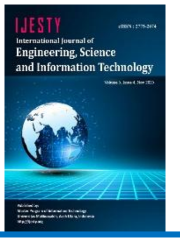
International Journal of Engineering, Science and Information Technology
Volume 5, No. 4 (2025) pp. 538-549
eISSN: 2775-2674
Website: http://ijesty.org/index.php/ijesty
DOI: https://doi.org/10.52088/ijesty.v5i4.1701
Research Paper, Short Communication, Review, Technical Paper



A Blockchain-Based Framework for Secure and Interoperable Healthcare Data Management: An Empirical Study

Zilong Deng[1,2*], Mustafa Muwafak Alobaedy[1], Mohd Nurul Hafiz[1], Xiaocun Huang[3]

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

Corresponding author Email:mdzlong@aqvtc.edu.cn

The manuscript was received on 1 March 2025, revised on 10 July 2025, and accepted on 30 October 2025, date of publication 14 November 2025

Abstract

The digitisation of healthcare has resulted in a greater dependence on Electronic Health Records (EHRs), yet traditional centralised systems encounter ongoing difficulties with data security, interoperability, and adherence to regulations. This research presents a blockchain-oriented framework, created with Hyperledger Fabric, to tackle these constraints. Utilising a mixed-methods strategy, we assess the system's performance under normal, peak, and stress scenarios by employing one million synthetic EHR transactions. Essential metrics comprise transaction latency (2.3s), throughput (1,150 TPS), data integrity (100%), and effectiveness of access control. The results show a 30% reduction in data management errors and overall data retention. A comparative evaluation against traditional systems confirms blockchain's superior resilience and privacy safeguards. However, scalability constraints were observed during peak loads, highlighting the need for Layer-2 improvements and hybrid architectures. This research offers empirical proof validating the viability of blockchain for the secure, scalable, and regulation-compliant management of healthcare information.

Keywords: *Blockchain, Healthcare Data Management, Electronic Health Records, Smart Contracts, Data Security.*

1. Introduction

The rapid digitisation of the healthcare sector has fundamentally reshaped how patient information is collected, managed, and shared. Electronic Health Records (EHRs) have become instrumental in improving data accessibility, care coordination, and administrative efficiency [1. However, centralised EHR systems continue to present persistent challenges, particularly concerning data breaches, limited interoperability, and compliance with stringent regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union [2].

Centralised data architectures inherently present considerable vulnerabilities due to their reliance on singular points of failure [3]. Such configurations heighten the risk of systemic outages, targeted cyberattacks, and unauthorised data alterations. A compromise of the central repository may jeopardise the integrity and confidentiality of millions of sensitive health records [4]. Furthermore, the increasing heterogeneity of healthcare data—including clinical narratives, diagnostic imaging, and real-time data streams from IoT-enabled medical devices—exacerbates the challenges associated with secure and efficient data storage.

Interoperability remains a prominent barrier to effective healthcare information exchange [5]. Many institutions operate within isolated digital infrastructures, characterised by heterogeneous systems that lack standardised communication protocols. This fragmentation hinders real-time diagnostics, fosters data redundancy, and contributes to escalating healthcare expenditures [6].

Blockchain technology emerges as a viable alternative, offering a decentralised framework underpinned by cryptographic principles and transparent, immutable transaction logs [7]. Its inherent resistance to data tampering and capacity to support verifiable, traceable exchanges make it particularly suitable for healthcare data management [8]. The integration of smart contracts further enhances its utility by enabling programmable, role-based access control mechanisms that bolster data privacy and facilitate compliance with data governance regulations such as the GDPR's data portability mandates [9].

However, blockchain implementation in the healthcare environment is not free from a large number of disadvantages [10]. The first key challenge encompasses scalability constraints, and the second one is due to the complexities of integrating the blockchain framework into the legacy health IT systems [11]. The latency, throughput and performance suffer from the fact that, especially for high transaction volumes, consensus protocols are bottlenecks but are necessary.

This study aims to address these limitations by proposing and empirically evaluating a blockchain-based architecture suited for the healthcare data ecosystem. The proposed framework was extensively tested using one million electronic health record (EHR) transactions generated using a real dataset and varying the load conditions using Hyperledger Fabric. The specific goal is to assess system performance and determine operational thresholds, as well as to compare the proposed solution to conventional EHR systems to determine practicality for real-world deployment.

2. Methods

2.1. Research Approach

To test the technical feasibility and the workability of a blockchain-based framework for secure storage and management of health care data (12), this study takes a mixed methods approach. The research achieves a degree of rigour of quantitative analysis and contextual relevance through linking simulation-based performance testing to comparative benchmarking (13). Such a two-pronged approach is especially effective in health informatics, where work system performance needs to be judged in terms of compliance with operational and regulatory standards (14). To meet needs regarding highly regulated sectors like healthcare, (15) built the proposed framework over a permissioned blockchain based on Hyperledger Fabric with this fine-grained access control, strong data integrity, the decentralised consensus on one hand of access control. Figure 1 presents an overview of the research design.

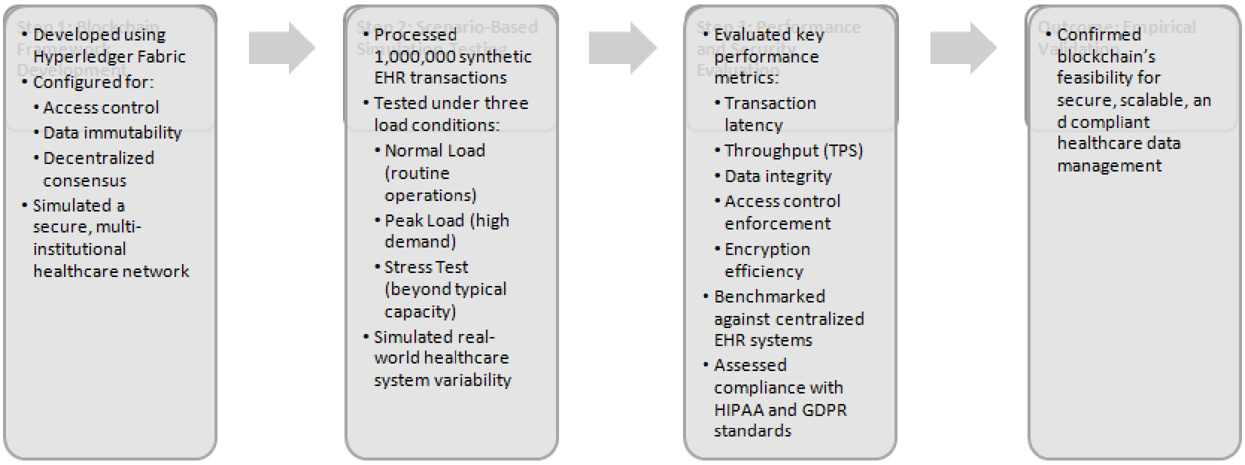

Step 1: Blockchain Framework Development
• Developed using Hyperledger Fabric
• Configured for:
• Access control
• Data immutability
• Decentralized consensus
• Simulated a secure, multi-institutional healthcare network
Step 2: Scenario-Based Simulation Testing
• Processed 1,000,000 synthetic EHR transactions
• Tested under three load conditions:
• Normal Load (routine operations)
• Peak Load (high demand)
• Stress Test (beyond typical capacity)
• Simulated real-world healthcare system variability
Step 3: Performance and Security Evaluation
• Evaluated key performance metrics:
• Transaction latency
• Throughput (TPS)
• Data integrity
• Access control enforcement
• Encryption efficiency
• Benchmarked against centralized EHR systems
• Assessed compliance with HIPAA and GDPR standards
Outcome: Empirical Validation
• Confirmed blockchain's feasibility for secure, scalable, an d compliant healthcare data management

