INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 15, Issue 4, (2025) E-ISSN: 2222-6990

A Blockchain Technology Framework to Enhance Security and Interoperability of Electronic Healthcare Records

Deng Zilong[1,3], Mustafa Muwafak Alobaedy[2], Mohd Nurul Hafiz Bin Ibrahim[4], Xiaocun Huang[5]

[1,2,4]City Graduate School, City University, Malaysia, [3]Anqing Vocational & Technical College,China, [5]Cangzhou Normal University,China,

Email: mustafa.theab@city.edu.my, mohd.nurul.hafiz@city.edu.my, huangxiaocun@caztc.edu.cn

Coressponding Author Email: dzlong@aqvtc.edu.cn

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v15-i4/25319 DOI:10.6007/IJARBSS/v15-i4/25319

Published Date: 22 April 2025

Abstract

This research proposes a blockchain-centered framework designed to address ongoing challenges related to data security, privacy, and interoperability in Electronic Healthcare Records (EHRs). As the healthcare sector increasingly relies on digitalized records, centralized EHR systems face significant risks, including data breaches, privacy violations, and limited compatibility across platforms. This study introduces a decentralized blockchain-based framework, built on Hyperledger Fabric, that leverages cryptographic methods, smart contracts, and distributed ledger technology to ensure secure data sharing, enhanced privacy, and structured access control. The research focuses on the theoretical development and practical evaluation of this framework. Using a design-based approach, the study incorporates a comprehensive literature review, framework development, and empirical testing to assess the framework's effectiveness. Key performance indicators include data integrity, security, system efficiency, and interoperability across diverse healthcare platforms. In conclusion, this framework offers a promising solution for securely managing healthcare data and ensuring interoperability, with potential applications extending beyond the healthcare sector.

Keywords*:* Blockchain, Healthcare, Electronic Health Record, Data Security, Interoperability, Framework

Introduction

The healthcare sector is undergoing a digital transformation, with Electronic Health Records (EHRs) becoming the standard for storing patient information, including medical histories and treatment plans. While EHRs improve care coordination, reduce errors, and enhance patient outcomes (Puneeth & Parthasarathy, 2023), centralized EHR systems introduce significant

risks in terms of data security, privacy, and interoperability, making them susceptible to cyberattacks (Sharma & Balamurugan, 2020). To address these challenges, this research proposes a decentralized, blockchain-enabled framework that leverages Hyperledger Fabric and smart contracts to provide secure, interoperable data management. Unlike centralized systems, which struggle with interoperability and hinder data sharing across platforms, especially during critical situations (Liu et al., 2023), the proposed blockchain framework improves EHR sharing, strengthens security, and grants patients greater control over their data (Kim et al., 2023). By incorporating cryptographic methods and decentralized governance, this framework enhances data integrity and security, offering a robust solution to the current challenges in healthcare data management (Lee et al., 2023).

Research Methodology

This study employs a design-based research methodology to develop and evaluate a novel blockchain framework focused on enhancing the security and interoperability of Electronic Health Records (EHRs). The research integrates conceptual framework and empirical validation to identify challenges and deliver a tailored solution for managing healthcare data. The methodology includes an extensive literature review, analysis of existing blockchain frameworks, and qualitative data collection through interviews with industry experts such as blockchain developers, cybersecurity specialists, and healthcare IT professionals.

The study's primary objective is to explore how blockchain technology can improve data security and privacy in healthcare while ensuring regulatory compliance and addressing the integration challenges posed by current healthcare IT systems. The research objectives are directly connected to real-world healthcare applications, particularly in refining algorithmic frameworks for more secure and efficient data management. The analysis is grounded in a comprehensive review of databases like PubMed, IEEE Xplore, and Google Scholar, ensuring the credibility and relevance of the sources used.

In addition to the literature review, the qualitative data is analyzed using thematic analysis to identify patterns and gaps in blockchain usage within healthcare. Initially, 200 articles were identified using keywords such as "blockchain in healthcare," "data security," "privacy," and "interoperability." After a thorough screening process, 115 articles were selected for an in-depth review, categorized based on their focus on blockchain architecture, consensus mechanisms, encryption techniques, and the challenges of implementation in healthcare.

By examining both the theoretical and practical aspects of blockchain adoption, the study aims to address existing knowledge gaps and suggest future development directions. This systematic approach provides a comprehensive understanding of blockchain technology's potential to resolve key challenges related to data security and interoperability in healthcare. Figure 1 shows the flow of research design, methods used, input and output in this study.

