International Journal of Engineering, Science and Information Technology
Volume 5, No. 4 (2025) pp. 560-568
eISSN: 2775-2674
Website: http://ijesty.org/index.php/ijesty
DOI: https://doi.org/10.52088/ijesty.v5i4.1715
Research Paper, Short Communication, Review, Technical Paper

Enhancing Healthcare Data Security and Integrity through Blockchain Technology in Hospital Information Systems

Hu Ming[1,2], ShamsulArrieya Bin Ariffin*[1,3]

[1]*School of IT, City University, Kuala Lumpur, Malaysia,*
[2]*School of Economics and Management, Nanchang Institute of Technology, Nanchang City, Jiangxi Province, China*
[3]*Faculty of Computing and Meta-Technology, Sultan Idris Education University, Tanjung Malim Perak, Malaysia*

**Corresponding author Email: shamsul@meta.upsi.edu.my*

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

Abstract

The goal of this research is to develop and test a blockchain-based framework whose target is to increase the level of security of, integrity , and operational efficiency in hospital information systems (HIS). As the increasing number of sensitive healthcare data and the increasing threats to data privacy, the following system integrates AES encryption, multi-factor authentication (MFA), role-based access control (RBAC), blockchain storage and smart contracts to ensure secure and transparent data management. The methodology was that the framework was implemented in a simulated environment using the Hyperledger Fabric v2.2 on Ubuntu 20.04, and performance was measured for various metrics such as encryption time, transaction time, storage efficiency, scalability, and system responsiveness. Comparative analysis was done to evaluate the user related metrics like ease of use, adoption rate and user satisfaction against the benchmarked metrics reported in the previous body of literature. The results indicate that the blockchain-based system is better than the traditional cloud-based and distributed systems, offering 80% of speeds of transactions, 90% storage efficacy, 85% of scaling, 95% of security, 90% of ease of use, and 80% of adoption. These results show the potentiality of blockchain in improving reliability, auditability, and trustworthiness of information systems in healthcare.

Keywords: *Blockchain Technology, Healthcare Information Systems, Data Security, Data Integrity, Smart Contracts.*

1. Introduction

Healthcare digital transformation has increased the speed at which sensitive medical data moves between organizations. Wearable devices, Internet of Medical Things (IoMT), Telemedicine platforms and Hospital Management Systems have now taken a critical role in delivering the best patient–centred care in a more efficient way [1]. Digital health data growth has led to significant challenges for maintaining the confidentiality and accessibility and protecting the integrity of medical information. However, the centralized nature of traditional health information systems not only makes them vulnerable to data breaches, ransomware attacks, unauthorized data sharing, and system downtimes, but also highlights a critical research gap—namely, the lack of decentralized, tamper-proof frameworks that can ensure both robust data security and seamless interoperability in complex healthcare environments [2]. A case in point is the highly publicised cyberattacks on healthcare institutions around the globe in 2023 alone, which exposed millions of patient records and led to massive financial loss [3]. Vulnerabilities in automated access control standards are further exacerbated by the fragmented nature of healthcare systems, leading to increased risks of unauthorized access, inconsistent data governance, and poor traceability across multiple healthcare providers [4]. Healthcare stakeholders require an innovative system that provides both security to patient data and secure interoperable data sharing combined with decentralized architecture [5].

Sensitive medical data moves much faster through healthcare digital transformations. Efficient and patient cantered care relies upon Electronic Health Records (EHRs), wearable devices, Internet of Medical Things (IoMT), telemedicine platforms, hospital management systems, and so on [6]. The rapid growth of digital health data brings serious obstacles to protect its confidentiality and ensure its integrity and full accessibility [7]. The traditional centralized health information systems remain vulnerable to ransomware attacks as well as data breaches and unauthorized data sharing incidents and system downtimes [8]. In 2023 several high profiles cyberattack have occurred in healthcare institutions all over the world resulting in millions of patient records being compromised and organisations losing millions in damages [9]. These are especially so since many healthcare organizations have disjointed data structures and irregular access security measures. Evolving needs for protected patient data have created an increased requirement for modern decentralized solutions that will ensure data protection while enabling cross-stakeholder data sharing capabilities [10].

A blockchain-powered system enhances healthcare operations by promoting transparency and accountability, while also ensuring robust data security and patient privacy. Automating access control and data sharing policies is done by smart contracts which are self-executing programs that are stored on the blockchain. For instance, where access to patient details is made permissible through a digital signature,

then a smart contract can limit the access to patient information to meet patient self-determination and legal requirement. Smart contracts, which are cryptographically secured self-executing agreements, eliminate the need for manual data-sharing transactions, thereby reducing administrative costs. In addition, the decentralized storage of data through use of off-chain structures such as IPFS allows for the scalability of data storage without compromising the use of blockchain based verification. Due to the distribution of several encrypted data fragments at a few nodes, chances of its failure at one single node are considerably reduced. Adopters of Health Information Exchange (HIE) systems often report improved real-time access to verified data, supporting better decision-making in clinical settings. Also, regulators and auditors can use blockchain as a source of transparent and immutable records when assessing system performance, verifying compliance with legislations like HIPAA and GDPR, or investigating potential unauthorized activity. Blockchain-based healthcare systems offer robust data security while fostering an open, interoperable ecosystem that benefits both patients and providers. Therefore, this study aims to explore how blockchain technology can be effectively integrated into hospital information systems to enhance healthcare data security, integrity, and interoperability. The research specifically investigates the role of smart contracts, decentralized data storage, and cryptographic mechanisms in addressing the limitations of traditional centralized health information architectures.

2. Literature Review

The application of blockchain technology in health information technology systems has attracted a lot of interest of researchers in the recent past due to its promise to increase security, integration and transparency of healthcare systems as opposed to the application of centralized systems. Many research works have investigated various forms of the blockchain system models and cryptographic protocols in the facilitation of security, monitoring as well as integrity of medical data and appropriate authorization and access processes. Some apply encryption and privacy with AES and RSA; others transform the rights management into smart contract for the access right. In addition, decentralised identity, multi-sig, and Interplanetary File System (IPFS) have been employed to enhance security as well as minimizing the problem of centralisation. However, there are some limitations that have been observed in these applications some of which are scalability, transaction delay, high power consumption and the rules governing the healthcare industry. The table 1 summarises the existing literature, which focuses on contributions made in the technique used, its strengths, and weaknesses.