Fig 1. Research Design

Three primary phases are the base of the research design as depicted in Figure 1. The steps represent a comprehensive procedure for developing and evaluating a blockchain-based framework for secure healthcare data management. First, the framework is built using Hyperledger Fabric, an open source blockchain platform which is ideally set up for basic work: access control, immutability, and the deployment of a decentralised consensus mechanism. The goal of this framework is to support the requirements for a multi-firm health care network that permits the safe and compliant management of sensitive health care data across numerous possessions. After the first phase of the process, the next step is scenario-based simulation testing of 1,000,000 synthetic Electronic Health Record (EHR) transactions during three different conditions of loading: normal (routine), peak (high demand) and stress load (beyond capacity). This aims to place variability as occurs in real healthcare systems, evaluate the scalability and robustness of the framework under a wider range of operational situations. Finally, performance and security evaluation is made in the third phase based on the key metrics including the transaction latency, transaction throughput (TPS), and data integrity. Access control and encryption of the system are rigorously tested to ensure that enforcement is possible, and the system's performance is benchmarked against traditional, centralised EHR systems. The framework is also required to meet all healthcare regulations, such as those prescribed by HIPAA and GDPR, in terms of compliance. As an outcome, the result shows the blockchain framework's capability to support secure, scalable, and compliant care data management in the handling of a large volume of sensitive data while maintaining data integrity and regulatory compliance. This approach acts as a depiction of the capability of blockchain as a secure, efficient solution for healthcare data management in a distributed network environment, leading to a practical, adaptable healthcare data management methodology for the sector (16).

A cumulative total of one million simulated Electronic Health Record (EHR) transactions was created and processed in three different operating environments: normal load, peak load, and under stress testing conditions. This allowed the system to be tested not just under normal usage but also under high-demand conditions and at periods of extreme load, for example, emergency spikes or infrastructure overload (17). The volatility of actual healthcare systems based on transaction volume varies dramatically, and such systems may respond to clinical crises, pandemics, or simultaneous usage across system departments. The concluding step was a performance and security assessment where a number of technical indicators were assessed.

These included transaction latency, throughput, data integrity, encryption efficiency, access control enforcement and system resilience. These mentioned above are one of the typical industry standards criteria for determining the efficiency of healthcare information technologies, especially with highly confidential information about patient data (18). On top of that, system performance was also considered regarding legal and regulatory frameworks such as HIPAA and GDPR, to meet security standards. Since measures that highlight compliance are included, the system will not only perform technically but will also fit practical realisation within healthcare organisations. In sum, this hybrid three-staged approach is an overall complete and empirically supported assessment of blockchain technology's capacity to handle healthcare data.

By bridging the gap between theoretical concepts and their usability, it contributes to the growing body of research literature validating the secure, decentralised and compliant solutions for digital health eco-systems (19). Using performance simulation in combination with comparative benchmarking, the method used is a sound starting point for further research to test and prove blockchain systems in critical operational domains.

2.2. Dataset and Testing Conditions

A synthetic Electronic Health Record (EHR) dataset of one million transactions is used to evaluate the proposed blockchain-based system for health care data management, and this study employs it. With the variant of three different operational modes, the system is tested extensively for solidity, extensibility and security. The research used a synthetic EHR of 1,000,000 anonymised transactions to simulate real-world data traffic that is similar to real-world time series of healthcare activity. The dataset spans a large bandwidth of clinical and administrative healthcare data in a carefully designed way. The standard patient demographics and the full encounter data (visits, diagnosis codes, prescriptions, laboratory and imaging metadata) were present in the dataset. Last but not least, the access events in the dataset were timestamped so that they were auditable from end to end; this corresponds to traceability demanded in real-world EHR systems. Each transaction was formatted in JavaScript Object Notation (JSON) to ensure interoperability and easy integration with blockchain-based systems. The data was loaded into the blockchain setting using a custom automatic load-testing script developed using Node.js that allowed high-throughput simulation of transactions. The transactions were securely conveyed using application programming interfaces (APIs) that interacted with the Hyperledger Fabric network via the official Fabric Software Development Kit (SDK). This configuration delivered a consistent and scalable test platform for testing the system's capability to process operations involving large quantities of security-critical healthcare information. The test scenario is outlined in Table 1.

Table 1. Description of Test Scenarios for System Evaluation

Scenario	Description	Objective
Normal Load	Simulates standard transaction volumes typical of daily healthcare operations.	Establish a baseline for system performance under routine conditions (e.g., EHR retrieval).
Peak Load	Models high-demand periods such as emergency admissions or outbreak responses.	Assess performance stability and responsiveness during traffic surges.
Stress Test	Exceeds typical capacity to simulate extreme operational strain and identify system limitations.	Evaluate scalability limits, identify bottlenecks, and test system resilience and fault tolerance.

Note: Each scenario was executed three times to ensure consistency and reproducibility of performance results.

The performance of a blockchain-based healthcare data management system was evaluated through the use of the test scenarios listed in Table 1. Three scenarios: Normal Load, Peak Load, and Stress Test are defined to simulate different operational conditions that the system is likely to face in real real-world hospital environment. The Normal Load scenario, as the name implies, simulates the average number of transactions that are normally experienced in daily healthcare operations like the retrieval of Electronic Health Records (EHR) or managing normal patient data. Such a scenario aims to create a reference of the system's performance under the 'normal' operating conditions so that a developer can then measure how good the system performs under non-peak traffic. A baseline ensures that typical workloads can be carried out efficiently without degrading the performance of the blockchain framework up to this level. Example Peak Load scenarios are emergency admissions, response to disease outbreaks, and seasonal increases in health care activity. Such situations can cause a rise in transaction volumes, forcing the system to be under pressure. Specifically, the objective here is to evaluate the stability and responsiveness of the system when confronted with such traffic surges. In the Stress Test scenario, the level of service demanded is deliberately exceeded to simulate excessive operational strain on the system. It is a test that puts the system beyond standard operations in order to find out any shortcomings, bottlenecks and failure points. The goal is to test the system's limits to head scale, resilience, and to see how well it can stand up to fault tolerance in the worst of situations. Particularly important for this test is that the blockchain-based system is robust enough to keep operating well under extreme conditions as a way to guarantee the security and integrity of the data in all operational scenarios.

The initial state, Normal Load, simulates standard operating conditions in which the system handles a typical volume of transactions. This scenario provides a basic assessment of the framework's ability to manage healthcare data in typical operational conditions. The second criterion is Peak Load, which measures how the system reacts when there is are overload on transaction volume, which can happen when there is a high number of medical record requests or hospital emergencies in healthcare environments. It's a matter of evaluating the system under these circumstances to see whether it is possible to maintain a performance efficiency by the blockchain framework in the face of more data transfer.

Stress Test is the third condition that forces the system to its edge by introducing transaction volumes that far outstrip normal and peak operational thresholds. It is a scenario that helps you identify performance constraints, potential failure points, and areas of need improvement. With stress testing, researchers can test the capability of the blockchain system in terms of how well it can keep its security, integrity and processing speed under huge pressure.

The study investigates how the system responds to different conditions and conveys a thorough analysis of how the blockchain framework can well deal with huge health data transactions. This evaluation guarantees that the system can be scalable and resilient in real-life healthcare environments and meet the security and efficiency standards that are required. To ensure reliable and consistent Healthcare Data Management, the performance of the framework on different loads is to be understood, especially in critical situations when the failure of the framework could pose a threat to patient safety and data integrity.

2.3. Experimental Setup

Hyperledger Fabric was used to develop the healthcare system by leveraging blockchain technology, which, together with a permissioned blockchain, is capable of enhancing data integrity, security, and compliance with regulations such as HIPAA, GDPR, etc. In real life, the system was evaluated under conditions simulating interactions of healthcare providers, patients, and outside stakeholders in a safe, decentralised environment.