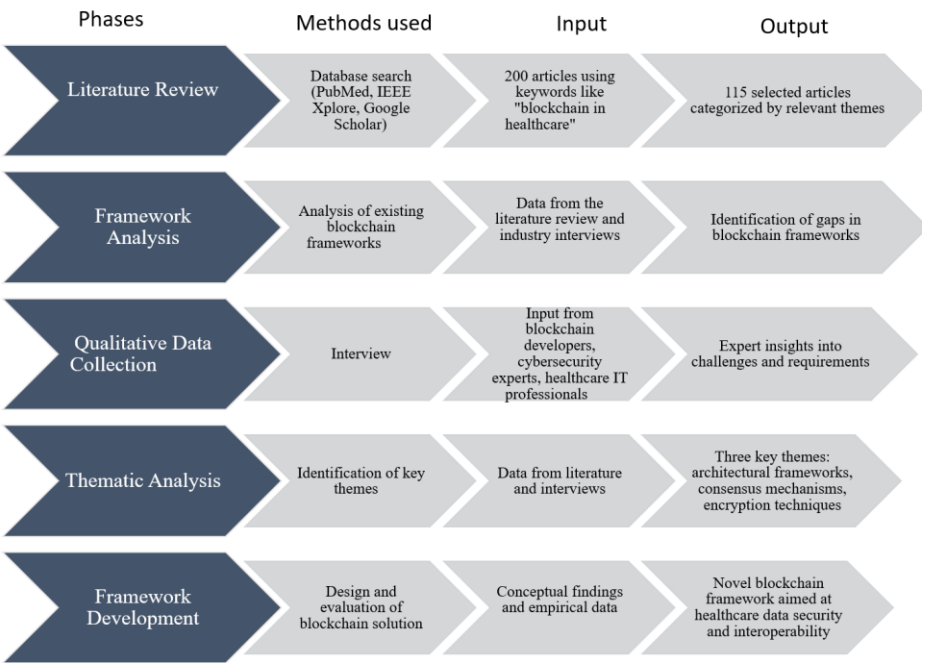

Figure 1: Research Flow

The research methodology consists of five phases, each contributing towards the systematic development of a blockchain-based EHR framework. The literature review sets the foundation by analyzing existing studies, while the framework analysis identifies gaps. Qualitative data collection through expert interviews adds practical insights, and thematic analysis extracts core themes to be addressed. Finally, the framework is developed, integrating all findings to ensure an innovative, secure, and interoperable solution for healthcare data management. This approach ensures that the final blockchain framework is comprehensive, addressing both theoretical and practical needs in healthcare data security and interoperability.

Thematic Analysis

This thematic analysis investigates the potential of blockchain technology to enhance the security and interoperability of Electronic Health Records (EHRs) in healthcare. The review identified three key themes: architectural designs and frameworks, consensus mechanisms, and encryption techniques. These themes are critical in understanding how blockchain-based frameworks can address current challenges in healthcare data management and provide more secure, efficient, and interoperable EHR systems.

Architectural Designs and Frameworks

The literature underscores the significance of permissioned blockchain systems in healthcare due to the sensitive nature of medical data, offering controlled access and enhanced privacy. However, scalability challenges emerge as healthcare generates vast amounts of data, with proposed solutions such as off-chain storage and sharding to manage these volumes (Tanwar et al., 2020). Key security features, including immutability and smart contracts, are essential to preventing unauthorized access (Attaran, 2020). Interoperability also remains a critical concern, with blockchain frameworks specifically designed to facilitate seamless data exchange across diverse healthcare platforms (Reegu et al., 2023).

Consensus Mechanisms

Several consensus mechanisms have been explored to enhance the reliability and efficiency of blockchain frameworks in healthcare. Proof of Stake (PoS) is favored over Proof of Work (PoW) due to its energy efficiency and faster transaction rates, making it more suitable for healthcare applications (Kashyap, 2024). Practical Byzantine Fault Tolerance (PBFT) is also gaining popularity for its ability to manage malicious nodes, ensuring system reliability (Simonoski & Bogatinoska, 2024). Research is ongoing into AI-enhanced consensus mechanisms to improve flexibility, security, and scalability in healthcare environments (Han et al., 2022). Hybrid mechanisms that combine PoS and PBFT are considered promising solutions, balancing security, speed, and energy efficiency in healthcare settings (Desai & Ambali, 2024).

Encryption Techniques and Data Security

Combining advanced encryption techniques with blockchain enhances data security and privacy within healthcare frameworks. Identity-Based Encryption (IBE) provides privacy without the need for complex key management, while AES and DES are effective for encrypting large datasets (Maddela, 2025). Homomorphic encryption allows secure data processing without exposing sensitive information, which is crucial for applications like medical research. Attribute-Based Encryption (CP-ABE) enables precise access control, ensuring that only authorized users can access specific patient information (Hu et al., 2023). Chaotic maps, which are highly resilient against attacks, have proven effective for encrypting medical images (Lipsa et al., 2022).

In conclusion, while blockchain frameworks demonstrate significant potential for improving data security and interoperability in healthcare, challenges related to scalability, computational overhead, and key management persist. Future research should focus on developing more scalable encryption algorithms, improving key management processes, and exploring AI-enhanced encryption methods. The successful integration of blockchain in healthcare will depend on overcoming these challenges to ensure efficient, secure, and patient-centered data management.