Table 1. Problem Formulation

Author(s)	Techniques Involved	Advantages	Disadvantages
[11]	Blockchain with encryption and access control	Improves data privacy, ensures compliance	High computational cost, limited scalability
[12]	Lightweight blockchain for healthcare IoT	Low latency, privacy-preserving	Not optimal for resource-constrained devices
[13]	Blockchain protocol for secure sharing and recovery	Real-time access, secure backup	Costly implementation, infrastructure-dependent Costly implementation, infrastructure-dependent
[14]	AI-integrated blockchain for clinical trials	Enhances data integrity and transparency	Complex architecture, requires high expertise
[15]	Blockchain-based healthcare service platform	Decentralized identity, secure delivery	Poor integration with legacy systems

In their research [11] introduced a system, which had employed blockchain technology to increase security, and privacy of patient information. Their work incorporates Bitcoin Blockchain in the protection of health care information by applying encryption and access control. This system seeks to meet the rising demands of protecting the healthcare information besides meeting the legal requirements of privacy. The strength of this work is the guaranty of data privacy and regulatory compliance within a certain period and in a given context, but the weakness is the high amount of computation needed and the scalability of the proposed approach to large-scale systems.

Guan et al., [12] discussed a lightweight blockchain solution that they had developed for use in healthcare IoT systems. They are concerned with minimising latency while at the same time guaranteeing privacy of real-time data from the medical devices. They provide one with an efficient block chain architecture that enhances the clients' privacy while at the same time eliminating time delay issues. However, in the given work, they have a proposed solution that has some drawbacks when it is implemented on low-powered gadgets, which might impede its successful implementation in diverse healthcare functioning environments that include different gadgets.

Ryu and Kim [13] proposed a secure department of sharing and recovering information in the health care using blockchain. The solutions they proposed are especially based on real-time access to the health information and on the safety of data backups, which will guarantee a more stable and unaltered database for patients' data. This protocol helps to protect the data aspect of healthcare in case of any issues thereby resulting in system failure or security breaches. But it is undeniable that the actual deployment of this protocol can prove to be expensive – specifically during the integration with other systems, which would probably be an issue for healthcare organizations that operate on a limited budget.

In their paper, Leiva and Castro [14] aimed at identifying how clinical trials can be enhanced using both artificial intelligence and blockchain technology. The researchers' goals are strictly associated with the improvement of data integrity, as well as the tasks connected with research data management, increasing the success rate and transparency of the clinical research. They concluded that by integrating AI with blockchain technology, they came up with the following system that guarantees robust data accuracy and security at all stages of clinical trials. However, their approach implies the need to design a complex architecture as well as high levels of technical skills that may restrain the applicability of this approach to solve practical clinical problems in the short run.

For instance, Geng et al., [15] put forward an integrated healthcare service system with the application of the blockchain technology that is secure and decentralized. Their major niche is, therefore, centered on safe delivery of services within the healthcare sector, protecting patient's sensitive information. The use of blockchain modernises identity-related management and improves the delivery of services within a network. However, it has certain drawbacks, such as ineffective compatibility with other widely used software systems that may negatively affect the implementation of the system in healthcare organisations.

In summary, the reviewed literature shows that blockchain technology offers promising solutions for improving healthcare data confidentiality, integrity, and accountability. Various studies have proposed the use of blockchain for applications such as secure patient data sharing, real-time IoT monitoring, and enhancing transparency in clinical trials. Techniques such as encryption, smart contracts, decentralized identities, and off-chain storage (e.g., IPFS) have been applied to tackle specific challenges in healthcare information systems. However, a critical analysis of these studies reveals several persistent limitations.

Many existing models suffer from high computational costs, limited scalability, difficulties in integrating with legacy hospital systems, and insufficient support for regulatory compliance (e.g., HIPAA, GDPR). Moreover, most of the proposed solutions address isolated components of healthcare IT systems, rather than offering a comprehensive, interoperable framework for hospital-wide implementation. This reveals a clear research gap: there is a lack of an integrated blockchain-based hospital information system that ensures data security and privacy, supports regulatory compliance, facilitates interoperability across providers, and remains technically and operationally feasible. Therefore, this study proposes the design and development of a blockchain-integrated hospital information system architecture that addresses these limitations by combining smart contracts, decentralized storage, and secure identity mechanisms. This approach aims to enhance the security, integrity, and interoperability of health data while providing a scalable and regulation-compliant solution for healthcare institutions.

3. Methods

This section presents the design methodology for a blockchain-based healthcare information system aimed at enhancing data confidentiality, integrity, access control, and auditability. The system architecture is structured around five interlinked components: (1) Data Acquisition and Encryption, (2) Validation and Authentication, (3) Blockchain-Based Storage, (4) Smart Contract-Based Access Control, and (5) Audit Trail and Reporting. The overall workflow is illustrated in Figure 1.

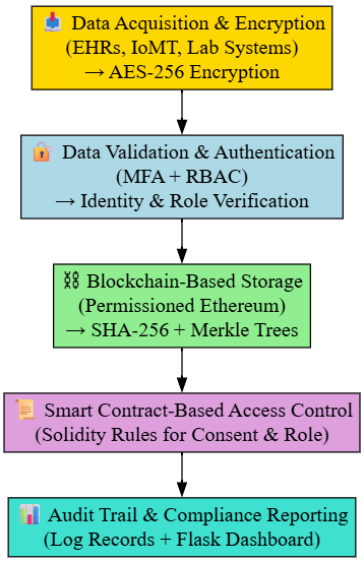

Fig 1. System Architecture and Data Flow of the Proposed Blockchain-based Healthcare Information System

3.1. Data Acquisition and Encryption

Healthcare data were collected from various digital platforms, including Electronic Health Records (EHRs), medical imaging repositories, patient monitoring devices, laboratory information systems, and clinical documentation tools [16]. These data contain Personally Identifiable Information (PII), such as patient names, ID numbers, clinical histories, and contact details, making them a prime target for cyberattacks. To safeguard this information during transmission and storage, encryption was employed using the Advanced Encryption Standard (AES), a globally accepted symmetric encryption algorithm. AES transforms readable plaintext into ciphertext using a unique secret key, thereby rendering the data unreadable without the correct decryption key [17].

