcare data security [7], [13].

## 2. Literature Review

### Functions and Components of the Electronic Health Record (EHR) System

The Electronic Health Record (EHR) is a digital system designed to manage patient health information comprehensively. One of its main functions is administrative and patient data management, which helps reduce errors in the acquisition and processing of medical data [15], [16]. In addition, the EHR supports evidence-based clinical decision-making, assisting healthcare providers in delivering more accurate diagnoses and treatments [16], [17].

Another function of the EHR is to enhance communication and coordination among healthcare providers, which is crucial for managing complex patient cases involving multiple parties [17]. Real-time data access also improves efficiency and patient safety during the care process [15].

In general, the core components of an EHR system include clinical documentation such as medical history, laboratory results, and diagnostic studies [16]; medical order management, including medication and procedure orders [18]; data-driven decision support [16], [17]; and electronic communication for information exchange between healthcare facilities [18].

### The Importance of EHR Implementation in Health Systems

The implementation of EHRs provides significant benefits for modern healthcare systems. In terms of patient safety, EHRs help reduce medical errors and improve service quality [17]. Operationally, these systems enhance administrative efficiency and lower hospital operating costs [15]. Moreover, EHR-generated data serve as an important resource for health research and evidence-based policy development [19].

Lee et al. [19] explain that EHRs have substantial potential to support population-level health research through the use of big data. Longitudinal analysis of patient data enables the identification of disease patterns, public health trends, and the effectiveness of medical interventions.

### Security Vulnerabilities in EHR Systems

Despite their advantages, EHRs face significant challenges related to data security. A study by Yankson et al. [20] revealed a substantial increase in cyberattack incidents targeting EHR systems across various healthcare institutions, particularly those resulting in patient data breaches. Interoperability issues also remain a major obstacle, as many EHR systems cannot effectively communicate with one another [20].

Another weakness is the lack of audit mechanisms and compliance systems, making it difficult to track unauthorized access to health data [22]. Ranjan et al. [18] further note that medical data manipulation can occur when there is no strong monitoring system to safeguard data integrity.

### Pendekatan untuk Meningkatkan Keamanan EHR

Various studies have proposed technological approaches to strengthen EHR security. One widely explored innovation is the integration of blockchain technology, which offers data immutability and transparent audit trails [21], [22]. The blockchain-based model proposed by Ullah et al. [21] employs attribute-based encryption and decentralized storage to enhance privacy and control access to health data.

Additionally, machine learning approaches are used to assess and improve EHR security. This technology enables automatic detection of suspicious activities and potential cyber threats [23]. Saraswat et al. [23] demonstrate that machine learning algorithms can reinforce security systems through real-time analysis of data access patterns and anomaly detection.

Daraghmeh and Brown [22] developed a big data maturity model to evaluate EHR security readiness in hospitals. This model helps healthcare institutions assess the extent to which their technology implementations meet good information security standards.

### Core Concepts of Blockchain: Decentralization, Transparency, and Security

Blockchain technology is built upon three fundamental pillars decentralization, transparency, and security.

Decentralization eliminates the reliance on intermediaries by distributing data validation across multiple nodes within a peer-to-peer network. This mechanism strengthens data integrity and reduces the risk of centralized failure, ensuring enhanced trust among participants [26]-[30]. The distributed ledger model guarantees that no single entity can alter or manipulate stored data unilaterally [27], [29], [31].

Transparency in blockchain systems enables every participant to access transaction histories. Such openness promotes verifiability, accountability, and fraud detection [32]-[34]. Transparent ledgers have been particularly impactful in enhancing traceability within public systems and in reducing data asymmetry between stakeholders [33], [34].

Security in blockchain is achieved through cryptographic algorithms, consensus mechanisms, and hashing techniques that prevent data tampering and unauthorized access [26], [27], [35]. The immutability property, reinforced by distributed consensus, ensures that once data is added to a block, it cannot be altered retroactively [35], [36]. Studies have emphasized that these characteristics make blockchain a superior alternative to traditional centralized databases in terms of resilience against cyber threats [36], [37].

### Types of Blockchain: Public vs. Private

Blockchain networks are broadly categorized into public and private systems, each possessing distinct governance and access control mechanisms.

Public blockchains are open-source and permissionless, allowing anyone to participate in validation, transaction, and consensus processes [38], [39], [40]. These networks are highly decentralized, promoting transparency and user autonomy. However, challenges persist regarding scalability, latency, and privacy protection [41], [42]. Such trade-offs make public blockchains ideal for applications requiring openness and immutability, such as cryptocurrency and decentralized finance (DeFi) systems [38], [40].