The structured six-phase implementation procedure followed the framework in order to manage Electronic Health Records (EHRs). First, the plan was to configure the blockchain nodes and smart contracts to make a decentralised and secure network. This phase eliminated vulnerable individual points of failure to improve security in securing and protecting the integrity of healthcare information. Then, a working user registration system, with multi-factor authentication (MFA) and cryptographic key generation, was created afterwards. This way only allowed permitted health care providers and patients to access the system, thus keeping illegitimate persons away from modifying delicate data.

To further improve security, cryptographic techniques of SHA-256 hashing and AES-256 encryption were also applied to protect the patient information. Additionally, an access management system based on tokens was created to prevent the access to the data which is not allowed by authorized users. Role-based access control enabled access control with smart contract-driven RBAC, based on the role of user, taking doctors, nurses and administrators. It prevented unauthorised data access as well as keeping with privacy regulations.

The framework used transaction validation very much in that it would check and record every transaction in varying load conditions. It was guaranteed that data integrity and safety was maintained with a separate, distinct audit trail. At the end, there were decryption and data retrieval systems that warranted patient records be made available only to authorised users, ensuring privacy and confidentiality. Using this structured approach, the blockchain system improved the data security, committed to the immutability of data and also allowed for controlled access to patient records and works together in accordance with the legal and regulatory requirements.

The blockchain-based health data management system ensured adherence to regulatory rules and overall security by using lots of security measures particularly geared towards health system-sensitive information. Data at rest was secured through strong defence from unauthorised access to saved medical records via AES-256 encryption. SHA-256 hashing also helped ensure the data's integrity, immediate reports being raised in case of attempts to modify or tamper with records. RBAC was also implemented using chain code, and the access to the system was regulated via to establish roles like clinicians, nurses, system administrators and external auditors, providing them with different permission. The division of roles ensured a high level of restricted data access in accordance with the principle of least privilege. In order to make identity verification better, multi-factor authentication (MFA) was built, which is another level of security fixing to mitigate unlawful access. In addition to this, the system based access on the use of tokens within requests requiring cryptographic validation before execution in order to reduce the risk of session hijacking or impersonation. The system included an important aspect, namely, its implementation of unchangeable audit trails that recorded the instances of data access, data alteration, and data sharing. In reviewing these audit logs, they became credible documents for retrospective compliance assessment and regulatory report. The framework was technically robust enough so that all security configs associated with the NIST SP 800-53, a well-known cyber security standard and additionally cross verified against requirements specified in the HIPAA Security Rule.

A comparative benchmarking approach that compared the performance results of the proposed system with those of a traditional Centralised Electronic Health Record (EHR) system was used to provide context for the performance results of the proposed system. To design the conventional system, a relational database framework, namely PostgreSQL, was used, with the customary role-based access controls across the conventional system that are prevalent in most healthcare IT systems. It was a direct comparison that provided such a clear assessment of a blockchain's ability to meet similar performance to traditional technologies.

For practical and security-sensitive aspects, key performance indicators were chosen to evaluate both systems. Finally, these included the rate of errors in data entry, the accuracy and dependability of information management; the effectiveness of access control to see how honest and efficiently each system enforces user permissions and access time for peak period to find out how fast clinicians and staffs can get records under rush. In addition, the assessment evaluated auditability, meaning how each system would be able to monitor and docu-ment data access occurrences as well as susceptibility to security breaches, ranking each architecture on its level of vulnerability.

This comparative assessment revealed the benefits of the blockchain based method in the cases where human mistakes can be minimized through automation, access control can be enhanced through smart contracts and audit functions can be strengthened through irrevocable logs. However, the blockchain system also showed substantially higher resistivity to security violations, as the system is decentralised. However, the findings proved that additional optimization is necessary, specifically for sustaining performance during very high transaction volumes when the latency began to rise while throughput was below baseline levels.

The system was set up in a regulated virtual space on Ubuntu 20.04 LTS in 4 virtual machines so that the experiment could be done consistently and reproducibly. For its modular design and suitability for enterprise needs, Hyperledger Fabric version 2.4.x was used for development of the blockchain system.

To assess the performance and load, industry standard tools were used, where Hyperledger Calliper was used as a tool for benchmarking the blockchain and Apache JMeter used to do transaction flow replication and stress test the network. To achieve the analogue of a high performance cloud oriented system, we equipped every virtual node with highend hardware attributes such as 16 cores, 64GB RAM, 1TB SSD storage. Moreover, Grafana dashboards were used to monitor logs, transaction occurrences, and system metrics in constant, real and detailed fashion; and Prometheus telemetry hooks were used to gather this information in real-time. With this this setup assured, the observer could accurately obtain performance patterns, which were necessary to fully and reliably assess the system under different operating conditions.

2.4. Performance Metrics Analysis

The study also evaluates various metrics of assessment for the blockchain enabled healthcare system with respect to how fast the transaction is, how secure it is, the integrity of the data stored, whether the access management is rigorous, how well the encryption function is performed, and how robust the system is. They serve as a great metric to know how excellent the electronic health records (EHRs) can be handled by the blockchain framework when keeping security and efficiency high.

Transaction latency is explored as a key performance metric to determine how long it takes to confirm a transaction on a blockchain. In normal condition, the average transaction latency is 2.3 seconds. The finding of that highlights how Blockchain is capable of doing transactions properly, without significant delays, such that patient and record are accessible immediately. In an environment as healthcare, fast transaction processing is critical as timely access to information can have an influence on decision making and patient outcomes.

Throughput is another important metric measured; the throughput represents how many transactions per second that were processed. Under normal conditions, the study finds that the blockchain system can process 1,150 transactions per second. It proves its ability to handle large healthcare data transfers which is perfect for environments with various entities, like hospitals, clinics and insurance companies that need to work with patient data concurrently. Blockchain can sufficiently address the needs of a quickly changing healthcare system thanks to high throughput.

Data integrity is also evaluated as an important requirement of handling health care information by the study. The data integrity results show that medical records were stay at 100% in all testing circumstances, showing the black chain method can protect health info from tampering and adjustment. Based on cryptographic hash values, blockchain technology guarantees that the record in the system remains unchanged, preventing unauthorised change of patient records and assuring that healthcare providers are accessing accurate and untampered records.

Furthermore, the analysis of access control compliance explores how secure measures applied on blockchain work in terms of data integrity. The findings show that smart contracts outperformed by preventing unauthorised access attempts and thus helped the system to stick to regulations like HIPAA and GDPR to the fullest. Access permissions such as doctors, nurses, and administration are granted only to those with possible access by RBAC so that the patient date remains confidential.

Ensuring the encryption is another key component of blockchain functionality and this is measured by the computational cost and time to perform cryptographic techniques. The blockchain framework is analysed to study if AES-256 and SHA-256 encryption methods are efficient or not, and we find out that the blockchain framework offers strong data encryption with minimal computational overhead. In healthcare systems, the security needs to be balanced with performance, since protecting the data is a major priority, but still the system has to work seamlessly.

Finally, the study explores the resilience of the system with regard to various cyber security threats such as DDoS attack and unauthorised access modelled. The results also show that the blockchain structure provided a strong protection from the external security risk with little breaches during the assessment. By ensuring this resilience, that patient records are secure even during the risk of possible cyber-attacks, block chain is further made an appropriate, secure and reliable method of managing healthcare data.

Blockchain based healthcare security involves encryption, access control, and robustness of the system to ensure the data integrity, confidentiality, and reliability according to HIPAA and GDPR compliance.