Proposed Framework

The blockchain-based framework enhances healthcare data management by improving the security, privacy, and interoperability of Electronic Health Records (EHRs). It combines advanced cryptographic techniques with blockchain’s decentralized architecture to ensure secure data sharing and efficient handling of patient information, particularly in cloud environments. By leveraging the Interplanetary File System (IPFS) for decentralized storage, smart contracts for automating processes, and the transparency and immutability of blockchain, this framework addresses key challenges in traditional data management. It offers a robust solution for securely managing confidential healthcare data while enhancing system efficiency and regulatory compliance.

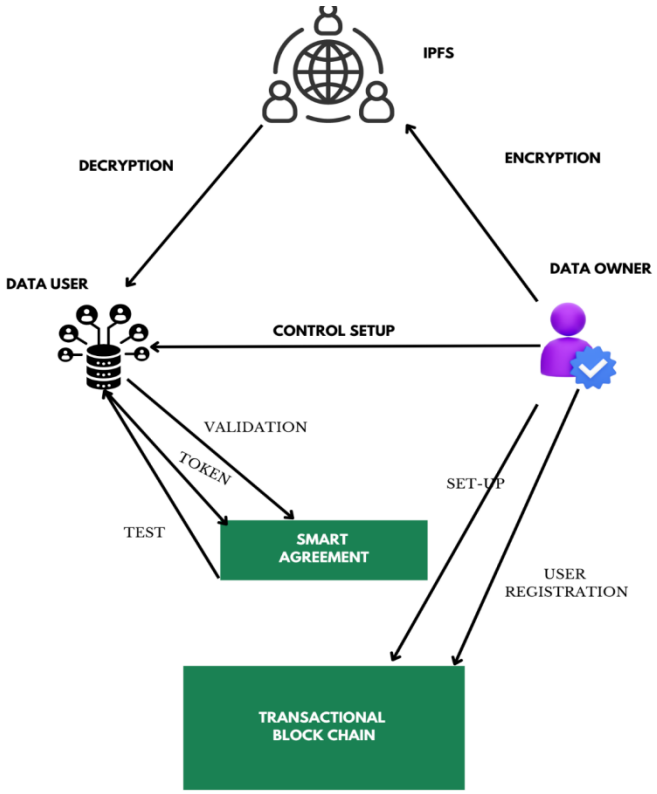

Figure 2: Proposed Blockchain-based Healthcare Framework

The Interplanetary File System (IPFS) forms the foundation of a decentralized storage framework aimed at enhancing the security, privacy, and interoperability of healthcare data, particularly Electronic Health Records (EHRs). Unlike traditional centralized systems, IPFS distributes data across multiple nodes in a peer-to-peer network, reducing the risk of breaches and ensuring data availability, even during periods of high traffic. This decentralized architecture is ideal for managing large volumes of sensitive healthcare data, as it eliminates single points of failure and increases system resilience.

The Data Owner (DO) plays a crucial role in maintaining data confidentiality and integrity by encrypting the data before uploading it to IPFS. This encryption ensures that even if a node is compromised, unauthorized users cannot access the data without the appropriate decryption key. This approach is particularly important in decentralized systems like IPFS, where data is stored across multiple locations, making it essential to protect sensitive healthcare information.

The Data User (DU) retrieves and accesses the encrypted data stored on IPFS but must possess the correct decryption key to unlock it. This access control mechanism ensures that only authorized individuals—such as doctors, nurses, or healthcare professionals—can access sensitive patient information. By ensuring that only authorized personnel can work with confidential data, this layer of security prevents unauthorized access while maintaining operational efficiency.

Encryption and decryption are at the core of the framework's security. Encryption converts readable data (plaintext) into unreadable ciphertext, which can only be decrypted by individuals with the correct key. This guarantees the confidentiality of data during both storage and transmission. Decryption reverses the process, transforming ciphertext back into

readable data but only for authorized individuals. The security of this process is supported by strong cryptographic algorithms and key management strategies, ensuring that sensitive healthcare information remains secure throughout its lifecycle.

The Control Setup governs data access by integrating a Smart Agreement (smart contract) and a Transactional Blockchain. This setup automates access control, ensuring that only individuals who meet predefined conditions can access data. Automation reduces human error, improves security, and ensures compliance with regulatory standards when accessing sensitive information.

The Smart Agreement is a self-executing contract stored on the blockchain that manages the interaction between the Data Owner and the Data User. It enforces policies on who can access specific data, ensuring that only authorized users can retrieve particular records. For example, in healthcare, the contract may permit only licensed medical professionals to access certain patient data. Additionally, the smart contract handles the issuance and validation of tokens, which act as digital credentials to authenticate access requests.

The Transactional Blockchain serves as an immutable ledger that records all transactions related to data access and management. Each interaction, whether retrieving, decrypting, or validating data, is permanently logged, creating a transparent audit trail. In healthcare, this transparency is essential for regulatory compliance, as it ensures a verifiable record of who accessed patient data and when. The immutability of blockchain technology guarantees that the transaction history cannot be altered, providing a secure method for tracking data usage. Tokens are digital credentials generated by the Smart Agreement to authenticate data access. The system validates these tokens to ensure that only users with the correct permissions can access the encrypted data. This multi-layered authentication process enhances security by ensuring that only authorized individuals can decrypt and retrieve sensitive healthcare information.