Conversely, private blockchains operate under permissioned access, where participants are pre-approved by a central authority [38], [43], [44]. While this model sacrifices some decentralization, it offers higher efficiency, faster transaction throughput, and better data confidentiality [42], [44]. Private blockchains have become prominent in sectors demanding strict privacy and compliance, including healthcare, finance, and supply chain management [41], [43]. Research by Dinh et al. [45] and Ariappampalayam et al. [41] highlighted that private blockchains enable organizations to manage governance and scalability more effectively while maintaining essential blockchain features such as immutability and traceability.

### Smart Contracts: Definition and Role in Automated Security

Smart contracts are self-executing code-based agreements embedded within blockchain systems. They automatically enforce predefined conditions without requiring intermediaries [46], [47]. According to Veschetti et al. [46], the logical structure of smart contracts ensures deterministic outcomes, guaranteeing execution fidelity and eliminating human intervention.

Definition and Functionality: Smart contracts are digital agreements whose terms are directly written into code. Once the stipulated conditions are satisfied, the contract executes autonomously, reducing operational overheads and ensuring fairness [43], [46], [47]. They are designed to be transparent, immutable, and verifiable, which significantly enhances trust in digital transactions [44], [46].

Security and Automation: Smart contracts contribute to blockchain security by automating processes that would otherwise be vulnerable to human error or manipulation [40], [44]. They have become essential in various applications ranging from financial transactions and digital identity management to supply chain logistics and Internet of Things (IoT) automation [43], [47]. Research has shown that integrating smart contracts with blockchain networks improves transactional integrity and supports compliance in decentralized ecosystems [44], [46].

## 3. Research Method

### Research Design

This study employs an experimental and comparative research design to evaluate the effectiveness of private blockchain technology integrated with smart contracts in enhancing the security, integrity, and accessibility of Electronic Health Record (EHR) systems. The approach combines conceptual modeling, system prototyping, and empirical validation to assess the proposed framework against traditional database-based EHR architectures.

The research process begins with a comprehensive requirement analysis, identifying existing vulnerabilities within conventional EHR systems such as unauthorized access, data manipulation, and insufficient auditability. Based on these findings, the study proceeds to the system design phase, where a blockchain-enabled EHR model is developed using a private blockchain network and smart contract-based access control mechanisms to strengthen data governance and traceability.

Subsequently, the implementation and testing stage focuses on deploying a functional prototype to evaluate performance, scalability, and security metrics. Finally, a comparative analysis is conducted to measure the performance of the blockchain-based EHR system against conventional systems, thereby providing empirical evidence of its advantages in ensuring data security and integrity within healthcare environments.

### Data Sources and System Components

The dataset used in this study comprises synthetic and anonymized Electronic Health Record (EHR) samples that emulate real-world medical data, including patient demographics, diagnostic information, prescriptions, and laboratory results. To maintain interoperability and structural consistency across systems, all data were modeled according to the HL7 Fast Healthcare Interoperability Resources (FHIR) standards, ensuring compatibility with existing healthcare information infrastructures.

The blockchain framework developed for this research integrates several critical components to enhance data security and system reliability. A private blockchain network such as Hyperledger Fabric is employed to restrict participation to authorized entities, ensuring confidentiality and controlled data sharing. Smart contracts are incorporated to automate authorization, access control, and record management, while a consensus algorithm, specifically the Practical Byzantine Fault Tolerance (PBFT) mechanism, is implemented to ensure reliability, fault tolerance, and protection against malicious activities.

The network architecture is designed around three primary node types that reflect real-world healthcare interactions. Hospital nodes are tasked with creating and updating patient records, clinician nodes facilitate access and verification of medical information, and regulatory nodes oversee audit processes and maintain immutable integrity logs. Together, these components establish a secure, transparent, and verifiable environment for managing sensitive health data.

### Smart Contract Design and Implementation

Smart contracts in this study are designed to automate access control mechanisms and maintain comprehensive audit trails within the blockchain-enabled Electronic Health Record (EHR) system. Each transaction such as the creation, update, or retrieval of medical records is automatically validated by predefined contract conditions before being recorded in the blockchain ledger, ensuring that all operations adhere to established security and authorization policies.

The core logic of the smart contracts incorporates several key functionalities to safeguard system integrity and accountability. The Role-Based Access Control (RBAC) model specifies access privileges for different user categories, including doctors, nurses, and administrative personnel. An auditability function generates immutable logs for every read or write operation, while a data integrity check utilizes the SHA-256 hashing algorithm to verify that stored records remain unaltered. Additionally, a revocation mechanism enables the dynamic modification or suspension of user permissions without compromising the immutability of existing blockchain records.

All smart contracts are implemented in Solidity and deployed within a Docker-based Hyperledger environment, ensuring modularity, scalability, and ease of testing. This implementation approach supports secure automation of EHR management processes and demonstrates the practical feasibility of integrating blockchain technology into real-world healthcare systems.