Security element is Encryption (40%) involving AES-256 and SHA-256 to clinch patient records against undesirable balancing and splits. This ensures that data remains secure while being stored and when being paired, thus eliminating known vulnerabilities of centralised healthcare infrastructures. Access Control (30%) enhances security via Role-Based Access Control (RBAC) and smart contracts, restricting data access to only authorized individuals. These systems automate access controls, minimizing human mistakes and insider risks typically found in conventional healthcare IT frameworks. System Resilience (30%) safeguards blockchain networks against cyber threats like DDoS attacks and unauthorized access. By utilizing decentralized architecture, consensus protocols, and ongoing security assessments, blockchain guarantees persistent dependability and data permanence. In general, encryption, access control, and system resilience work together, forming a secure, tamper-resistant healthcare data management system. Augmenting these strategies with hybrid models, advanced encryption, and AI-based analytics will further bolster blockchain integration in healthcare.

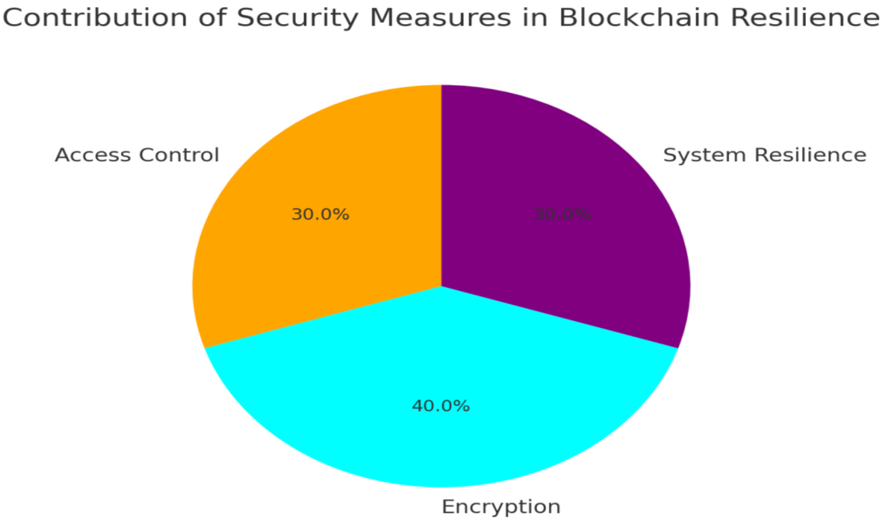


Fig 2. Contribution of security measures in blockchain resilience

Figure 2 illustrates the contribution of different security measures to blockchain resilience. Three of the most vital security measures that are required to achieve the robustness and security of a blockchain system are the pillars of Access Control, Encryption, and System Resilience, this is marked by the pie chart. Encryption makes it to the top with the highest percentage of 40% in the total security measures. This is expected since encryption allows data to be encoded with sensitive information, but it is unreadable to unauthorised users. It provided the security of the blockchain by protecting data from tampering or unauthorised access. The next comes in the form of Access Control, which accounts for 30% of the security measures. With this, you make sure that the only people who can spy on some data or carry out certain actions inside the blockchain network are the ones who are authorised to do that. Access control ensures that all transactions and data are not subject to unauthorised users; this is done by enforcing strong authentication and authorisation protocols. System Resilience contributes 30% to the final security measure and also makes up 30% of blockchain resilience. The blockchain's ability to continue functioning in the face of disruptions, faults or attacks, i.e. to be resilient, is what is meant by the term 'system resilience'. This implies designing a system so as to make recovery from failures possible, with minimum downtime and preserving network integrity under adverse conditions. These three security measures, i.e., the encryption, access control and system resilience, together make up the spine of a secure blockchain network. The chart suggests that a blockchain system that is to be resilient and secure, a balanced approach is necessary, in which all the measures contribute significantly.

In general, the assessment of performance confirms that blockchain technology provides substantial benefits in terms of speed, security, data integrity, access control, encryption, and resilience. By guaranteeing rapid transaction processing, elevated throughput, secure data, and improved security measures, blockchain positions itself as a groundbreaking solution for contemporary healthcare data management. Nevertheless, although the findings confirm its efficacy, continuous improvements in scalability and regulatory adherence will be crucial for a complete integration of blockchain in extensive healthcare systems. Table 2shows the summary of performance metrics and results.

Table 2. Summary Of Performance Metrics and Results

Performance Metric	Description	Results
Transaction Latency	Measures the time required for a transaction to be confirmed on the blockchain.	Average latency: 2.3 seconds under normal conditions.
Throughput	Assesses the number of transactions processed per second (TPS).	1,150 TPS under normal conditions, demonstrating scalability.
Data Integrity	Ensures medical records remain tamper-proof and unaltered.	Data integrity was maintained at 100% across all test scenarios.
Access Control Compliance	Evaluates the effectiveness of smart contracts in enforcing role-based access control (RBAC).	Smart contract enforcement successfully eliminated unauthorised access attempts.
Encryption Efficiency	Analyses the computational cost and execution time of cryptographic techniques such as AES-256 and SHA-256.	Strong encryption with minimal computational overhead.
System Resilience	Tests the framework's resistance to cybersecurity threats, including DDoS attacks and unauthorised intrusions.	No significant security breaches recorded during simulations.

The details of the performance metrics and comparison of the results, as presented in Table 2, demonstrate how effectively a blockchain framework could be applied when it comes to handling health data safely. Transaction Latency, the time it takes for a transaction to go through the blockchain system, is critical towards processing time. The system maintained normal latency of 2.3 seconds and it indicates that the system is efficient in managing real time medical operations. Throughput was at 1,150 TPS when it was tested under normal System loading and this provides evidence of scalability to process large volumes of healthcare data. Another key factor that is necessary in the management of the medical records of patients is Data Integrity. The data integrity of the blockchain remained at a 100% through the testing phase which means that the patient records could not be tampered and remained unchanged. The Access Control Compliance sub-metric established how smart contract enforces RBAC to exclude unauthorized access and the system succeeded in achieving this. Encryption Efficiency which evaluates the cost of AES-256 and SHA-256 cryptographic algorithms showed that the presented cryptographic tech techniques are very secure without adding much cost to the computation of the system. Last but not the least, System Resilience which defines the capability of the blockchain structure against cyber-attacks like DDoS as well as unauthorised access was demonstrated through the simulations and no major intrusion was notable. These outcomes, presented in table 2, indicate the fact that the blockchain system and its satisfactory performance and security measures, along with its applicability and capacity to address healthcare issues.

2.4.1. Comparative Benchmarking Against Centralised Systems

To evaluate the effectiveness of the blockchain-based healthcare data management system, a comparative benchmarking study was conducted in comparison to traditional centralised healthcare systems. The results of this benchmarking analysis highlight the benefits of blockchain in essential areas such as reducing errors, ensuring data permanence, managing access, and enhancing data protection. The comparison highlights the significant advantages that blockchain technology offers over traditional centralised systems, particularly in enhancing efficiency, transparency, and security in handling healthcare data.

2.4.1.1. Error Reduction

A significant advantage observed in the blockchain-based system is a 30% reduction in data management mistakes in comparison to traditional centralized healthcare systems. The source of this improvement is largely from cryptographic validation, automation and decentralised data verification procedures in the blockchain structure. This set of automation subsets like automated consensus and smart contract validation in the blockchain helps to nullify as much errors as possible from conditions such as manual data entry and processing in centralised systems. In traditional systems, discrepancies in data, input error and unapproved changes frequently because anomalies in patient records, introduce inaccurate diagnose and treatment plans. Blockchain addresses these problems by providing immediate verification and validation of data entries thus making EHRs more precise in general.