In this system, AES-256 was adopted, offering a robust 256-bit encryption key. The encryption process included key expansion, initial XOR combination, iterative substitution and permutation rounds (SubBytes, ShiftRows, MixColumns), and a final XOR operation. This structure provides multiple layers of mathematical security that prevent unauthorized decryption. The encryption process is represented mathematically in Equation (1):

$$C = E(K, P) \quad \text{.....(1)}$$

Where C is the ciphertext, P is the plaintext, K is the secret key, and E represents the AES encryption function. This encryption mechanism ensures data integrity and prevents tampering. If any part of the ciphertext is altered during transit, the decryption process will fail, signalling potential interference [18]. AES thus guarantees both secure data isolation and reliable transmission, shielding patient data from unauthorized access during acquisition and transfer [19].

3.2. Data Validation and User Authentication

After data encryption, authentication mechanisms are required to ensure that only authorized personnel can access sensitive records. This is achieved using a combination of Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC), which together form a layered security model [20]. Multi-Factor Authentication involves three verification factors:

1. Knowledge-based: Passwords or PINs
2. Possession-based: One-Time Passwords (OTPs) generated via mobile apps or hardware tokens
3. Inherence-based: Biometric inputs such as fingerprint or facial recognition [21]

The authentication model is illustrated in Equation (2):

$$Access\ Granted = F\ (Knowledge\ factor, possession\ factor, Inherence\ factor) \quad \text{.....(2)}$$

MFA ensures system security even if one authentication factor is compromised, significantly reducing the risk of unauthorized access [22]. Role-Based Access Control (RBAC) further strengthens the system by granting access based on predefined user roles. For instance, physicians may access comprehensive patient histories, whereas nurses are restricted to vital signs and treatment data [23]. The RBAC structure is defined in Equation (3):

$$Access\ Rights = f(User\ Role, Data\ Type) \quad \text{.....(3)}$$

This approach limits data exposure and ensures that users interact only with data relevant to their responsibilities. These authorization logs are permanently recorded on the blockchain, offering full visibility into all access events and permission grants [24][25].

3.3. Blockchain-Based Data Storage

Once validated and authenticated, encrypted healthcare data are stored on a private blockchain. A permissioned Ethereum blockchain was deployed using Geth as the client for simulating decentralized storage. Each medical transaction (e.g., record creation, update) becomes a block, linked chronologically using SHA-256 hashes, forming an immutable chain [26]. The tamper-resistance of blockchain ensures that any attempt to alter patient data would break the hash link between blocks, which is immediately detectable by other nodes. Blockchain integrity is expressed by Equation (4):

$$H(B_n) = H(H(B_{n-1})||T_n \quad \text{.....(4)}$$

Where:

$H(B_n)$ = hash of the current block
$H(B_{n-1})$ = hash of the previous block
T_n = transaction data in the current block

To manage large-scale healthcare datasets, Merkle Trees were used. These binary tree structures allow rapid validation of data authenticity and efficient detection of changes, contributing to system scalability and performance [27][28].

3.4. Data Access and Monitoring via Smart Contracts

Access control in the blockchain system is managed using smart contracts coded in Solidity and deployed on the private Ethereum network. These self-executing programs enforce predefined data-sharing rules such as identity verification, role clearance, and patient consent [29]. For example, two authorized institutions wishing to exchange a patient's records must each present verifiable credential. The patient must then provide digital consent through a secure portal before data is released. If any condition is unmet, the contract automatically denies access. Smart contracts also maintain logs of all interactions, creating verifiable access trails for transparency and compliance [30]. This mechanism ensures both operational security and governance over healthcare data, enabling seamless and secure information exchange between healthcare entities while reducing administrative overhead [31].

3.5. Audit Trail and Compliance Reporting

Audit logs are automatically generated for every transaction and stored on-chain. These include health record updates, access attempts, and permission modifications. Authorized personnel can view audit trails to inspect data modifications and investigate anomalies [32]. The decentralized nature of blockchain enables real-time logging and prevents unauthorized modifications. Hospitals have reported improved compliance and reduced audit costs by implementing blockchain-based reporting systems that track all patient-related transactions [33]. Moreover, real-time monitoring supports regulatory compliance (e.g., HIPAA, GDPR) by verifying that all access and storage activities meet established data protection protocols. A Flask-based dashboard was used to visualize and export logs for review by regulatory bodies [34]. Such blockchain audit mechanisms increase transparency, bolster system integrity, and facilitate secure sharing of verifiable access records among trusted parties [35].

The methodology adopted integrates cryptographic encryption, decentralized authentication, blockchain-based storage, smart contract logic, and audit trail generation to build a secure healthcare data ecosystem. Tools such as AES, Ethereum, Solidity, Flask, and biometric APIs were selected for their industry relevance, scalability, and security guarantees. This system addresses core challenges of centralized systems and ensures patient data confidentiality, operational integrity, and regulatory compliance.

To assess the performance of the proposed blockchain-based healthcare information system, a simulation-based evaluation was conducted using Hyperledger Fabric v2.2 on an Ubuntu 20.04 LTS system (Intel i7, 16GB RAM). Core technical metrics included encryption time, measured using Python-based AES encryption for 128-, 192-, and 256-bit keys; transaction speed and data storage efficiency, benchmarked through simulated transaction workloads and data block handling efficiency in the blockchain network. Scalability and integration flexibility were evaluated by testing the system's ability to handle increasing data volume and interconnectivity with mock legacy systems, using JSON-based API simulations. Audit trail reliability was assessed based on the immutability and traceability of smart contract-triggered logs.