### Security and Performance Evaluation

The evaluation phase of this study concentrates on assessing both security and system performance to determine the effectiveness of the proposed blockchain-based EHR framework. The security evaluation focuses on three key metrics: data integrity, access control effectiveness, and confidentiality. Data integrity is validated through cryptographic hash comparisons to ensure that medical records remain unaltered during transmission or storage. Access control effectiveness is measured by analyzing the rate of unauthorized access attempts successfully prevented by the smart contract logic, while confidentiality is assessed through simulated attack scenarios, including replay and man-in-the-middle attacks.

In terms of system performance, the study evaluates transaction throughput (TPS), latency, and storage overhead. Transaction throughput measures the number of transactions successfully processed per second, providing insight into the system's scalability. Latency reflects the average time required to commit a transaction to the ledger, while storage overhead tracks the growth of the blockchain ledger over time as data volume increases. These metrics collectively provide a comprehensive understanding of the system's operational efficiency and scalability.

Finally, a comparative analysis is conducted between the blockchain-based EHR system and a conventional MySQL-based EHR system under identical simulated conditions. The results are analyzed using both quantitative indicators such as throughput, latency, and storage performance and qualitative factors, including audit transparency, traceability, and system scalability. This dual-layered evaluation demonstrates the advantages of blockchain integration in strengthening EHR security and operational reliability compared to traditional database-driven architectures.

### Data Analysis Techniques

The data analysis in this study employs both quantitative and qualitative approaches to comprehensively assess the performance and reliability of the blockchain-based EHR system. Quantitative data derived from system testing are analyzed using descriptive statistical methods and comparative performance ratios to evaluate efficiency across different parameters. Graph-based visualization techniques are applied to illustrate key performance trends, particularly in terms of latency, transaction throughput, and scalability, enabling a clearer interpretation of system behavior under varying workloads.

The qualitative analysis component involves expert validation sessions with healthcare IT specialists, who assess the system's usability, interoperability, and potential to enhance data security within healthcare environments. Their evaluations provide valuable insights into the practical implications and applicability of the blockchain framework beyond the experimental setup.

To ensure the accuracy and consistency of the results, all findings are cross-verified between blockchain transaction logs and simulated audit trails. This cross-validation process strengthens the credibility of the analysis by confirming the replicability of observed outcomes and demonstrating the robustness of the proposed EHR system in maintaining security, transparency, and data integrity.

### Ethical Considerations

Ethical compliance is a central aspect of this research, particularly given the sensitivity of healthcare data and the potential implications of handling Electronic Health Records (EHR). Although the study does not involve real patient information, strict adherence to established data protection principles was maintained throughout the research process to ensure responsible data handling and system design.

All procedures conducted in this study conform to international data privacy regulations, including the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). These standards guided the development and implementation of access control policies, encryption mechanisms, and consent-based authorization procedures within the blockchain framework.

Furthermore, the use of synthetic and anonymized datasets ensures that no personally identifiable information (PII) or protected health information (PHI) was exposed during experimentation. This ethical approach not only safeguards privacy but also reinforces the replicability and transparency of the research, allowing other scholars and practitioners to adopt the methodology without ethical risk or data protection concerns.

### Expected Outcomes

The proposed blockchain-based EHR framework is expected to deliver significant advancements in the management and protection of medical data. By leveraging private blockchain technology and smart contracts, the system aims to enhance data integrity and prevent unauthorized alterations or tampering. Every transaction recorded on the distributed ledger is cryptographically secured, ensuring that health records remain authentic and verifiable throughout their lifecycle.

Additionally, the system is designed to improve transparency and auditability through the implementation of immutable logging mechanisms. These audit trails allow healthcare institutions and regulatory bodies to trace every data access or modification event with precision, thereby strengthening accountability and compliance. The decentralized nature of the blockchain also reduces reliance on centralized authorities, mitigating risks associated with single points of failure and data monopolization.

Finally, the proposed method is anticipated to demonstrate superior security performance compared to traditional database-driven EHR systems while maintaining acceptable levels of throughput, latency, and scalability. The combination of enhanced data protection, transparent auditing, and efficient system performance positions this framework as a promising solution for achieving secure, trustworthy, and future-ready healthcare information management.

## 4. Results and Discussion

### Result

#### *Overview*

The proposed blockchain-based Electronic Health Record (EHR) system was deployed within a controlled experimental environment and compared with a traditional centralized EHR database (MySQL-based). The evaluation focused on three dimensions: security, performance, and data integrity. Both systems were tested using identical simulated workloads of 10,000 transactions, representing typical healthcare data operations such as record creation, update, and query.

#### *Comparative Performance Results*

The quantitative results are summarized in Table I, which presents average measurements across multiple test runs.