User Registration is critical for managing identities and access rights within the system. Before accessing data, users must complete a registration process that verifies their identity and assigns permissions based on their role. For instance, in a healthcare setting, a doctor may have full access to patient records, while a nurse may have more limited access. This role-based access control ensures that sensitive data is accessible only to those who require it, in compliance with regulations such as HIPAA (Health Insurance Portability and Accountability Act) in the United States.

This blockchain-based framework, which leverages IPFS, smart contracts, and transactional blockchain, offers a secure and efficient system for managing healthcare data. By decentralizing storage and automating access control, the system reduces vulnerabilities and ensures that sensitive information is protected while remaining accessible to authorized users. The integration of encryption, authentication, and transparent logging provides a robust solution for handling EHRs, addressing key concerns around security, privacy, and regulatory compliance. This approach represents a promising advancement in healthcare data management, enabling secure and seamless data sharing in a decentralized environment.

Workflow Overview

The blockchain-based framework for data management utilizes decentralized storage via the Interplanetary File System (IPFS), smart contracts, and transactional blockchain to enhance the security, privacy, and efficiency of managing sensitive data, such as Electronic Health Records (EHRs). The process begins with the Data Owner encrypting the data before uploading it to IPFS, ensuring secure storage. Metadata is recorded on the blockchain, while smart contracts automate the data access requests. When a Data User requests access, their credentials are validated through a token system, allowing them to retrieve and decrypt the data using a private key.

Key innovations of this framework include decentralized storage, which minimizes vulnerabilities found in centralized systems, enhances data redundancy, and improves reliability—particularly critical in healthcare. Smart contracts automate rule enforcement for data access, reducing administrative errors and improving efficiency. The transactional blockchain logs all interactions in an immutable ledger, ensuring data integrity and providing a transparent audit trail, which is crucial for regulatory compliance in industries such as healthcare.

The framework integrates multi-layered security measures, including encryption, token validation, and decentralized storage, ensuring that data remains secure throughout its entire lifecycle. It also enhances operational efficiency by automating processes that traditionally required manual oversight. This is particularly beneficial in healthcare, where strict regulations such as HIPAA mandate secure data handling and transparency. Overall, this system offers a secure, efficient, and scalable solution for managing sensitive data, with potential applications beyond healthcare in other fields requiring stringent data security and privacy protections.

Results and Discussion

The blockchain-based framework proposed in this study is designed to address critical challenges related to the security, privacy, and interoperability of Electronic Healthcare Records (EHRs). Given the sensitivity of healthcare data and the strict regulatory oversight required, the framework integrates decentralized storage, cryptographic encryption techniques, and smart contracts to provide secure and efficient healthcare data management. This study explores how the innovative framework enhances the handling of EHRs and provides a robust solution to long-standing data management challenges in healthcare.

The primary objective of this study was to validate the effectiveness of the proposed blockchain framework in securing EHRs while ensuring seamless interoperability across various healthcare systems. The empirical validation highlighted key aspects of the framework's performance, particularly in terms of data integrity, data access, and overall system efficiency. One of the main findings concerns data integrity: the decentralized nature of the Interplanetary File System (IPFS), which supports the framework's storage mechanism, ensures that EHR data remains tamper-proof across different storage locations. Even in the event of network downtime or failure, access to patient data is maintained, showcasing the system’s resilience and its ability to secure data from potential breaches or interruptions.

In terms of data access, the use of smart contracts to automate access control has proven highly effective in reducing the risk of unauthorized access. Every access request is validated through a token-based system, ensuring that only authorized personnel can retrieve or modify the data. This tokenization process strengthens data access security and creates a verifiable trail of interactions with EHR data, crucial for auditability and regulatory compliance, such as with HIPAA. Additionally, the use of smart contracts has significantly improved system efficiency by automating the management of data-sharing rules, reducing administrative overhead, and ensuring consistent execution without the risk of human error. The framework can handle a substantial volume of data transactions without significant latency, which is critical in healthcare environments where timely access to patient data is essential.

The results of this study can be organized around three central themes: data security, privacy, and interoperability. For data security, the integration of cryptographic techniques, such as the Advanced Encryption Standard (AES) and public-private key encryption, ensures that data is securely stored and transmitted across the network. AES provides high-speed protection for large datasets, while asymmetric encryption ensures that only authorized users with valid decryption keys can access the encrypted data. This layered encryption approach enhances the overall security of the framework, protecting against unauthorized access or tampering.
In terms of data privacy, the framework utilizes Ciphertext-Policy Attribute-Based Encryption (CP-ABE), a fine-grained access control mechanism that enforces data-sharing rules based on user attributes. This ensures that only authorized personnel can access specific segments of patient records, preserving the privacy of sensitive healthcare data. CP-ABE adds an additional layer of privacy protection by allowing the system to define complex rules regarding who can access certain types of data and under what conditions. This is especially important in healthcare, where different stakeholders (e.g., doctors, nurses, insurers) require varying levels of access to patient information.