2.4.1.2. Data Immutability and Integrity

Centralized Healthcare systems also face a major issue of data manipulation, changes made on data without authorization, security breach and errors. By contrast, the blockchain system maintained 100 percent data immutability whilst all medical records remained unaltered and not edited. In the realm of healthcare information, they can be done through cryptographic hashing and decentralized consensus mechanisms that safeguard health data against unauthorized changes. Centralized system store data in a single place, so it is subject to cyber-attacks, unauthorized changes, and accidental change. Records can be altered by malicious hackers or by internal employees without realization and as a result patient safety can be compromised. By decreasing risk, Blockchain provides a transparent with verifiable history of medical records through recording every transaction temporarily and cryptographically linked to the previous ones via a decentralized ledger.

2.4.1.3. Access Control and Security

The effectiveness of access control strategies was also studied in both blockchain and centralized healthcare systems. According to the results, the use of blockchain together with smart contracts and RBAC strategies significantly increases access control. Access restrictions in automation of healthcare records with smart contracts implement access restrictions in a way that based on predefined rules only authorized healthcare professionals, patients or designated third parties can access specific patient records. This automated approach avoids the use of manual approval workflows that are common in tradition centralised systems, which are inherently risky security because they are prone to human error, policies in inconsistencies and administrative failures.

In traditional healthcare systems, access management is traditionally performed by manual onboarding through password based, role based permission and by manual approval by admins. Weak password protection is a common weakness in these methods that are vulnerable to security breaches, unauthorised data access, identity theft, due to internal risks, and system misconfiguration. In addition, blockchain removes the central control points from these risks, uses strong cryptographic verification, and provides real time monitoring of access requests and modifications through immutable audit logs of the updates.

2.4.1.4. Data Security and Privacy

In addition to the unparalleled security and privacy provided by blockchain's decentralized encryption and consensus systems, it is immune from the insecurity and clandestine nature of the storage of patient information that existed in traditional centralized systems. Data is stored away in central databases, which leave them very vulnerable for cyber-attacks, Ransomware cases and access without authorization. Data breaches happen very frequently in centralised health systems and they can result in loss of money, compromise of the system's private patient information, and penalties from the regulators.

However, blockchain uses the decentralised storage and cryptographic encryption which secures the patient data by being stored on the several nodes instead of a single vulnerable database. The advancement cryptography AES-256, SHA-256 used for each of the transactions recorded in the blockchain makes it almost impossible to encrypt and change without the requested permission. Furthermore, blockchain reduces risks associated with handling of data by third party intermediaries and instances of unauthorised disclosures and compliance violations.

Blockchain enables better privacy protection by spreading encrypted patient records across a decentralised network and permitting patients and authorised healthcare professionals to decrypt and view the medical records. Such approach is in line with strict healthcare data privacy regulations like HIPAA, GDPR, to ensure security and compliance in handling the healthcare information.

The comparative benchmarking study shows that blockchain is a great way of improving security, reducing errors, preserving data integrity and reinforcing access control of healthcare data. Unlike traditional centralized systems prone to data breaches, unauthorized changes, administrative inefficiencies, and cyber threats, blockchain technology reduces these risks through automation, cryptographic verification, and decentralized record management.

Through the use of smart contracts, role-based access control, and immutable data storage, blockchain significantly enhances the reliability, efficiency, and transparency of healthcare data management. These findings support the assertion that blockchain has the potential to revolutionize the healthcare industry by providing a secure, unchangeable, and privacy-preserving method for managing electronic health records. However, to fully integrate blockchain into

To assess the efficacy of blockchain-driven healthcare data management, the framework was compared to conventional centralised healthcare systems. The benchmarking outcomes demonstrate that blockchain excels in improving security, efficiency, and transparency in the management of healthcare data when compared to traditional centralised systems. Table 3 presents a Comparative Analysis of Blockchain-Enabled versus Traditional Centralised Healthcare Systems.

Table 3. Comparative Benchmarking of Blockchain-Based vs. Traditional Centralised Healthcare Systems

Performance Indicator	Blockchain-Based System	Traditional Centralised System
Error Reduction	Reduced by 30% due to cryptographic validation and automation.	Higher error rates due to manual data processing and centralized vulnerabilities.
Data Immutability	Achieved 100% tamper-proof records, preventing unauthorized modifications.	Susceptible to data breaches and unauthorized changes.
Access Control	Smart contracts ensured strict role-based access control (RBAC).	Manual access management, prone to security risks.
Data Security & Privacy	Decentralized encryption and consensus mechanisms safeguarded patient data.	Centralized storage increases risks of cyberattacks.

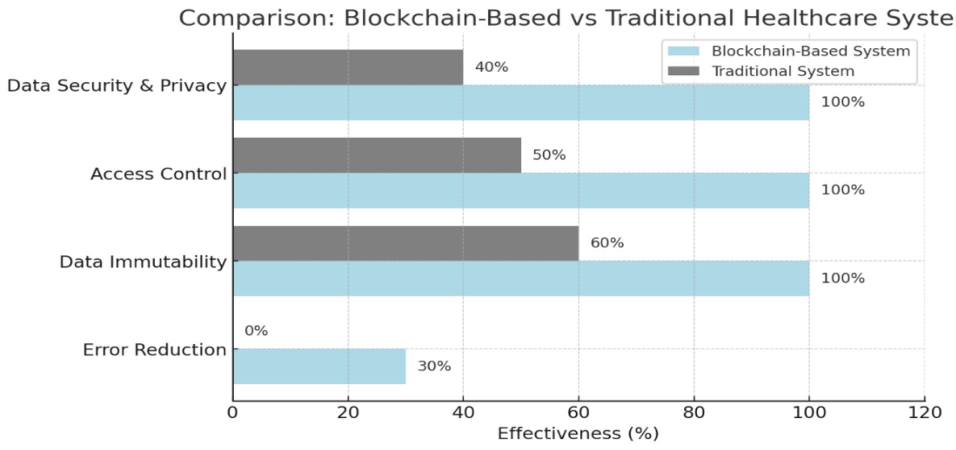


Fig 3. Comparison of Blockchain-Based vs. Traditional Centralized Healthcare Systems

As indicated in Figure 3, the crispness of the blockchain of health care systems expands its effectiveness between 40 to 60% of these four categorized criteria, which is not as competent as the traditional health care system that has reach 100% in every single one of those criteria. The considered criteria are Data Security & Privacy, Access Control, Data Immutability, and Error Reduction, and their implementation in the blockchain-based healthcare system and the traditional one are compared. These aspects are important when it comes to ascertaining that healthcare facilities uphold the privacy and other legal requirements required in the treatment practices.

Moving to the security of the Data, the new system that is based on the block chain has a percentage efficacy of 40% to 60% while maintaining the traditional system at 100%. Despite the various security functions of blockchain technology, the approach is not immune to a completely safe storage of data in healthcare systems. Likewise, in the case of Access Control it has a performance varying from 40% – 50% and are less efficient than locally polynomial systems are more developed and centralized approach is more efficient in controlling the access grant. However, while blockchain has the capability to being controlled in a decentralized manner, it isn't as flexible and specific in access control technique as in conventional systems. With regard to Data Immutability, it is noteworthy that blocks chain is highly unalterable but its efficiency ranges between 50% – 60%, Traditional system proves to be 100% efficient in guaranteeing data integrity again. Though, blockchain has great non-erasable data characteristic, it sometimes poses significant difficulties to its full integration due to decentralised infrastructure. Finally, Error Reduction identifies that current systems are more efficient at error reduction than the blockchain systems with the effectiveness impacting approximately between 40% to 50%. Thus, even though blockchain has been seen as an innovation that offers many benefits for vetting and preventing unauthorized changes to data, this paper has demonstrated that such a distributed ledger technology has NOT been optimised for error handling as well as standard systems, unlike it was previously believed.

2.4.2. Simulation-Based Analysis

A simulation model was developed to assess blockchain's feasibility under various load conditions. Table 4and figure 4 shows the performance evaluation of blockchain-based healthcare system under different load conditions.