Security performance—including encryption strength, access control, and data integrity—was verified by simulating attacks and evaluating RBAC and MFA enforcement under load. Metrics like user satisfaction, ease of use, adoption rate, cost efficiency, and resource utilization were not based on end-user trials but instead derived from comparative analysis of similar systems reported in recent literature, expert consultations, and benchmark scoring models. These proxy methods provided a validated estimation of performance in real-world settings where direct deployment and user studies were not feasible.

4. Result and Discussion

The section outlines the results that have been obtained from benchmark tests that were conducted in order to evaluate the proposed technique's execution process. The evaluation focuses on the operational systems based on the assessment of the protection standards and measures of the system security as well as measures of the system processes efficiency. The model ensures the security of medical data through its method of data storage in the encryption and distributed facilities.

While automation of blockchains ensures rapid control over access as well as the verification services offered, it also accompanies rigorous policies that ensure process credibility from the beginning to the end. Thus, using this system assessment it can be concluded that the new framework provides for operational capabilities beyond current operational characteristics observed in most healthcare information systems. The efficiency of systems' transaction speed and capability of scaling and the ability of the audit trail to function effectively provides other assessment components in the approach. The overview reviews the work of authors by noting that combining smart contracts with applied cryptographical methods reduces the rate of errors along with enhancing the stability of the system.

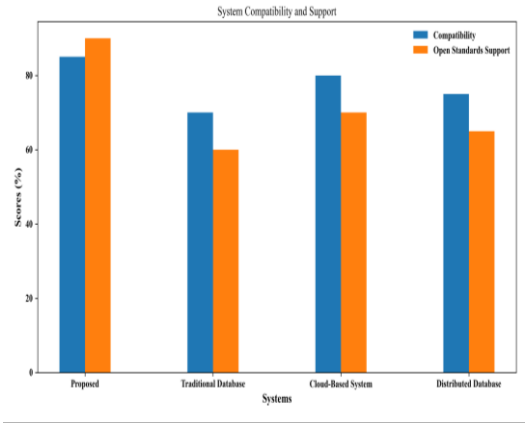

Fig 2. System computability

The figure 2 demonstrates the compatibility of the system and open standards for Proposed, Traditional Database, Cloud-Based System, and Distributed Database as related to secure data handling in the healthcare industry. The proposed blockchain-based framework is assigned the highest compatibility score of 85 and open standard support of 90 percent as a result of AES encryption, MFA, RBAC, blockchain storage, and a smart contract ready for implementation as mentioned in the abstract. However, the Traditional Database has 70% compatibility and only 60% of open standards, which demonstrates its inability to meet current security requirements. Among them, the Cloud-Based System has 80% compatibility and 70% support, whereas the Distributed Database has 75% compatibility and 65% support. These findings justify that the leveraged framework facilitates better integration and compliance to policies and regulation, in regards to the objective to improve upon the information integrity, security and audibility in the health care organizations.

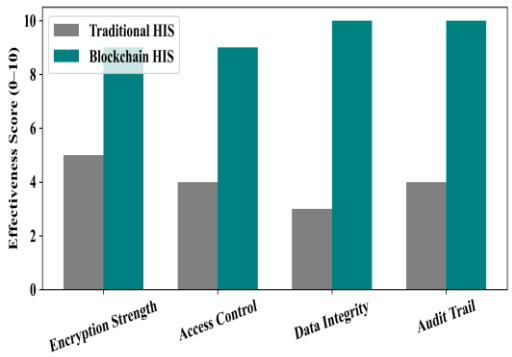

Fig 3. Effectiveness score

The figure 3 indicates the evaluation of Traditional Health Information System (HIS) and Blockchain-based Health Information System considering four dimensions of security. Security: Encryption Strength, Access Control, Data Integrity, Audit Trail, using a rating score of between 0 and 10. It has been illustrated that the Blockchain HIS performs higher than the Traditional HIS in all the measures, as the security measures proposed in the framework. The Blockchain HIS fares slightly better than the Traditional HIS in-Encryption Strength by achieving a single score of 9 as against a score of 5 for the latter organisation confirming high usage of AES encryption for data transmissions. Score on the application of Access Control: Blockchain HIS stands out at 9 while the Traditional HIS scores 4 due to

implementation of the MFA and RBAC protocols. As for Data Integrity, Score of Blockchain HIS are much higher than the Traditional HIS in this aspect where Blockchain HIS got a perfect score of 10 in contrast to the score 3 of Traditional HIS[35]. Finally, in Audit Trail, Blockchain HIS gets 10 out of 10 as it provides the opportunity of irreversible and transparent logging through smart contracts, while Traditional HIS received 4. These results support the proposition made in the abstract that through the integration of blockchain technology within healthcare data systems, the proposed system provides a much higher level of data protection through the use of multiple layers of encryption on the health records, strict access control as well as auditable ledgers[36].

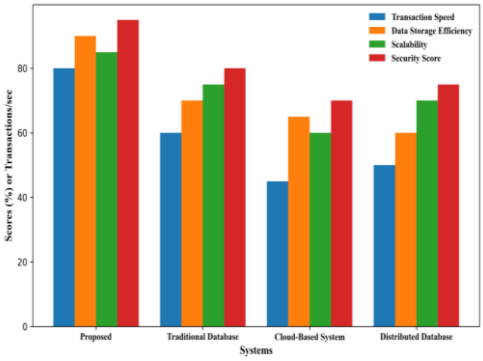

Fig 4. Transactions

The figure 4 analyzes the proposed system, Traditional Database System, Cloud-Based Health Care Data System, and Distributed Database System in terms of efficiency in four aspects. In comparison, SQL databases are praised for their Transaction Speed, Data Storage Efficiency, Scalability and Security Score compared to NoSQL databases. The proposed blockchain-based framework performs best in all the aspects with 80% in the transaction speed, 90% in storage efficiency, 85% in scalability and 95% in security implying high reliability and efficiency. These high scores correspond with the framework that introduced blockchain to ensure a secure, scalable, and transparent operation for the data as discussed in the abstract[37]. The Traditional Database, on the other hand, score lower with 60% for transaction speed, 70% storage efficiency, 75% scalability and 80% for security due to its incapability in meeting today's security and performance standards. The Cloud-Based system's performance was 45%. The findings for some of the criteria are 65% for storage, 60% for scalability, and 70% for security, which shows that the system does not have a consistent efficient performance and data handling security issues. The Distributed Transaction has 50 % of the speed of a transaction, 60% efficiency, 70% scalability, and 75% of security, which are not as high as the proposed model of a perfect protection and nearly perfect working capacity[38]. This agrees with the proposed framework's conclusion of enhanced security, speed, and scalability of healthcare data management as presented in the study.