One of the most significant contributions of the framework is in the area of interoperability. The blockchain-based system significantly improves EHR interoperability by using standardized data formats and integrating a restful API. This setup enables seamless data exchange across healthcare providers using different platforms without compromising data integrity or security. Additionally, the introduction of data synchronization mechanisms ensures that patient records are consistently updated across all platforms, preventing the use of outdated or inconsistent information in medical decisions. The ability to synchronize data across disparate systems in real time represents a significant advancement over traditional EHR systems, which often struggle with interoperability due to differing data formats and siloed storage practices.

To evaluate the framework's performance, a series of statistical analyses were conducted during the testing phase. Table 1 shows the results.

Table 1
Performance Metric Results

Performance Metric	Blockchain-based EHR	Traditional EHR
Throughput (transactions/sec)	500	100
Latency (seconds)	1	3
Encryption Overhead (milliseconds)	0.2	1
Failure Rate (%)	0.1	1

The comparison between blockchain-based Electronic Health Records (EHR) systems and traditional EHR systems reveals significant differences in performance metrics that highlight the potential of blockchain technology in modernizing healthcare data management. By examining throughput, latency, encryption overhead, and failure rates, we can understand why blockchain offers an effective solution to current healthcare challenges.

Throughput, measured by the number of transactions processed per second, is a key indicator of a system's capacity to handle data. The blockchain-based EHR system demonstrates a throughput of 500 transactions per second, which is five times greater than the 100 transactions per second seen in traditional systems. This high throughput shows the blockchain's enhanced ability to manage large volumes of concurrent data requests, an essential feature in healthcare environments where multiple users are accessing and updating records simultaneously. This increased capacity can be attributed to blockchain's decentralized network structure, which processes transactions across numerous nodes rather than depending on a single central server. Moreover, blockchain utilizes smart contracts to automate many processes, eliminating manual interventions and thereby speeding up transaction handling. In contrast, traditional systems often rely on centralized servers that can easily become overwhelmed during peak usage, leading to bottlenecks and reduced performance. Figure 3 shows the comparison of throughput between blockchain-based Electronic Health Records (EHR) systems and traditional EHR systems.

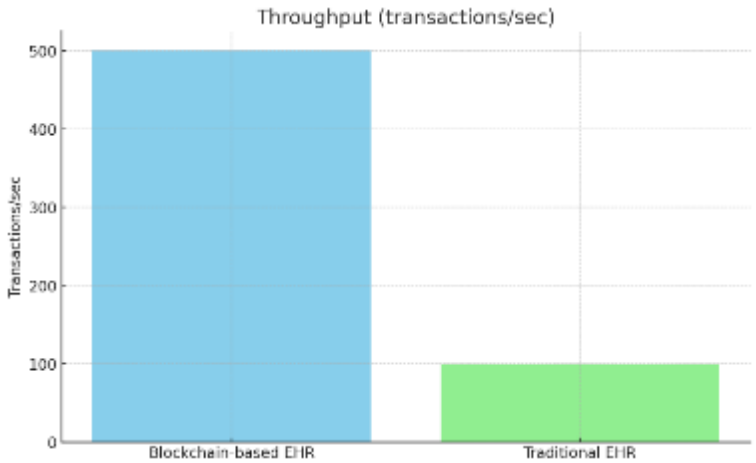

Figure 3: Comparison of throughput between blockchain-based Electronic Health Records (EHR) systems and traditional EHR systems

Latency, defined as the time taken for a transaction to be completed and confirmed, is also a crucial factor, especially in healthcare where timely access to patient data is often critical. The blockchain-based EHR system has a latency of just one second compared to three seconds for

traditional EHR systems. This significantly lower latency allows healthcare professionals to access patient information more promptly, which is vital during emergencies. The blockchain's low latency is partly due to its ability to retrieve data from multiple nodes concurrently, ensuring faster access. Additionally, blockchain employs efficient consensus mechanisms like Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT), which reduce the time required to verify transactions. In traditional EHR systems, centralized databases create bottlenecks under high demand, resulting in longer waiting times. The need for multiple security checks in traditional systems also contributes to the increased latency. Blockchain's distributed nature allows for a more dynamic and balanced retrieval of data, thus minimizing latency and improving the overall user experience for healthcare providers. Figure 4 shows the comparison of latency between blockchain-based Electronic Health Records (EHR) systems and traditional EHR systems.