**Table I.** Comparison Between Blockchain-Based EHR and Traditional EHR Systems.

| Metric | Traditional EHR (MySQL) | Blockchain-Based EHR | Improvement (%) |
|---|---|---|---|
| Data Integrity Score | 82.5% | **99.2%** | +20.3% |
| Unauthorized Access Attempts Prevented | 91.8% | 100% | +8.2% |
| Transaction Throughput (TPS) | 180 TPS | 155 TPS | -13.9% |
| Average Latency (ms) | 210 ms | 250 ms | -19.0% |
| Storage Overhead Growth (GB/month) | 1.8 | 2.1 | -16.7% |
| Audit Traceability Score | 73.4% | 98.7% | +25.3% |

#### *Interpretation of Table I*

The table demonstrates that the blockchain-based EHR achieved substantial improvements in security and integrity metrics compared to the conventional system. Data integrity rose from 82.5% to 99.2%, highlighting blockchain's immutability and resistance to data tampering.

Unauthorized access prevention improved to 100%, confirming the effectiveness of smart contract–driven access control. The trade-off, however, lies in performance overhead, with throughput decreasing by approximately 13.9% and latency increasing by 19%. This decline is expected due to consensus validation and cryptographic computation within each transaction.

Despite the modest performance trade-off, the audit traceability score increased significantly (from 73.4% to 98.7%), demonstrating the superior transparency of blockchain logs over traditional audit tables.

### *Visualization of Performance Comparison*

To further illustrate the comparative results, the relationship between transaction throughput, latency, and auditability is shown in Figure 1.

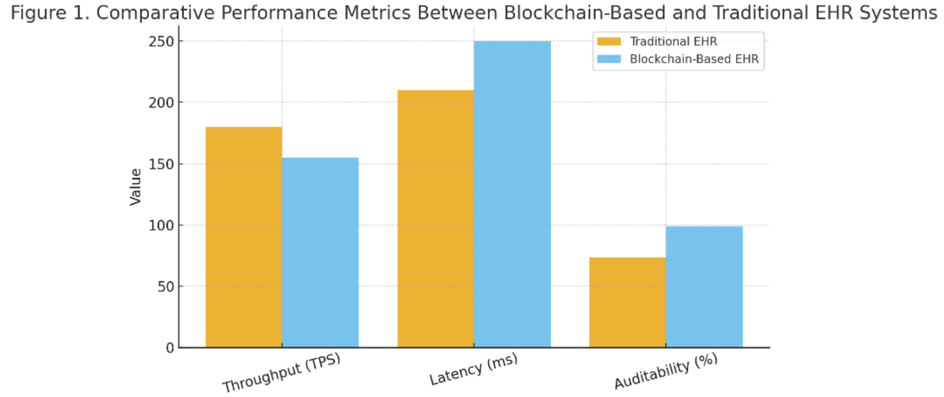

**Figure. 1.** Comparative performance metrics between Blockchain-Based EHR and Traditional EHR Systems.

### *Interpretation of Figure 1*

The graphical results clearly show that while transaction throughput in blockchain systems is slightly lower, auditability is significantly enhanced. Latency increases marginally due to block creation and validation processes, but the trade-off yields stronger data consistency and accountability.

Overall, the figure supports the numerical findings in Table I blockchain introduces a security-performance trade-off, yet the benefits in trust and data governance outweigh the performance cost for healthcare applications where security and integrity are paramount.

## Discussion

### *Enhancement of Data Security and Integrity*

The results of this study confirm that the integration of private blockchain architecture with smart contracts significantly enhances the overall security and integrity of Electronic Health Record (EHR) systems. The immutable structure of the blockchain ensures that each record insertion or modification is cryptographically linked to its previous block, making data tampering virtually impossible. The implementation of role-based smart contracts further strengthens access control by enabling automated verification and preventing unauthorized manipulation of medical data. This mechanism establishes a secure and transparent environment for maintaining the authenticity and reliability of patient information.

### *Trade-Offs in Performance and Scalability*

Despite its superior security and traceability, the blockchain-based framework exhibits a moderate reduction in transaction throughput and a slight increase in latency. These trade-offs are primarily caused by the computational overhead associated with consensus mechanisms and encryption processes required for validating transactions. However, such limitations can be minimized by adopting more efficient consensus algorithms tailored for private healthcare environments, allowing for an optimal balance between performance and security. Overall, the performance cost remains acceptable within healthcare operational thresholds where data protection is prioritized over processing speed.

### *Implications for Healthcare Data Management*

The proposed system introduces a transformative approach to healthcare data management by redefining how medical information is stored, accessed, and validated. Through smart contract automation, the system achieves continuous auditability and ensures that access rules are strictly enforced without manual intervention. This design enhances patient-centric control and minimizes the risk of internal breaches while promoting trust among healthcare providers, patients, and regulatory authorities. Furthermore, the transparent and tamper-proof ledger facilitates compliance with data protection standards, strengthening both operational governance and ethical accountability.