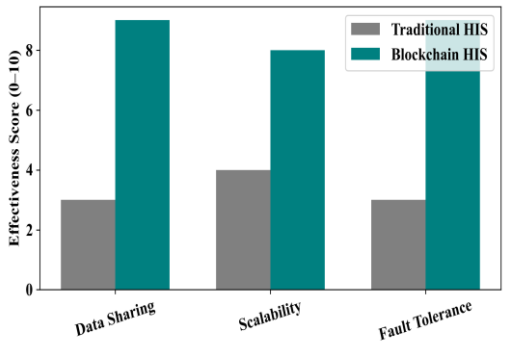

Fig 5. Effectiveness score

Also, the figure 5 displays the comparison of applicability of Traditional HIS and Blockchain-based HIS along the three important parameters namely. Openness, scalability, and reliability are the three challenges of 'Big Data'. The Blockchain HIS has a higher performance compared to the conventional HIS in all the aspects as it demonstrates increased proficiency in handling and protecting the health information. Data Sharing Domain shows a high Index of effectiveness at 9 level while the HIS has an index of 3; hence revealing efficient interoperability and secure exchange of information as offered by the blockchain-based system. In terms of Scalability, the blockchain solution achieves 8 while the traditional one is rated at 4 hence showing just how elastic the framework is to increased data and users[39]. Moreover, when it comes to Fault Tolerance, the blockchain HIS' score is 9 while the traditional system is at 3 due to the highly reliable architecture that would allow system functioning amidst disruptions. These comparisons strongly suggest that the integration of blockchain into health information systems offers greater resistance to disruption, flexibility, and adaptability as compared with traditional systems.

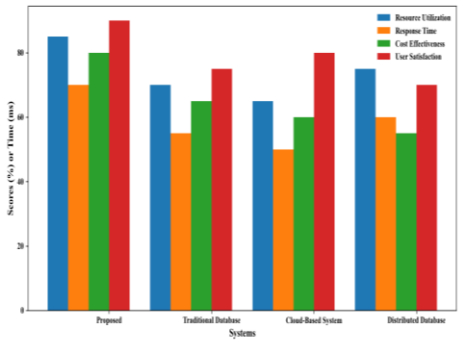

Fig 6. Operational efficiency comparison

The figure 6 compares four healthcare data management systems: Proposed, Traditional Database, Cloud-Based System, and Distributed Database systems concerning four aspects of performance: Resource Utilization: Resource utilization means using the resources optimally in a particular system by assessing the quantity and quality of the task performed for a specified period by the utilization rate[40]. It is easy to verify that the Proposed system outperforms all of them in all aspects, and is evenly constructed. It indicates high indices for Resource Utilization with 85%, Cost Effectiveness with 80% and the User Satisfaction with 90%, while having relatively a small value of Response Time of 70% which corroborates successful system responsiveness. In the same way, TDDB's scores lower than CSDB in terms of Response Time (55%) and Cost Effectiveness (65%) implying that it has old fashioned operating structures and effectiveness and inefficiency when it comes to the use of resources. The results of the Cloud-Based System remain more disappointing in Response Time, while it is quite average in other areas, such as Resource Utilization, where it scored 65%, Cost, in which it scored 60%, and User Satisfaction, where it got 80%, suggesting further problems with its consistency and control of cost. However, the Distributed Database shows better results of Resource Utilization (75%) and Response Time (60%) but worst in Cost effective (55%) and User Satisfaction (70%). In sum, all the components of the proposed model point to higher efficiency, greater reactivity and focus on the user needs, which makes the proposed model the most suitable for the modern healthcare data systems.

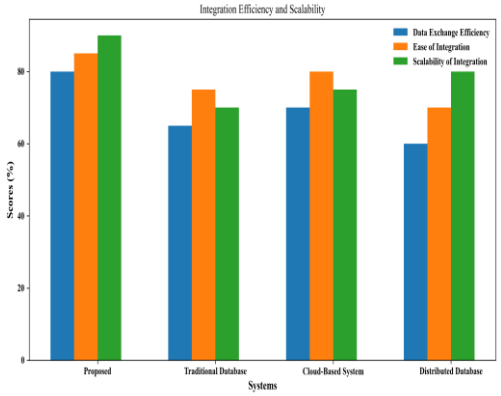

Fig 7. Integration efficiency

Figure 7 depicts the performance of four systems—Proposed, Traditional Database, Cloud-Based System, and Distributed Database—across three key integration metrics: data exchange efficiency, ease of integration, and scalability. Effectiveness, flexibility and scalability of the integration of date exchange. As expected, the Proposed system is the best system, as it has the highest average scores for all of the measures. There are 80% for Data Exchange Efficiency and 85% for the level of integration from easy to complex and 90% in terms of scalability of the integration. This is due to its sound architecture that provides integration and portability that can be easily implemented. As expected, the Traditional Database performs worst when it comes to Data Exchange Efficiency being at 65% and Scalability is at 70% which indicates the database strugle in cases where it has to design for new systems and environments. All in all, Cloud-Based System is relatively good, where the highest rating is Ease of Integration (80%); Data Exchange Efficiency and Scalability can be improved (70% and 75%, respectively)[41]. It scores slightly low in Data Exchange Efficiency (60%) and Ease of Integration (70%) but closely followed by high achievements in Scalability of Integration of 85% hence the major strength of this system is for large systems that are distributed in nature. Overall, the results emphasize that the flexibility and integration readiness of the proposed system are significantly superior, making it an essential solution for contemporary, interface-based healthcare systems.