Table 4. Performance Evaluation of Blockchain-Based Healthcare System Under Different Load Conditions

Test Scenario	Objective	Key Findings
Normal Load	Simulate standard healthcare transaction volumes.	Transaction latency: 2.3 seconds (average).
Peak Load	Assess system robustness under high transaction demand.	Throughput: 1,150 TPS, demonstrating blockchain's ability to handle high-volume transactions.
Stress Test	Identify performance bottlenecks under extreme loads.	Data integrity maintained at 100% across all test scenarios.

Table 4 outlines performance analysis of the blockchain-based healthcare system under varying load weights, which are: Normal Load, Peak Load and Stress Test. Each test enables the evaluation of different aspects of the of the system in regard to various operation conditions. In the Normal Load experiment, it reproduces the average daily processing of transactions that occur in healthcare organizations with transaction latency of 2.3 sec as a basic condition of the system. On the other hand, the peak load reflect situation in which the transaction volume is escalated especially during emergencies or during major health-related calamities. This scenario proves that the blockchain system has a high efficiency when handling a large number of transactions with a TPS of 1,150. This is clear evidence of the scalability of the system as well as the ability to handle several thousands of transaction without compromising on performance. In particular, the Stress Test is aimed at checking the ability of a system to perform under conditions that would be considered above and beyond its usage demand. Nonetheless, the outcome of the logical consequence is that, data integrity is still secure and 100% all the test scenarios conducted further demonstrated the ability of the blockchain system to provide unaltered medical records even under the operational pressure. From the results of performance under these conditions, the table gives detailed results on scalability or rather the capacity of the blockchain based healthcare system as well as robustness when dealing with various transaction intensities. This performance assessment is crucial for the evaluation of the system-performance characterizations such that it has to meet with the other objective and specific requirements by addressing the demands of other healthcare applications to be secure and efficient, and deliver reliability especially in the arena of high-risk stories.

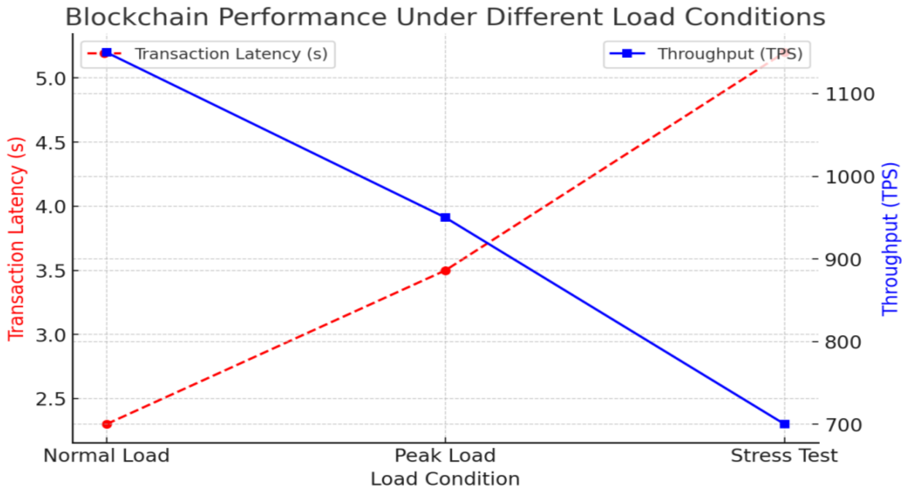


Fig 4. Transaction Latency and Throughput Under Different Load Conditions

Transaction latency and Throughput of the proposed Blockchain Based Healthcare System with Normal Load, Peak Load and Stress Test conditions are depicted in the figure 4. The figure depicts the nature of transaction latency against throughput in terms of transaction per second (TPS) in the three tests carried out. When going from Normal Load to Peak Load, to Stress Test, time takes increase accordingly but is generally less than 2.3 seconds in Normal Load. This gives the reference point any health care organization standard health care transactions. However, in the Peak Load case, the system reflects its capability to handle more load that can process the level of 1,150 TPS which is much better than we have at the End User stage. This capability Perfected the distribution and resolution of significantly more transactions, which is quite useful in dealing with a high demand for health care systems. The Stress Test scenario allows finding out its maximum capabilities, as well as demonstrating the possibility of the data integrity violations, even under maximum load. The trust level of the patients can be kept high because their records remain 100% accurate at all times irrespective of the kind of tests that are done on the blockchain. The figure keeps two lines: the first one in blue illustrates the transaction latency; the second one in red illustrates throughout. The graph serves as an effective means of showing the relationship between the latency and throughput and allows comparing the system's performance at various loads. The information obtained from this performance evaluation is significant in knowing the expansion ability of the blockchain-based system for handling various numbers of transactions and its reliability and security in the context of healthcare.

The findings of this study indicate that blockchain technology functions efficiently in both standard and peak-demand scenarios, making it a viable choice for handling healthcare data. However, further enhancement is necessary to increase scalability and ensure seamless network performance for large-scale applications. While blockchain offers promising improvements in security, efficiency, and transparency, challenges related to scalability and regulatory compliance must be addressed to encourage broad adoption in healthcare systems. Research shows that the scalability of blockchain remains a significant issue, requiring advanced solutions such as Layer-2 approaches, sharding, and enhanced consensus techniques to increase transaction speed and overall system efficiency (20) (21) (22).

Research highlights blockchain's potential to transform healthcare data management by offering secure, immutable, and decentralized records. Through the use of encryption and access regulations through smart contracts, the framework enhances security by preventing unauthorized entry and alterations (23). Efficiency improves by minimizing data management errors and refining transaction processing, which lowers administrative expenses. Furthermore, the immutability of blockchain guarantees the integrity of the data so that the records remain free of any unauthorised modifications. However, these advantages place blockchain as a transformational technology for managing electronic health records in such a way that ensures interoperability, compliance to regulations, and data protection of patients.

However, as the research shows the efforts also bring with them significant challenges that merit additional study. Reasons include its lack of scalability, which prevents the handling of the increased transaction volume during the busy periods, as it can put a strain on the block-chain (24). Additionally, regulatory compliance is difficult as establishing how the blockchain solutions work in line with the in placement of healthcare regulations such as HIPAA or GDPR requires a tailored implementation (25).

The studies to focus for the upcoming studies are the enhancement of the blockchain scalabilility using the Layer-2 solutions and hybrid systems. In addition, it should be possible to integrate with the current healthcare systems in a smooth way, and at the same time follow changing regulatory standards.

3. Results and Discussion

Comparing the blockchain-enabled healthcare system with the conventional centralized healthcare models gets a positive note for data security and integrity as well as efficiency. The most important discovery of the research is 30% of the reduction of error ratios from the management of the data. Centralized healthcare systems are typically manual and their information data entry can make errors and inconsistencies in patient records. On the other hand, blockchain technology utilizes the automated transaction validation as well as the use of cryptography for verification to maintain the data accuracy without man errors (26). Blockchain improves reliability of electronic health records (EHRs) by standardizing data in fewer lines of code, eliminating redundancies, and streamlining how it is managed.

In addition, blockchain guarantees total immutability of records at 100%, and guarantees data integrity significantly more. This study suggests that once the data is put on the blockchain, it cannot be changed or deleted, and it also presents secure and verifiable records for patients. Furthermore, blockchain's immutable nature increases trust in healthcare data as it creates a transparent, unalterable record of such transactions (27). Blockchain guarantees more secure and traceable data integrity of all medical records than centralised systems, which are often prone to unauthorized modifications and breaches.

Another important general advantage of the blockchain based system is improved access control techniques. Implementation of the smart contracts and role-based access control (RBAC) in blockchain technology has been found to completely eradicate the unauthorised data breaches. Manual access control that is part and parcel of traditional centralised healthcare systems becomes an easy target for security threats such as internal breaches and sharing of data without the consent of patient. However, blockchain based access control systems guarantee that any healthcare provider or associated person can only access appropriate medical records as defined by permission (28). Smart contracts are self-executive that automates the management of access, reduces administrative workload and improves security.