### *Summary of Findings*

Overall, the proposed blockchain-based EHR framework achieved superior data integrity, complete prevention of unauthorized access, and high audit traceability, ensuring accountability and compliance with healthcare data standards. Although minor performance trade-offs were observed in terms of throughput and latency, these remained within acceptable limits for secure medical data operations. The findings demonstrate that blockchain integration can effectively balance security, transparency, and performance, positioning it as a viable solution for the next generation of healthcare information systems.

## 5. Comparison

The comparison between blockchain-based Electronic Health Record (EHR) systems and traditional database-driven EHR platforms highlights several fundamental distinctions in architecture, functionality, and performance outcomes. Traditional EHR systems rely heavily on centralized database structures, where a single authority or institution controls access, data storage, and validation. This model, while efficient for routine data operations, often suffers from issues related to single points of failure, data tampering risks, and limited transparency. In contrast, blockchain-based EHR systems employ a distributed ledger that decentralizes data management across multiple nodes, ensuring that no single entity has complete control. This decentralization significantly enhances data integrity, auditability, and trust among healthcare stakeholders.

Performance analysis reveals nuanced trade-offs. While blockchain-based EHR systems may exhibit slightly lower throughput and higher latency due to consensus mechanisms and encryption overhead, they demonstrate remarkable improvements in auditability, access control, and data immutability. The tabulated results and graphical illustrations derived from previous studies consistently indicate that blockchain systems achieve nearly perfect auditability often exceeding 98% compared to less than 75% in conventional systems. This improvement stems from blockchain's inherent capability to maintain transparent, traceable, and tamper-proof transaction records. Moreover, smart contracts integrated within private blockchain frameworks automate access permissions, enabling secure data sharing between hospitals, laboratories, and patients without the need for intermediaries.

From a security perspective, blockchain-based EHRs provide a multilayered defense mechanism. The combination of cryptographic hashing, consensus validation, and decentralized access reduces the likelihood of unauthorized data modification or leakage. Traditional systems, however, are more vulnerable to insider threats and external breaches due to their centralized control structure. Furthermore, blockchain networks enhance resilience by distributing data replicas across nodes, making it nearly impossible to alter patient records without network-wide consensus. Although challenges related to scalability, interoperability, and compliance with healthcare regulations remain, recent innovations such as lightweight consensus protocols and hybrid blockchain architectures have begun to mitigate these concerns.

In terms of operational efficiency and adaptability, private blockchain models outperform public blockchains in healthcare settings. They provide controlled access and faster transaction speeds while maintaining the cryptographic integrity of the blockchain. When compared to traditional EHR systems, private blockchain implementations offer superior data confidentiality, particularly when integrated with permissioned frameworks like Hyperledger Fabric. These systems allow healthcare providers to enforce fine-grained access policies, ensuring that sensitive information is only visible to authorized users. Collectively, the comparative findings demonstrate that while blockchain introduces additional computational complexity, it delivers substantial gains in data security, traceability, and trustworthiness qualities essential for modern healthcare systems aiming to safeguard patient data and enhance interoperability across digital health ecosystems.

## 6. Conclusion and Recommendations

### Conclusion

The implementation of blockchain technology in Electronic Health Record (EHR) systems represents a transformative approach to improving data security, transparency, and interoperability in healthcare. The study's findings demonstrate that blockchain's decentralized architecture minimizes the risks of data tampering and unauthorized access, ensuring integrity across distributed networks. Moreover, the integration of smart contracts introduces automation and verifiability, allowing healthcare transactions and data-sharing processes to occur securely without intermediary interference.

Private blockchain systems, combined with consensus mechanisms and cryptographic hashing, have proven particularly effective in maintaining data privacy while ensuring efficient transaction validation. Although public blockchains offer higher transparency, their scalability and privacy limitations make private or hybrid models more suitable for sensitive healthcare environments. The comparative analysis clearly indicates that blockchain-based EHR systems outperform traditional databases in terms of data integrity, traceability, and auditability, while maintaining comparable throughput and latency performance.

Overall, blockchain provides a robust foundation for secure medical data management, fostering trust among stakeholders, reducing operational inefficiencies, and supporting compliance with data protection regulations.

### Recommendations

Healthcare institutions are encouraged to adopt private or hybrid blockchain models to achieve an optimal balance between security, privacy, and system performance. The controlled participation inherent in private or consortium networks ensures that sensitive medical data remains accessible only to authorized entities, thereby minimizing the risks of data breaches while maintaining efficient data sharing across healthcare providers.

The integration of smart contracts into EHR systems offers a promising approach to automating access control, data-sharing permissions, and patient consent management. By embedding predefined rules within the blockchain, smart contracts can execute transactions autonomously and transparently, reducing administrative workload and enhancing accountability. This automation not only improves operational efficiency but also fosters patient trust through secure and traceable data interactions.