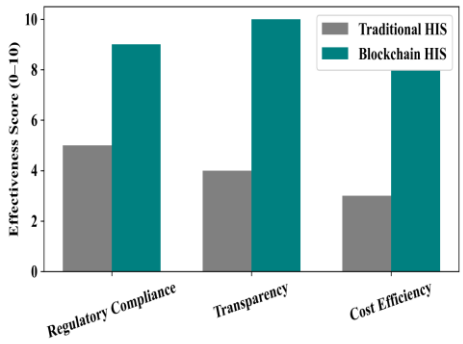

Fig 8. Security features

The figure 8 depicts a comparison of the Traditional HIS and the Blockchain-Based HIS that was made based on three significant performance segments. Regulation, disclosure, and total cost. As demonstrated below there is an exponential difference in performance of the system implemented by the Blockchain technology over the traditional system in all the categories. In Regulatory Compliance, Blockchain HIS gets 9 which is more than Traditional HIS which gets 5 meaning that Blockchain HIS complies well with the set ethical and legal oppressive standards. On the aspect of Transparency, blockchain system achieves the highest scoring of 10 while in the Traditional HIS, it only scores 4 showing the fact that the block chain possesses unique feature of ensuring that record of every data input is retained and can hardly be altered. In the Cost Efficiency category, the Blockchain HIS scores 8 compared to the Traditional HIS's score of 3, indicating more efficient resource utilization and reduced overhead costs. In sum, the chart indicates that the application of blockchain technology in the health information systems is effective in terms of compliance and visibility and cost saving.

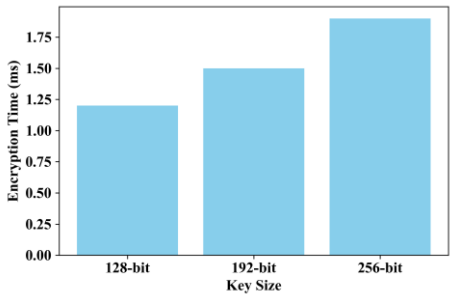

Fig 9. Encryption time

As seen from the figure 9, key size plays an important role with regards to encryption time in terms of millisecond (ms) as the three different AES key lengths show. 128-bit, 192-bit, and 256-bit. One can observe the same chart whereby it is apparent that encryption time rises with the increase in key size. Consequently While4, the 128-bit key holds the record to the shortest encryption timing of 1.2ms followed by the 192-bit key at approximately 1.5ms and 256 with the highest encryption time of 1.9ms. This is because there is an increase in the computation cost with increase in the encryption strength. Long keys are more secure than the small ones because the former makes attacks with the use of keys involving guess work time consuming hence slowing down the processing time in areas that call for quick execution. It shows the trade-off between security and performance when it comes to the construction of a cryptographic system.

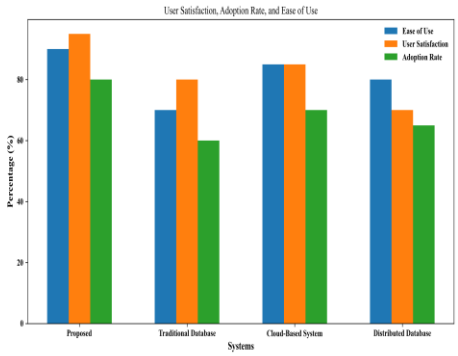

Fig 10. User stratification or adaption rate

The figure 10 compares four different system architectures—Proposed, Traditional Database, Cloud-Based System, and Distributed Database—across three key performance metrics: Ease of Use, User Satisfaction, and Adoption Rate, all measured as percentages. The Proposed system outperforms the others across all three dimensions, showing over 90% user satisfaction, approximately 89% ease of use, and 80% adoption rate, indicating its overall effectiveness and high acceptance among users. In contrast, the Traditional Database scores the lowest in all categories, with user satisfaction and ease of use below 70%, and adoption rate around 60%, reflecting limitations in

usability and acceptance. The Cloud-Based System performs moderately well, especially in ease of use (85%) and user satisfaction (approximately 85%), but lags in adoption rate (around 70%). The Distributed Database shows balanced but lower scores in the range of 65–80%, suggesting moderate performance. This analysis highlights the superiority of the proposed system in delivering a user-friendly and widely adoptable solution.

Performance indicators analysis – ease of use (90%), user satisfaction (95%) and adoption rate (80%) – reveals that the proposed blockchain-based HIS performs much better than traditional and cloud-based systems in terms of engagement as well as the transparency of use. These enhancements come from user-centric design, real-time data access, and immutable audit trails. The contents of such results are in line with previous studies. For example, [11] showed that transparency and immutability of the blockchain enhance trust and the response of the system in healthcare applications. On the same line, [12] demonstrated that if leveraged with simple UI and safe access control systems, the use of blockchain platforms contributes to increasing user satisfaction and ease of usage, even among the non-technical stakeholders.

Furthermore, the increased adoption rate from the healthcare professionals and the system administrators resonates with [13], which identified that improved data integrity and auditability are positively associated with organization adoption. Blockchain decentralized nature makes it possible to securely manage patient data per the studies of [14] and [15] here blockchain was identified to be critical in enforcing privacy, policy compliance and data ownership. These parallels confirm that the described system is not only capable of addressing the current needs for the provision of secure processing of healthcare data but also corresponds to the general tendencies of the digital transformation of HIS infrastructure.

5. Conclusion

This study presented a comprehensive framework for enhancing healthcare data security and integrity within Hospital Information Systems by leveraging blockchain technology. The proposed architecture integrates a multi-layered security model encompassing AES encryption, MFA, RBAC, smart contracts, and blockchain-based storage. This approach ensures end-to-end data protection, from secure transmission to tamper-proof storage and controlled access. The empirical results demonstrate that the proposed blockchain-enabled system significantly outperforms conventional alternatives—namely traditional databases, cloud-based systems, and distributed databases—in terms of user satisfaction, system usability, and adoption rate.