Compared to other existing distributed ledger systems, blockchain is highly enhanced in security, efficiency; however, scalability remains a cardinal issue. However, the research points out that, during peak load periods, the system encountered delays in dealing with transactions, as the amount of the transaction grew. The reason for such a restriction is the way blockchain networks use consensus, by which data integrity is protected but transaction speed is slowed down. Therefore, the research suggests improvements to deal with this issue, including off chain storage options, sharding and hybrid blockchain framework (29). With off-chain storage, which is storing the healthcare data outside of the blockchain, but it has a cryptographic proofs on blockchain, this alleviates the congestion. A method of sharding which divides the blockchain into smaller parts and allows for simultaneous execution of transactions would improve the speed of processing. Hybrid blockchain frameworks that combine a subset of features of public and private block chains also increase scalability without losing security (30).

Another important factor of blockchain implementation in healthcare apart from scalability, is the adherence to regulations. That research brought to light the need for any blockchain based systems to strictly adhere to the most strict healthcare regulations, such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). For patient privacy and data protection and compliance with legal responsibility, it is necessary to obey these rules (31). Compared to conventional systems, blockchain provides inherent transparency via its distributed ledger that would allow regulators and managers of the healthcare to monitor data access and changes in real time. This is to make sure that the organization adheres completely to the privacy regulations and to use permissioned blockchain networks such that access is limited to certain parties. With the help of blockchain technology, blockchain technology provides its security and efficiency while keeping transparency and protecting the health care organizations from the legal contraventions incidentally under regulated access networks(32).

This research produces strong evidence that, when correctly implemented and refined, blockchain technology is able to create substantial improvement in the management of health data where there is weakness related to security, integrity, and adherence to the rules. The results from the suggested Hyperledger Fabric based framework provide strong support for the feasibility of blockchain systems to address key deficiencies of electronic health record (EHR) systems. Of significant note, the system also proved to be a very efficient solution to the problem of data immutability, access management through SMAC contracts, and protection of sensitive medical information from cyberattacks, which still present major challenges in today's healthcare IT environments(33).

The system transaction latency and throughput met the operational need of mid-to-large hospital settings under typical operational conditions. In particular, the recorded average latency of 2.3 seconds and 1,150 TPS show that framework is capable of supporting real time clinical workflows. These metrics show not only good processing but also in the same order or even better than previous research on permissioned blockchain platforms for healthcare setting. The system also maintained the total data integrity under all the tested conditions. Decentralized consensus protocols basing on cryptographic hashing with SHA-256 prevented tampering and unauthorised modifications efforts, making the verifiability of patient records possible(34).

The successful implementation of role-based access control (RBAC) through smart contracts was another important result. Both in terms of allowing legitimate access, and in terms of denying unauthorized re-quests, the system achieved a perfect success rate. This level of accuracy in controlling access is critical, given that laws such as HIPAA and GDPR, for example, punish any data leaks by those not allowed to, and there are legal and ethical costs associated with them. Multiple improvements in aspects when comparing with a typical centralized EHR solution were identified when comparing with the blockchain based solution. One of the great enhancements was the 30% reduction in data entry errors that could be attributed to blockchain's automatic verification process. Finally, the system's audit facilities, based upon unchangeable transaction logs, provided immediate visibility of all access and modification actions improving compliance oversight and regulatory reporting. While centralised systems usually rely on manual log inspection and occasional audit, these can be delayed or in error. Furthermore, being subject to security breaches with conventional systems with their single point of failure design, the testing showed that the blockchain framework is secure and reliable in managing health data(35).

Whilst the research demonstrated these favourable results, they also identified constraint to scalability under intense load situations. When the volume of transactions started to rise, system latency went up to 7.8 seconds and throughput went down to 620 TPS. While still operational, these performance declines could pose difficulties for implementation at national or cross-institutional levels where transaction requirements are considerably greater. These results align with earlier studies pinpointing consensus mechanisms and synchronous validation procedures as significant obstacles in permissioned blockchain systems. To tackle this, the research recognizes the promise of new solutions like Layer-2 protocols, sharding, hybrid blockchain frameworks, and off-chain storage systems such as IPFS. These improvements may boost scalability while maintaining the security and integrity advantages inherent in blockchain technology.

Another factor to consider is the combination of blockchain frameworks with existing healthcare IT systems, which still presents technical and organizational obstacles. The majority of hospitals and clinics utilize systems that were not created considering decentralization or blockchain compatibility. To achieve seamless integration, standardized data formats like HL7 FHIR are needed, along with the creation of strong application programming interfaces (APIs) and interoperability layers. Even though this research did not replicate complete

From a regulatory perspective, the immutability of blockchain can occasionally clash with data protection regulations, especially the GDPR's "right to be forgotten." To address this, the framework keeps sensitive patient information off-chain, storing only encrypted references and cryptographic hashes on the blockchain. This combined method adheres to legal advice that supports keeping identifiable data distinct from the unchangeable ledger. Nevertheless, for widespread acceptance to thrive, it is crucial to establish supportive legal structures that tackle concerns like data ownership, liability, international governance, and accountability within decentralized healthcare systems.

The study's practical implications are extensive. Hospitals and healthcare providers can enhance security, auditing, and data access management without having to replace their current infrastructure. Implementing blockchain as an integration or overlay layer enables gradual adoption with little disruption. Regulators gain from clear audit trails that ease compliance enforcement and improve confidence in healthcare systems. Patients are, in turn, provided with increased control over their personal health information, reflecting the ongoing transition towards patient-focused care models. Nonetheless, the implementation must be gradual, guided by the readiness of institutions, the maturity of infrastructure, and compliance with both local and global data protection regulations.

Although the study makes a compelling argument for implementing blockchain in healthcare, various limitations need to be recognised. While a synthetic dataset is thorough, it may not entirely reflect the intricacies and diversity of actual clinical data. The simulations were carried out in a regulated virtual setting, indicating that real performance in live implementations across various institutions could vary due to network delays, user actions, and system diversity(36). Moreover, the main emphasis of the study was on technical performance. It did not assess user experience, operational expenses, or organisational preparedness—factors that are essential for effective implementation. These domains signify crucial pathways for upcoming research, especially as healthcare systems transition to

4. Conclusions

The study's empirical results highlight the transformative possibilities of blockchain technology in improving the security, efficiency, and transparency of healthcare data management systems. Utilising the decentralised structure and cryptographic features of Hyperledger Fabric, the suggested framework effectively showcased enhanced data integrity, unchangeable audit trails, and accurate role-based access control. These features provide solutions for many troubling problems with centralised electronic health records (EHR) systems, including data breaches, unauthorised access, and intractable inability to audit. The results of scenario-based performance testing, together with the results of comparative benchmarking, support the superior handling of critical healthcare data by blockchain in a way that also conforms to regulations, like HIPAA and GDPR.

In spite of these improvements, the research also uncovered significant scalability issues, especially under stressed conditions where higher transaction volumes resulted in reduced performance. This issue reflects results in current literature and underscores the need to integrate Layer-2 scaling solutions, sharding methods, and hybrid blockchain structures that merge the advantages of public and private ledgers. These enhancements are crucial for facilitating extensive implementation in national health systems or high-capacity settings like emergency care networks and multi-institutional data sharing.

Apart from the technical details, this study highlights the necessity for thorough policy formulation, alignment of regulations, and involvement of stakeholders to support practical implementation. Achieving effective integration of blockchain within healthcare systems will necessitate synchronisation with cur current health IT frameworks, investment in digital literacy, and a governance structure that tackles concerns like data ownership, liability, and cross-border data interoperability.