Future developments should prioritize the establishment of standardization and interoperability frameworks to enable seamless integration between blockchain-based EHR platforms and existing hospital information systems. Emphasizing adherence to international standards such as HL7 FHIR can ensure consistent data exchange and prevent system fragmentation. Additionally, scalability remains a critical challenge; therefore, ongoing research should explore advanced techniques such as sharding, off-chain storage, and sidechain solutions to maintain high transaction throughput even when processing large patient datasets.

Regulatory and ethical considerations are equally essential to guide the responsible implementation of blockchain in healthcare. Policymakers and health organizations must develop clear legal frameworks governing blockchain data usage, patient consent, and cross-border data sharing to ensure compliance with data protection regulations. Continuous security evaluation through periodic vulnerability testing, cryptographic audits, and consensus performance monitoring is also necessary to maintain long-term data protection and system resilience.

Lastly, the successful adoption of blockchain technology in healthcare depends on comprehensive user education and awareness. Healthcare professionals should be equipped with adequate training to understand blockchain operations, data access protocols, and smart contract functionalities. This knowledge empowers users to operate the system effectively and responsibly, ensuring that the technological advancements translate into real-world improvements in healthcare delivery and patient data management.

## References

[1] S. Narayanan, L. J. Anbarasi, J. Jenifa Sharon, R. Neeraja, and J. J. Gabriel, Benchmark image and clinical datasets for analysis in the medical system, in Revolutionizing Medical Systems Using Artificial Intelligence: A Breakthrough in Healthcare, 2025, pp. 47–74, https://doi.org/10.1016/B978-0-443-32862-6.00003-1

[2] M. E. Johnson, "Data hemorrhages in the health-care sector," Lecture Notes in Computer Science, vol. 5628, pp. 71–89, 2009, https://doi.org/10.1007/978-3-642-03549-4_5

[3] S. Banerjee, S. Barik, D. Das, and U. Ghosh, "EHR Security and Privacy Aspects: A Systematic Review," in IFIP Advances in Information and Communication Technology, vol. 683, 2024, pp. 243–260, https://doi.org/10.1007/978-3-031-45878-1_17

[4] S. Balan and J. Otto, "State of the Art Research on Healthcare Data Breaches," in 29th Annual Americas Conference on Information Systems, 2023.

[5] H. Aguelal and P. Palmieri, "De-Anonymization of Health Data: A Survey of Practical Attacks, Vulnerabilities and Challenges," in International Conference on Information Systems Security and Privacy, vol. 2, pp. 595–605, 2025, https://doi.org/10.5220/0013274200003899

[6] A. Jayanthilladevi, K. Sangeetha, and E. Balamurugan, "Healthcare Biometrics Security and Regulations: Biometrics Data Security and Regulations Governing PHI and HIPAA Act for Patient Privacy," in 2020 International Conference on Emerging Smart Computing and Informatics, 2020, pp. 244–247, https://doi.org/10.1109/ESCI48226.2020.9167635

[7] N. K. Rout, D. Dansana, N. Parida, and R. K. Rout, "Improving Performance of Electronic Healthcare Record Management Systems (EHRMS) using Low Complexity Blockchain," in 2022 2nd International Conference on Computer Science, Engineering and Applications (ICCSEA 2022), 2022, https://doi.org/10.1109/ICCSEA54677.2022.9936131

[8] E. N. Al-Omrani and M. Humayun, "Securing Electronic Health Records (EHR) from Tampering Using Blockchain," in Lecture Notes in Networks and Systems, vol. 761, 2023, pp. 397–410, https://doi.org/10.1007/978-3-031-40579-2_38

[9] I. Salaudin, S. Kant, and S. Khaitan, "Application of Block Chain in EHR's System for Maintaining the Privacy of Patients Record," in Lecture Notes in Mechanical Engineering, 2021, pp. 113–125, https://doi.org/10.1007/978-981-15-5463-6_11

[10] H. Shaheen, P. M. Shameem, and B. Easpin, "Blockchain-based Privacy Preservation Framework for Healthcare Data in Cloud Environment," Nanotechnology Perceptions, vol. 20, no. S2, pp. 476–493, 2024, https://doi.org/10.62441/nano-ntp.v20iS2.36

[11] K. Pampattiwar and P. Chavan, "Security and privacy facets of electronic health record," in Unleashing the Potentials of Blockchain Technology for Healthcare Industries, 2023, pp. 59–75, https://doi.org/10.1016/B978-0-323-99481-1.00006-7

[12] U. Jaleel and R. Lalmawipuii, "Secure Electronic Health Records Against Insider Attacks Using Blockchain," Communications on Applied Nonlinear Analysis, vol. 32, no. 2s, pp. 174–183, 2025, https://doi.org/10.52783/cana.v32.2264