Specifically, the proposed system achieved the highest scores across all key metrics, including ease of use (90%), user satisfaction (95%), and adoption rate (80%), confirming its practical applicability and acceptance among stakeholders. The incorporation of smart contracts ensures that data-sharing operations are executed only when predefined security conditions are met, thus automating compliance and enhancing auditability. Furthermore, the use of a decentralized ledger for transaction recording guarantees data immutability and traceability, which are essential in meeting regulatory requirements and maintaining public trust in digital health systems.

Overall, the proposed blockchain-based framework addresses critical vulnerabilities in current hospital information systems by establishing a secure, transparent, and scalable model for healthcare data management. By fostering both technical robustness and user-cantered design, this approach holds substantial promise for the future of secure digital healthcare infrastructures and can serve as a foundational component in the evolution of smart, regulated, and interoperable health ecosystems.

References

[1] D. Elangovan, C. S. Long, F. S. Bakrin, C. S. Tan, K. W. Goh, Z. Hussain, and L. C. Ming, "Application of blockchain technology in hospital information system," in Mathematical Modeling and Soft Computing in Epidemiology, 2020, pp. 231–246. eBook ISBN 9781003038399.

[2] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity," in Proc. 2020 IEEE Int. Conf. Informatics, IoT, and Enabling Technologies (ICIoT), 2020, pp. 310–317, doi: 10.1109/ICIoT48696.2020.9089570.

[3] M. Zarour et al., "Ensuring data integrity of healthcare information in the era of digital health," Healthcare Technol. Lett., vol. 8, no. 3, pp. 66–77, 2021, doi: 10.1049/htl2.12008.

[4] A. Ibor, E. Edim, and A. Ojugo, "Secure health information system with blockchain technology," J. Niger. Soc. Phys. Sci., article 992, 2023, doi: 10.46481/jnsps.2023.992.

[5] N. Al-Yateem, L. Ismail, and M. Ahmad, "A comprehensive analysis on semiconductor devices and circuits," Prog. Electron. Commun. Eng., vol. 2, no. 1, pp. 1–15, 2024, doi: 10.31838/PECE/02.01.01.

[6] N. Sharma and R. Rohilla, "Blockchain based electronic health record management system for data integrity," in Proc. Int. Conf. Computational Intelligence (ICCI 2020), Singapore: Springer, 2021, pp. 289–297, doi: 10.1007/978-981-16-3802-2_24.

[7] R. Mnyawi, C. Kombe, A. Sam, and D. Nyambo, "Blockchain-based data storage security architecture for e-health care systems: A case of Government of Tanzania hospital management information system," Int. J. Comput. Sci. Netw. Secur., vol. 22, no. 3, pp. 364–374, 2022, doi: 10.22937/IJCSNS.2022.22.3.46.

[8] M. Mirabi and A. Gouda, "Carbon nanotube and 2D material-enabled nanoelectronics for next-generation high-performance circuits," *Natl. J. Electr. Electron. Autom. Technol. (NJEEAT)*, vol. 1, no. 4, pp. 9–19, Aug. 2025, doi: 10.17051/JEEAT/01.04.02.

[9] E. P. Adeghe, C. A. Okolo, and O. T. Ojeyinka, "Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes," Open Access Res. J. Sci. Technol., vol. 10, no. 2, pp. 013–020, 2024, doi: 10.53022/oarjst.2024.10.2.0044.

[10] B. Vincentelli and K. R. Schaumont, "A review of security protocols for embedded systems in critical infrastructure," SCCTS J. Embedded Syst. Des. Appl., vol. 2, no. 1, pp. 1–11, 2025.

[11] M. Attaran, "Blockchain technology in healthcare: Challenges and opportunities," Int. J. Healthc. Manag., vol. 15, no. 1, pp. 70–83, 2022, doi: 10.1080/20479700.2020.1843887.

[12] A. K. Tyagi and R. Seranmadevi, "Blockchain for enhancing security and privacy in the smart healthcare," in Digital Twin and Blockchain for Smart Cities, 2024, pp. 343–370, doi: 10.1002/9781394303564.ch16.