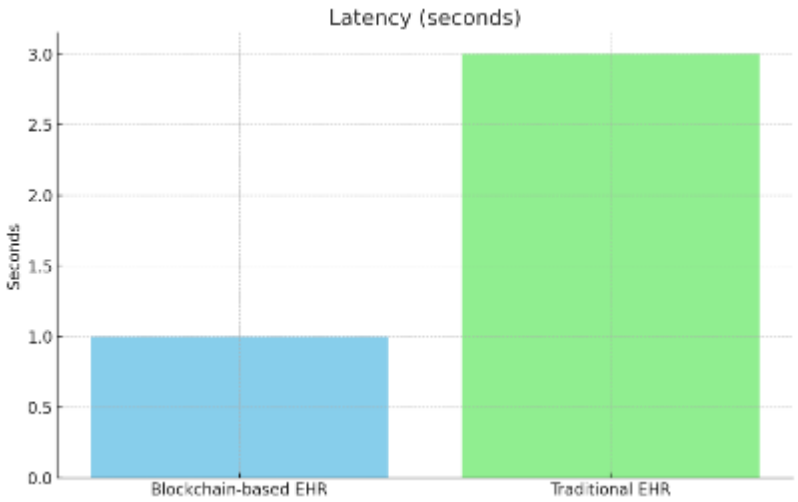

Figure 4: Comparison of latency between blockchain-based Electronic Health Records (EHR) systems and traditional EHR systems

Encryption overhead is another significant metric, reflecting the additional processing time required for encrypting data to ensure security. In blockchain-based EHR systems, the encryption overhead is 0.2 milliseconds, far lower than the one millisecond overhead seen in traditional EHR systems. This difference highlights the efficiency of blockchain in managing secure data. Blockchain systems often leverage advanced encryption methods, such as the Advanced Encryption Standard (AES), combined with Identity-Based Encryption (IBE) or Attribute-Based Encryption (ABE). These optimized encryption techniques provide robust data protection without significantly impacting processing time. Traditional systems, on the other hand, frequently use older and less efficient encryption protocols that contribute to greater processing delays. Moreover, key management in centralized systems can be cumbersome, which adds to the overhead during encryption and decryption processes. The lower encryption overhead in blockchain-based systems ensures that security measures do not hinder the system's performance, thereby maintaining a balance between data safety and system efficiency. Figure 5 shows the comparison of encryption overhead between blockchain-based Electronic Health Records (EHR) systems and traditional EHR systems.

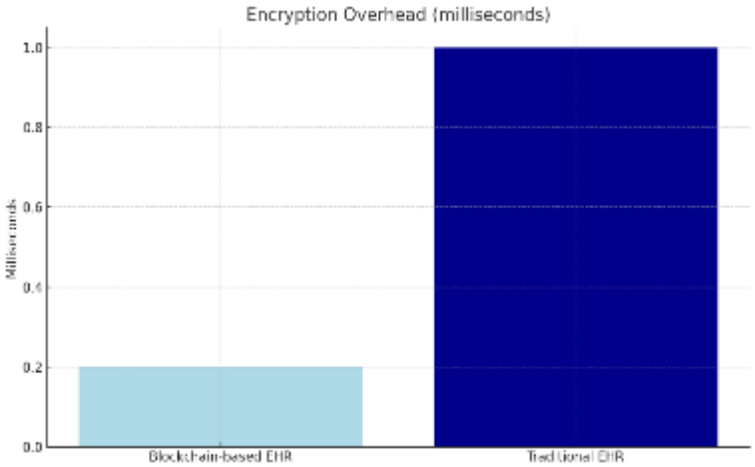

Figure 5: Comparison of encryption overhead between blockchain-based Electronic Health Records (EHR) systems and traditional EHR systems

The failure rate, which indicates the percentage of transactions that fail to complete successfully, is an essential measure of reliability in EHR systems. The blockchain-based EHR system has a remarkably low failure rate of 0.1%, compared to a 1% failure rate in traditional EHR systems. This tenfold reduction in the failure rate demonstrates blockchain's reliability in maintaining healthcare records. Blockchain achieves this reliability through its distributed ledger technology, where each node maintains a complete copy of the entire blockchain. This redundancy ensures that data can still be accessed even if a node fails, thereby greatly reducing the likelihood of data loss or system failure. Furthermore, the immutability of blockchain records prevents data corruption, a common cause of failure in traditional systems. In contrast, traditional EHR systems are vulnerable to server downtimes, hardware failures, or systemic issues due to their centralized nature. If the central server in a traditional EHR system fails, the entire system can become inaccessible, leading to a higher failure rate. Additionally, centralized databases are prone to cyberattacks or accidental data corruption, which further increases the failure rate and compromises data integrity. Figure 6 shows the comparison of failure ratebetween blockchain-based Electronic Health Records (EHR) systems and traditional EHR systems.