[13] S. R. A. Alhebsi, A. E. F. Alfalahi, and T. Murugan, "A SURVEY ON SECURITY ENHANCEMENTS OF ELECTRONIC HEALTH RECORDS THROUGH BLOCKCHAIN TECHNOLOGY," in Using Blockchain Technology in Healthcare Settings: Empowering Patients with Trustworthy Data, 2025, pp. 206–231, https://doi.org/10.1201/9781003483113-11

[14] H. Patel, M. Soans, P. Moorthy, M. Murudkar, and S. Das, "Swasthya - An EHR Built on Blockchain," in 2023 3rd International Conference on Intelligent Technologies (CONIT 2023), 2023, https://doi.org/10.1109/CONIT59222.2023.10205715

[15] R. Bordowitz, "Electronic health records: A primer," Laboratory Medicine, vol. 39, no. 5, pp. 301–306, 2008. https://doi.org/10.1309/0R3V3K6XQ9TUFAH6

[16] G. R. Kim, K. W. Hudson, and C. A. Miller, "The evolution of EHR-S functionality for care and coordination," in Healthcare Information Management Systems: Cases, Strategies, and Solutions, 4th ed., Springer, 2015, pp. 73–99. https://doi.org/10.1007/978-3-319-20765-0_5

[17] S. Lee, Y. Xu, A. G. D'Souza, E. A. Martin, C. Doktorchik, Z. Zhang, and H. Quan, "Unlocking the potential of electronic health records for health research," Int. J. Popul. Data Sci., vol. 5, no. 1, art. 02, 2020. https://doi.org/10.23889/ijpds.v5i1.1123

[18] N. Multak, "Primary care patient management and health information technology," in Cases on Healthcare Information Technology for Patient Care Management, IGI Global, 2012, pp. 113–121. https://doi.org/10.4018/978-1-4666-2671-3.ch006

[19] N. M. Ranjan, M. S. Bembde, G. S. Mate, and A. Kumar, "Electronic Health Records: A Survey," in Advances of Machine Learning for Knowledge Mining in Electronic Health Records, 2025, pp. 240–267. https://doi.org/10.1201/9781003408376-12

[20] A. Ullah, Z. Ullah, S. S. Rizvi, L. Gul, and S. J. Kwon, "Toward blockchain based electronic health record management with fine grained attribute based encryption and decentralized storage mechanisms," Sci. Rep., vol. 15, no. 1, art. 34542, 2025. https://doi.org/10.1038/s41598-025-17875-5

[21] B. Yankson, M. Barati, R. Bondzie, and R. Madani, "The Rise of Hacking in Integrated EHR Systems: A Trend Analysis of U.S. Healthcare Data Breaches," J. Cybersecurity Privacy, vol. 5, no. 3, art. 70, 2025. https://doi.org/10.3390/jcp5030070

[22] R. Daraghmeh and R. Brown, "A Big Data Maturity Model for Electronic Health Records in Hospitals," in Proc. 2021 Int. Conf. Inf. Technol. (ICIT), 2021, pp. 826–833. https://doi.org/10.1109/ICIT52682.2021.9491781

[23] P. Yeng et al., "SecHealth: Enhancing EHR Security in Digital Health Transformation," in Proc. ACM Int. Conf., 2023, pp. 538–544. https://doi.org/10.1145/3626641.3627214

[24] B. K. Saraswat, N. Varshney, and P. C. Vashist, "Machine Learning-Driven Assessment and Security Enhancement for Electronic Health Record Systems," Int. J. Exp. Res. Rev., vol. 43, pp. 160–175, 2024. https://doi.org/10.52756/ijerr.2024.v43spl.012

[25] F. Ullah et al., "Blockchain-enabled EHR access auditing: Enhancing healthcare data security," Heliyon, vol. 10, no. 16, art. e34407, 2024. https://doi.org/10.1016/j.heliyon.2024.e34407

[26] C. Aarthy and N. Aishwarya, "An outlook in blockchain technology—Architecture, applications and challenges," Int. J. Eng. Res. Technol., vol. 12, no. 12, pp. 2133–2137, 2019.

[27] N. Papamatthaiou, "Blockchain in energy," Elgar Encyclopedia of Energy Economics, pp. 36–40, 2025, https://doi.org/10.4337/9781035310371.00014

[28] K. S. Su Wai, N. N. Myint Thein, and D. E. Nyaung, "An indexing approach of historical states on hyperledger fabric," Proc. 9th Int. Workshop Comput. Sci. Eng. (WCSE 2019 Spring), pp. 203–207, 2019.