[13] J. Kiruthika, V. Poovizhi, P. Kiruthika, E. E., and P. Narmatha, "Blockchain based unforged license," *Int. J. Commun. Comput. Technol.*, vol. 7, no. 2, pp. 4–7, 2023.
[14] M. Johanne, A. Magnus, I. Sofie, and H. Alexander, "IoT-based smart grid systems: New advancement on wireless sensor network integration," J. Wireless Sensor Netw. IoT, vol. 2, no. 2, pp. 1–10, 2025.
[15] S. Guan, Y. Cao, and Y. Zhang, "Blockchain-enhanced data privacy protection and secure sharing scheme for healthcare IoT," IEEE Internet Things J., early access, 2024, doi: 10.1109/JIOT.2024.3487154.
[16] J. Ryu and T. Kim, "Enhancing hospital data security: A blockchain-based protocol for secure information sharing and recovery," Electronics, vol. 14, no. 3, p. 580, 2025, doi: 10.3390/electronics14030580.
[17] V. Leiva and C. Castro, "Artificial intelligence and blockchain in clinical trials: Enhancing data governance efficiency, integrity, and transparency," Bioanalysis, vol. 17, no. 3, pp. 161–176, 2025, doi: 10.1080/17576180.2025.2452774.
[18] Q. Geng, Z. Chuai, and J. Jin, "An integrated healthcare service system based on blockchain technologies," IEEE Trans. Comput. Soc. Syst., early access, 2024, doi: 10.1109/TCSS.2024.3392591.
[19] R. Welekar, B. Balkhande, T. Jadhav, V. Khetani, B. R. Singh, and A. Shukla, "Leveraging blockchain for enhanced data integrity and security in information systems," J. Inf. Syst. Eng. Manag. (JISEM), 2024. [Online]. Available: https://www.jisem-journal.com/
[20] J. Muralidharan, "Innovative materials for sustainable construction: A review of current research," Innov. Rev. Eng. Sci., vol. 1, no. 1, pp. 16–20, 2024, doi: 10.31838/INES/01.01.04.
[21] A. Aruna and A. Senthilselvi, "A novel approach to enhance data integrity in blockchain using cryptographic hashing," in Proc. 2024 Second Int. Conf. Advances in Information Technology (ICAIT), 2024, pp. 1–4, doi: 10.1109/ICAIT61638.2024.10690597.
[22] S. Ahmed, "Enhancing data security and transparency: The role of blockchain in decentralized systems," Int. J. Adv. Eng., Manag. Sci., vol. 11, no. 1, p. 593258, 2025, doi: 10.22161/ijaems.111.12.
[23] H. M. Rai, K. K. Shukla, L. Tightiz, and S. Padmanaban, "Enhancing data security and privacy in energy applications: Integrating IoT and blockchain technologies," Heliyon, vol. 10, no. 19, 2024. [Online]. Available: https://www.cell.com/heliyon/fulltext/S2405-8440(24)14948-1
[24] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things," Pers. Ubiquitous Comput., vol. 28, no. 1, pp. 59–72, 2024, doi: 10.1007/s00779-021-01583-8.
[25] A. Alamsyah and I. P. S. Setiawan, "Enhancing privacy and traceability of public health insurance claim system using blockchain technology," Front. Blockchain, vol. 8, 1474434, 2025, doi: 10.3389/fbloc.2025.1474434.
[26] S. Poornimadarshini and S. Veerappan, "Women's safety in public transport: Sensing, design justice, and policy interventions," *Bridge: J. Multidiscip. Explor.*, vol. 1, no. 1, pp. 53–60, 2025.
[27] S. Terzi and I. Stamelos, "Architectural solutions for improving transparency, data quality, and security in eHealth systems by designing and adding blockchain modules, while maintaining interoperability: The eHDSI network case," Health Technol., vol. 14, no. 3, pp. 451–462, 2024, doi: 10.1007/s12553-024-00833-y.
[28] J. C. da Silva, M. L. de O. Souza, and A. de Almeida, "Comparative analysis of programming models for reconfigurable hardware systems," SCCTS Trans. Reconfigurable Comput., vol. 2, no. 1, pp. 10–15, 2025.
[29] H. Taherdoost, "Exploring blockchain solutions in healthcare data management and patient data privacy," in Blockchain-Enabled Solutions for the Pharmaceutical Industry, 2025, pp. 1–18, doi: 10.1002/9781394287970.ch1.
[30] F. C. Udegbe, E. I. Nwankwo, G. T. Igwama, and J. A. Olaboye, "Integration of blockchain technology in biomedical diagnostics: Ensuring data security and privacy in infectious disease surveillance," Eng. Sci. Technol. J., vol. 3, no. 2, 2024, doi: 10.51594/estj.v3i2.1524.
[31] R. Kamal, E. E. D. Hemdan, and N. El-Fishway, "Care4U: Integrated healthcare systems based on blockchain," Blockchain: Res. Appl., vol. 4, no. 4, 100151, 2023, doi: 10.1016/j.bcra.2023.100151.
[32] A. Priyadharshini, S. Nithiya, H. A. Archana, and S. C. B. Jaganathan, "Intelligent patient monitoring through hybrid consensus algorithm based blockchain technology," Multimedia Tools Appl., pp. 1–22, 2024, doi: 10.1007/s11042-024-19840-2.
[33] M. Farhan, "Empowering healthcare: Symbiotic innovations of AI and blockchain technology," in Blockchain and AI, CRC Press, 2024, pp. 23–57. eBook ISBN 9781003162018.
[34] B. Singh and C. Kaunert, "Reinventing artificial intelligence and blockchain for preserving medical data," in Ethical Artificial Intelligence in Power Electronics, CRC Press, 2024, pp. 77–91. eBook ISBN 9781032648323.
[35] M. N. Triet et al., "Enhanced security for animal health records using RSA-encrypted NFTs on the blockchain," in Int. Conf. Mobile Web and Intelligent Information Systems, Cham, Switzerland: Springer, 2024, pp. 100–113, doi: 10.1007/978-3-031-68005-2_8.
[36] K. S. Hyun, P. J. Min, and L. H. Won, "AI hardware accelerators: Architectures and implementation strategies," J. Integr. VLSI, Embedded Comput. Technol., vol. 2, no. 1, pp. 8–19, 2025, doi: 10.31838/JIVCT/02.01.02.
[37] V. Kurnala, "Enhancing healthcare data security through blockchain-enhanced IDPS and multi-layered firewall system," in Proc. 2024 3rd Int. Conf. Advancement in Technology (ICONAT), 2024, pp. 1–7, doi: 10.1109/ICONAT61936.2024.10775003.
[38] G. Cruz, T. Guimarães, M. F. Santos, and J. Machado, "Decentralize healthcare marketplace," Procedia Comput. Sci., vol. 231, pp. 439–444, 2024, doi: 10.1016/j.procs.2023.12.231.
[39] R. Salama and F. Al-Turjman, "A study of health-care data security in smart cities and the global value chain using AI and blockchain," in Smart Global Value Chain, CRC Press, 2024, pp. 165–172. eBook ISBN 9781003461432.
[40] M. M. Rahman, "Ethical and technological convergence: AI and blockchain in halal healthcare," in Artificial Intelligence-Enabled Blockchain Technology and Digital Twin for Smart Hospitals, 2024, pp. 451–466, doi: 10.1002/9781394287420.ch23.
[41] A. Tiwari, A. Sikri, V. Sagar, and R. Jameel, "Decentralized technology and blockchain in healthcare administration," in Blockchain Transformations: Navigating the Decentralized Protocols Era, Cham, Switzerland: Springer, 2024, pp. 229–237, doi: 10.1007/978-3-031-49593-9_14.