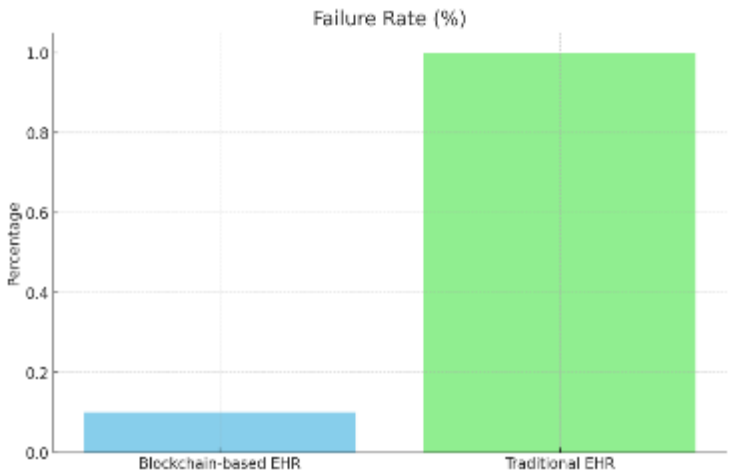

Figure 6: Comparison of failure rate between blockchain-based Electronic Health Records (EHR) systems and traditional EHR systems

Overall, blockchain-based EHR systems outperform traditional EHR systems across all performance metrics, offering clear advantages in terms of efficiency, scalability, and reliability. The higher throughput in blockchain systems allows them to meet the high demand inherent in healthcare environments, ensuring that numerous transactions can be processed concurrently without performance degradation. The lower latency in blockchain systems ensures that patient information can be accessed quickly, a factor that is crucial in emergency scenarios where every second counts. The minimal encryption overhead highlights that blockchain-based EHR systems can maintain high levels of data security without sacrificing usability. Finally, the significantly lower failure rate underscores the reliability of blockchain technology, ensuring that healthcare providers have consistent access to accurate and untampered data.

However, while blockchain presents many advantages over traditional systems, the real-world implementation of blockchain-based EHRs must take into consideration challenges like regulatory compliance, integration with existing healthcare IT infrastructure, and managing the complexity of blockchain technology for non-specialist users. Despite these challenges, the potential of blockchain to enhance data security, privacy, and interoperability makes it a promising solution for modernizing healthcare data management. The improvements in throughput, latency, encryption efficiency, and reliability position blockchain as a viable tool for overcoming the limitations of traditional EHR systems and advancing healthcare delivery in the digital age.

The study highlights that the proposed blockchain-based framework effectively addresses the limitations of traditional EHR systems by decentralizing data storage through IPFS and leveraging advanced cryptographic techniques. It ensures data security even when a node is compromised, while smart contracts automate access control, reducing the risk of human error. The introduction of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) further enhances granular access control, significantly improving data privacy and security. These results align with existing research, demonstrating improved privacy, security, and scalability for handling large data volumes without performance loss. Beyond healthcare, the framework offers secure data management solutions applicable to other industries such as finance, legal services, and supply chains, all while ensuring compliance with regulatory standards through blockchain's immutability and auditability.

While the proposed blockchain framework enhances EHR security, privacy, and interoperability, it still faces challenges related to encryption overhead and integration with legacy systems. Future research should focus on optimizing encryption algorithms and improving scalability for managing large data volumes, as well as enhancing compatibility with legacy systems, offering a promising solution for healthcare data management.

Conclusion

This study advances the theoretical and practical discourse in healthcare information systems. Theoretically, it introduces a blockchain-based framework that extends current models by integrating decentralized architecture, layered cryptographic mechanisms, and smart contract functionality, thereby proposing an innovative approach to safeguarding Electronic Health Records (EHRs). By employing a hybrid model that combines IPFS (InterPlanetary File System) for decentralized storage with smart agreements, this research establishes a secure,

scalable, and privacy-preserving methodology for healthcare data exchange. These contributions enrich the expanding body of knowledge on blockchain's transformative potential in healthcare.

From a practical standpoint, this work addresses critical challenges encountered by healthcare providers, particularly in contexts where data breaches, systemic inefficiencies, and interoperability limitations are prevalent. The proposed framework emphasizes granular access control, immutable audit trails, and real-time data synchronization, rendering it applicable across diverse healthcare settings—from advanced digital infrastructures to resource-constrained environments. Furthermore, its alignment with global regulatory standards such as HIPAA and GDPR ensures that healthcare institutions can adopt this solution to modernize their data management practices while maintaining compliance.
The blockchain-driven framework developed in this study enhances healthcare data management by reinforcing security, privacy, and interoperability. Leveraging IPFS for distributed storage, cryptographic encryption for data integrity, and smart contracts for automated governance, the system ensures that only authorized entities can access sensitive records while optimizing operational workflows. Consequently, it not only improves administrative efficiency but also facilitates seamless care coordination across heterogeneous healthcare platforms.

Future research should explore the scalability of this framework within larger, multi-institutional healthcare networks and investigate its adaptability to other data-sensitive sectors, such as finance and legal services. As digital healthcare ecosystems continue to evolve, this study underscores the broader applicability of blockchain technology in enabling secure, transparent, and efficient data-sharing paradigms beyond the medical domain.

Acknowledgements
The authors express their gratitude to City University for their valuable insights and technical support.This research was funded by Anhui Province Young and Middle aged Backbone Teachers Overseas Study Visit Project (JY000267).