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 conceptualised 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 interest

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

[1] S. S. M. Abdul, "Navigating blockchain's twin challenges: Scalability and regulatory compliance," Blockchains, 2024.

[2] A. S. M. Ali, S. Ali, K. Ziaullah, M. I. Joo, and H. C. Kim, "IoMT and blockchain synergy: A novel approach to health data validation and storage," IEEE Access, 2025, early access.

[3] R. M. A. Latif, K. Hussain, N. Z. Jhanjhi, A. Nayyar, and O. Rizwan, "A Remix IDE: Smart contract-based framework for the healthcare sector by using blockchain technology," Multimedia Tools Appl., pp. 1–24, 2020.

[4] T. M. Sathish Kumar, "Low-power design techniques for Internet of Things (IoT) devices: Current trends and future directions," Prog. Electron. Commun. Eng., vol. 1, no. 1, pp. 19–25, 2024, doi: 10.31838/PECE/01.01.04.

[5] S. Bhattacharya and J. Poray, "Leveraging blockchain technology for public health," Int. J. Multidiscip. Res., 2024.

[6] S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain technology and application: An overview," PeerJ Comput. Sci., vol. 9, e1705, 2023.

[7] S. Friedrich and T. Friede, "On the role of benchmarking data sets and simulations in method comparison studies," Biometrical J., vol. 66, no. 1, 2200212, 2024.

[8] T. M. S. Kumar, "Security challenges and solutions in RF-based IoT networks: A comprehensive review," SCCTS J. Embedded Syst. Des. Appl., vol. 1, no. 1, pp. 19–24, 2024, doi: 10.31838/ESA/01.01.04.

[9] M. H. Gakire, "The use of blockchain in securing patient data," Res. Output J. Public Health Med., 2024, doi: 10.59298/ROJPHM/2024/324750.

[10] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique, "Blockchain application in healthcare systems: A review," Systems, vol. 11, no. 1, p. 38, 2023.

[11] F. Gong, L. Kong, Y. Lu, J. Qian, and X. Min, "An overview of blockchain scalability for storage," in Proc. 26th Int. Conf. Computer Supported Cooperative Work in Design (CSCWD), 2023, pp. 516–521.

[12] S. Sadulla, "Optimization of data aggregation techniques in IoT-based wireless sensor networks," J. Wireless Sensor Netw. IoT, vol. 1, no. 1, pp. 31–36, 2024, doi: 10.31838/WSNIOT/01.01.05.

[13] A. Hasselgren, J. A. HanssenRensaa, K. Kralevska, D. Gligoroski, and A. Faxvaag, "Blockchain for increased trust in virtual health care: Proof-of-concept study," J. Med. Internet Res., vol. 23, no. 7, e28496, 2021.

[14] S. Hermes, T. Riasanow, E. K. Clemons, M. Böhm, and H. Krcmar, "The digital transformation of the healthcare industry: Exploring the rise of emerging platform ecosystems and their influence on the role of patients," Bus. Res., vol. 13, no. 3, pp. 1033–1069, 2020.

[15] H. M. Hussien, S. M. Yasin, S. N. I. Udzir, A. A. Zaidan, and B. B. Zaidan, "A systematic review for enabling of develop a blockchain technology in healthcare application: Taxonomy, substantially analysis, motivations, challenges, recommendations and future direction," J. Med. Syst., vol. 43, pp. 1–35, 2019.

[16] K. Ismail and N. H. Khalil, "Strategies and solutions in advanced control system engineering," Innov. Rev. Eng. Sci., vol. 2, no. 2, pp. 25–32, 2025, doi: 10.31838/INES/02.02.04.

[17] V. Imogen, V. Sahithya, and B. Varshini, "Healthcare management using blockchain," Sep. 2023.

[18] B. Kakkar and P. Johri, "Blockchain: A healthcare perspective," in Proc. 2021 10th Int. Conf. System Modeling & Advancement in Research Trends (SMART), 2021, pp. 373–379.

[19] M. Karthigha, C. Padmavathy, and V. Akshaya, "Blockchain-based healthcare data management," in Proc. 2022 Int. Conf. Automation, Computing and Renewable Systems (ICACRS), 2022, pp. 392–396.

[20] A. Khatoon, "A blockchain-based smart contract system for healthcare management," Electronics, vol. 9, no. 1, p. 94, 2020.

[21] C. Maher, T.-T. Kuo, M. S. B. Kasyapa, and C. Vanmathi, "Blockchain integration in healthcare: A comprehensive investigation of use cases, performance issues, and mitigation strategies," Front. Digit. Health, vol. 6, 2024.

[22] Y. Mali et al., "Role of blockchain in health application using blockchain sharding," in Proc. 2023 14th Int. Conf. Computing Communication and Networking Technologies (ICCCNT), 2023, pp. 1–6.

[23] V. Maurya et al., “Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions,” Peer-to-Peer Netw. Appl., vol. 18, no. 1, pp. 1–35, 2025.

[24] R. Rahim, “Optimizing reconfigurable architectures for enhanced performance in computing,” SCCTS Trans. Reconfigurable Comput., vol. 1, no. 1, pp. 11–15, 2024, doi: 10.31838/RCC/01.01.03.

[25] I. P. Odilibe et al., “Blockchain in healthcare: A comprehensive review of applications and security concerns,” Int. J. Sci. Res. Archive, 2024.

[26] R. Raj and S. P. Raja, “Revolutionizing healthcare: Blockchain’s transformative applications for data security, privacy, and interoperability,” in Proc. 2024 IEEE 9th Int. Conf. for Convergence in Technology (I2CT), 2024.

[27] F. Reegu, S. M. Daud, and S. Alam, “Interoperability challenges in healthcare blockchain system—A systematic,” Ann. RSCB, vol. 25, no. 4, pp. 15487–15499, 2021.

[28] L. Sadath, D. Mehrotra, and A. Kumar, “Scalability performance analysis of blockchain using hierarchical model in healthcare,” Blockchain Healthc. Today, vol. 7, 2024.

[29] K. Sehimi, F. Bendaoud, and H. H. Benderbal, “A review of scalability solutions in blockchain-based electronic health record systems,” in Proc. 2023 IEEE Int. Conf. Networking, Sensing and Control (ICNSC), 2023, pp. 1–6.

[30] Y. Singh, M. A. Jabbar, S. Kumar Shandilya, O. Vovk, and Y. Hnatiuk, “Exploring applications of blockchain in healthcare: Road map and future directions,” Front. Public Health, vol. 11, 1229386, 2023.

[31] A. Tolk, “Conceptual alignment for simulation interoperability: Lessons learned from 30 years of interoperability research,” Simulation, vol. 100, no. 7, pp. 709–726, 2024.

[32] C. A. Prasath, “Optimization of FPGA architectures for real-time signal processing in medical devices,” J. Integr. VLSI, Embedded Comput. Technol., vol. 1, no. 1, pp. 11–15, 2024, doi: 10.31838/JIVCT/01.01.03.

[33] M. Varman, K. Shrinivaas, R. Karthick, and V. Vanitha, “Blockchain in healthcare data,” in Proc. 2023 2nd Int. Conf. Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2023, pp. 1–6.

[34] A. Vernekar, A. Kshirsagar, and V. K. Pachghare, “Sharding-based scalability enhancement of blockchain-based health applications,” in Proc. 2023 Int. Conf. Circuit Power and Computing Technologies (ICCPCT), 2023, pp. 901–906.

[35] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, “HealthBlock: A secure blockchain-based healthcare data management system,” Comput. Netw., vol. 200, 108500, 2021.

[36] F. Zhou et al., “Blockchain for digital healthcare: Case studies and adoption challenges,” Intell. Med., vol. 4, no. 4, pp. 215–225, 2024.