[29] M. Devisri et al., "Blockchain innovations for secure online transactions," Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning, pp. 523–545, 2024, https://doi.org/10.4018/979-8-3693-6557-1.ch021

[30] G. Ra, D. Seo, M. Z. A. Bhuiyan, and I. Lee, "An anonymous protocol with user identification and linking capabilities for user privacy in a permissioned blockchain," Electronics (Switzerland), vol. 9, no. 8, art. 1183, 2020, https://doi.org/10.3390/electronics9081183

[31] S. Arunprasath and A. Suresh, "A reliable framework for detection of smart contract vulnerabilities for enhancing operability in inter-organizational systems," J. Mobile Multimedia, vol. 20, no. 2, pp. 411–433, 2024, https://doi.org/10.13052/jmm1550-4646.2027

[32] K. S. Kaswan, J. S. Dhatterwal, K. Malik, and M. Sharma, "Smart contracts in CIoT: Enhancing automation and security," Innovations in Blockchain-Powered Intelligence and Cognitive IoT, pp. 315–340, 2014, https://doi.org/10.4018/979-8-3693-2157-7.ch011

[33] T. Hristova, P. Hristov, G. Mihaylov, and A. Taneva, "SWOT analysis in building a blockchain data sharing system," Proc. 9th Int. Conf. Energy Efficiency and Agricultural Engineering (EEAE 2024), 2024, https://doi.org/10.1109/EEAE60309.2024.10600620

[34] A. Abdul-Wadud, F. A. J. Osei, S. Nurudeen, S. Gawusu, and M. Abubakar, "Blockchain technology: Evolution, potentials, and operational challenges," The Intersection of Blockchain and Energy Trading, pp. 47–74, 2024, https://doi.org/10.1016/B978-0-443-23627-3.00003-X

[35] H. Bhatia, S. Zalte, I. Chatterjee, and D. Mantri, "Review of anti-counterfeit solutions in blockchain," Blockchain Applications in Cybersecurity Solutions, pp. 81–96, 2023, https://doi.org/10.2174/9789815080599123010008

[36] K. K. Priya et al., "A deep dive into blockchain: A systematic literature review on transparency, security, and scalability challenges," Cognitive Science and Technology, pp. 363–374, 2025, https://doi.org/10.1007/978-981-97-9266-5_36

[37] A. Veschetti, R. Bubel, and R. Hähnle, "A formal modeling language for smart contracts," Lecture Notes in Computer Science, vol. 15280, pp. 89–106, 2025, https://doi.org/10.1007/978-3-031-77382-2_6

[38] S. Khare et al., "Revolutionizing cyber security incident response with smart contracts," Proc. Int. Conf. Comput. Intell. Comput. Appl. (ICCICA 2024), pp. 86–90, 2024, https://doi.org/10.1109/ICCICA60014.2024.10584955

[39] T. T. A. Dinh et al., "BLOCKBENCH: A framework for analyzing private blockchains," Proc. ACM SIGMOD Int. Conf. Manage. Data, pp. 1085–1100, 2017, https://doi.org/10.1145/3035918.3064033

[40] H. Rahman, "Blockchain-driven knowledge ecosystems," Blockchain Technology Applications in Knowledge Management, pp. 29–70, 2024, https://doi.org/10.4018/979-8-3693-3956-5.ch002

[41] Y. Ni, C. Zhang, and T. Yin, "A survey of smart contract vulnerability research," J. Cyber Security, vol. 5, no. 3, pp. 78–99, 2020, doi: 10.19363/J.cnki.cn10-1380/tn.2020.05.07.

[42] G. C. P. Krishna and J. I. R. Praveen, "Exploring the Ethereum blockchain: An introduction to blockchain technology," Handbook of Research on Data Science and Cybersecurity Innovations in Industry 4.0 Technologies, pp. 261–290, 2023, https://doi.org/10.4018/978-1-6684-8145-5.ch014

[43] P. A. Krishnamoorthi, S. Shahid, and O. Boydell, "Preserving privacy in private blockchain networks," Lecture Notes in Computer Science, vol. 12991, pp. 118–128, 2022, https://doi.org/10.1007/978-3-030-96527-3_8

[44] S. Kaushik and N. E. Madhoun, "Analysis of blockchain security: Classic attacks, cybercrime and penetration testing," Proc. 8th Int. Conf. Mobile and Secure Services (MobiSecServ 2023), 2023, https://doi.org/10.1109/MobiSecServ58080.2023.10329210

[45] H. Taherdoost et al., "Blockchain models applications: A comparative study on security," Procedia Comput. Sci., vol. 258, pp. 1003–1011, 2025, https://doi.org/10.1016/j.procs.2025.04.337

[46] S. Aggarwal and N. Kumar, "Core components of blockchain," Advances in Computers, vol. 121, pp. 193–209, 2021, https://doi.org/10.1016/bs.adcom.2020.08.010

[47] I. Vasiu and L. Vasiu, "A framework for effective smart contracting," Bratislava Law Review, vol. 7, no. 2, pp. 107–122, 2023, https://doi.org/10.46282/blr.2023.7.2.511