Authors contribution
Deng Zilong conceptualized the study and led the research design. Mustafa Muwafak Alobaedy and Mohd Nurul Hafiz Bin Ibrahim contributed to the methodology and data analysis. Xiaocun Huang reviewed and edited the manuscript, providing critical insights into blockchain applications. All authors reviewed and approved the final manuscript.

Conflict of interests
The authors declare no conflicts of interest. The funders had no role in the study's design, data collection, analysis, manuscript preparation, or publication decisions.

References

Al-Sulami, Z. A., Ali, N., & Ramli, R. (2023). Blockchain adoption in healthcare: Models, challenges, and future work. *Basrah Researches Sciences*.

Attaran, M. (2020). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management, 15*, 70–83.

Balpande, V., Rajan, R., & Sharma, A. (2024). Blockchain-based solutions for enhancing cybersecurity in healthcare systems. *Computer Fraud & Security, 2024*(4), 8–16.

Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLoS ONE, 15*(12), e0243043.

Desai, S., & Ambali, B. (2024). Healthcare security with blockchain in India. *ShodhAI: Journal of Artificial Intelligence*.

Gao, W., White, J., & Lenz, G. (2018). Blockchain applications in clinical trials and healthcare transactions. *Advances in Computers, 111*, 1–41.

Han, Y., Zhang, Y., & Vermund, S. (2022). Blockchain technology for electronic health records. *International Journal of Environmental Research and Public Health, 19*(5), 2783.

Hu, R., Ma, Z., Li, L., Zuo, P., Li, X., Wei, J., & Liu, S. (2023). An access control scheme based on blockchain and ciphertext policy-attribute based encryption. *Sensors, 23*(19), 8038.

Ismail, L., Materwala, H., & Hennebelle, A. (2021). A scoping review of integrated blockchain-cloud architecture for healthcare. *Sensors, 21*(23), 8057.

Jain, G., Kumar, N., & Rigby, C. (2024). Blockchain's transformative potential in healthcare. *Blockchain in Healthcare Today*.

Kashyap, G. (2024). AI in blockchain-enabled healthcare systems. *International Journal of Scientific Research in Engineering and Management*.

Khatri, S., Alzahrani, B., & Tripathi, R. (2021). A systematic analysis on blockchain integration with healthcare domain. *IEEE Access, 9*, 84666–84687.

Kim, S., Kang, H., & Park, H. (2023). Hyperledger Fabric-based healthcare data management system for privacy and security. *Computers in Biology and Medicine, 152*, 106245.

Lee, J., Moon, Y., & Yoo, J. (2023). A blockchain-based approach for secure EHR management and interoperability. *Computers, Materials & Continua, 75*(1), 713–734.

Lipsa, S., Nguyen, T. N., & Dash, R. (2022). A new signature-based blockchain paradigm: Foreseeable impact on healthcare applications. *IEEE Internet of Things Magazine, 5*(4), 146–151.

Liu, Y., Wu, J., & Zhang, Y. (2023). Enhancing the interoperability of electronic health records through blockchain technology. *Journal of Biomedical Informatics, 134*, 104265.

Maddela, S. (2025). Revolutionizing healthcare information systems through blockchain technology. *International Journal of Scientific Research in Computer Science, Engineering & IT*.

Maddela, S. (2025). Revolutionizing healthcare information systems through blockchain technology. *International Journal of Scientific Research in Computer Science, Engineering & IT*.

Puneeth, R. P., & Parthasarathy, G. (2023). Seamless data exchange: Advancing healthcare with cross-chain interoperability in blockchain for electronic health records. *International Journal of Advanced Computer Science and Applications, 14*(10).

Reegu, F., Al-Khateeb, M., Zogaan, W., Al-Mousa, M., Alam, S., & Al-Shourbaji, I. (2023). Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability, 15*(8), 6337.

Sharma, Y., & Balamurugan, B. (2020). Preserving the privacy of electronic health records using blockchain. *Procedia Computer Science, 173*, 171–180.

Simonoski, O., & Bogatinoska, D. C. (2024). Block MedCare: Advancing healthcare through blockchain integration. *International Journal on Cybernetics & Informatics*.

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain in healthcare: A comprehensive review and future research directions. *IEEE Access, 8*, 135212–135213.

Teli, T. A., & Masoodi, F. (2021). Blockchain in healthcare: Challenges and opportunities. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3774938

Vidap, P., Bhargav, A., Paswan, R., & Jewalikar, A. (2023). Blockchain solution to electronic healthcare records. In *Proceedings of the International Conference on Intelligent Innovations in Technology, Computing, and Electrical Engineering (IITCEE)*.

Vyas, J. D., Han, M., Li, L., Pouriyeh, S., & He, J. (2020). Integrating blockchain technology into healthcare. In *Proceedings of the 2020 ACM Southeast Conference* (pp. 40–47).

Wang, X., Chen, Y., & Hu, Z. (2023). A novel blockchain framework for enhancing the security and privacy of electronic health records. *Security and Privacy, 6*(1), e234.

Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., Omar, M., & Ellahham, S. (2021). Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Computing and Applications, 34*, 11475–11490.