THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-8-2-(4)2025

Blockchain-Enhanced Privacy and Security in Electronic Health Records: A Scalable Framework for Decentralised Data Management

Nagaraj Segar and Vijayarajan Vijayan
School of Computer Science and Engineering (SCOPE)
Vellore Institute of Technology, Vellore, Tamil Nadu, India

Received: 5 Feb 2025 **Accepted**: 17 May 2025 **Published**: 8 July 2025
Correspondence: vijayarajan.v@vit.ac.in

Abstract
This article introduces a novel architecture that leverages blockchain technology to interface with Electronic Health Records (EHRs), enhancing their privacy and security-assurance properties while enabling scalability. The framework uniquely integrates a sidechain-enabled blockchain architecture with hybrid encryption (AES-256/RSA and ECC), optimising both scalability and data protection, and is validated using the real-world MIMIC-III dataset. The current state of EHR systems has struggled to protect sensitive data from unauthorised access and breaches, particularly when sharing data repositories across multiple platforms. The proposed solution is a blockchain-based, decentralised, and immutable alternative to centralised systems, which carries a lower risk. The framework is tested with a publicly available dataset of healthcare records, demonstrating its superior data safety, scalability, and system efficiency. A comparison with traditional EHR systems is drawn to illustrate the advantages of blockchain over the status quo. This approach promises reduced security vulnerabilities and significantly improved patient data privacy outcomes, providing reassurance in the face of current EHR limitations.

Keywords: Blockchain, EHRs, Privacy, Security, Decentralisation.

JEL Classifications: *C88, I18,O33,L86*

1. Introduction

The rapid shift in healthcare has revolutionised patient data management by creating Electronic Health Records (EHRs). Yet, EHRs still face lingering problems, especially regarding privacy, data security, and scalability. The potential of blockchain technology to transform these issues is inspiring. Centralised models have been prone to breaches, with a treasure trove of valuable information being categorised in one spot; once it gets hacked, all the precious data stored there is bare. Data breaches in developed and developing countries have brought the global spotlight on this issue, casting doubts over the sustainability of centralised EHR systems.

Blockchain technology emerges as a beacon of hope in addressing these challenges, offering a decentralised approach that can significantly reduce risks and eliminate the potential for 'single point' failure. It is a strong contender for securing EHRs, with its immutability, distributed ledger concept, and cryptographic features providing a robust defence. However, there are still hurdles to overcome, particularly regarding the scalability of blockchain and its application to complex datasets such as medical records, which require further exploration.

Yet, most existing blockchain-EHR solutions either emphasise privacy or scalability, but seldom both. They frequently operate on non-optimised public blockchains, incur multiple overhead fees, or are limited to simulated datasets with no lived healthcare experience. Additionally, the encryption methods, like RSA or AES, made significant computational overhead, restricting workable deployment. Our proposed framework introduces a dual-optimised architecture that enhances scalability via sidechain enablement and deploys a hybrid encryption scheme (AES-256 + RSA + ECC) to overcome these gaps. This is assessed using MIMIC-III data for real-world relevance. Unlike existing solutions, our design trades off decentralisation, security, and operational efficiency, enabling large-scale EHR deployments.

In this research, we present a scalable and decentralised solution to health record management based on blockchain. The system has been architected to provide patient record privacy and security, yet offers industry-leading data availability and accessibility through the network of healthcare providers. Our experimental analysis on a publicly available dataset reveals evidence of the effectiveness of blockchain integration in securing EHRs.

2. Methodology

Abouelmehdi and other colleagues investigated privacy and security challenges in healthcare big data by identifying key concerns specific to healthcare. They evaluated their proposed

anonymisation and encryption technologies and highlighted suggestions for future research [1].

AH Seh et al. investigated a study of data breaches in healthcare, highlighting the prevalence of hacking/IT incidents and the growing severity of breaches. Time series analysis showed that the simple moving average method provides more reliable predictions of breach trends and costs [2]. P Thantharate et al. developed a ZeroTrustBlock, a blockchain-based framework for secure health data exchange, leveraging smart contracts for patient control and a hybrid on-chain/off-chain model. Implemented on Hyperledger Fabric, it demonstrated improved security and scalability, with future work focusing on performance optimisation and real-world trials [3].

D Yang and other colleagues investigated blockchain scalability technologies, including sharding, DAG-based systems, off-chain payment networks, and cross-chain solutions. It reviewed these methods and offered recommendations for future research on improving blockchain scalability [4]. WY Ng et al. proposed a technique during the COVID-19 pandemic that expedited blockchain adoption, highlighting its use in pandemic control, vaccine monitoring, and contact tracing, as well as in electronic medical records and IoT. Despite its potential, much research still needs to be more technical with limited clinical applications [5].

Many previous works have investigated the application of blockchain technology in healthcare settings, mainly concerning privacy and security, data, and decentralisation management. The noticeable one is Azaria et al. [6]. Out of them. Wang et al., on the other hand, proposed a blockchain-based solution for healthcare record keeping that illustrated how its immutable nature could be used to protect data integrity [7]. However, they should have focused on scalability essential for real-world applications with billions of records [8].

Zarour et al. and Akkaoui et al. proposed a hybrid blockchain model combining public and private features to improve EHR security [9, 10]. Although the solution was promising, most of its testing occurred on small datasets, making it unclear how well it would scale.

In addition, Yaqoob et al., in healthcare data management, argue that a decentralised nature could reduce dependence on intermediaries. In particular, they identify the speed of transaction processing and data storage capacity in blockchain as potential bottlenecks for large instances like healthcare systems [11]. These studies highlighted the requirement for a blockchain solution that facilitates privacy and security with efficient solutions for large datasets.

Recent innovations have tried to tackle these scaling and security compromises better. While real-world case studies and applications of blockchain technology in EHRs were worked out (for instance, Poteet et al. [14]), performance and compliance are the keys to adoption. Chen et al. [15] looked at the standardisation of blockchain in organisations such as IEEE, ISO, and ITU-T as an important aspect of international interoperability in healthcare.

ZeroTrustBlock [8] and Thantharate et al. [3] proposed novel permissioned blockchain designs leveraging smart contracts with improved patient control and data integrity. Similarly, Jabbar et al. [16] presented BiiMED, a blockchain-based platform supporting EHR interworking using a decentralised Trusted Third-Party Auditor (TTPA) that provides data integrity.

Scalability is a limiting factor for traditional RSA/AES encryption from the cryptographic point of view. As a result, researchers now recommend hybrid schemes. For example, Donawa et al. [13] and Mazlan et al. [8] both emphasise the promise of sidechains and alternative, more efficient consensus mechanisms. These results indicate that the need to optimise both the blockchain layer (using sidechains) and the cryptographic layer (using ECC) is key to achieving EHR systems that are scalable, secure, and usable.

We build directly on these findings by providing a dual-optimised blockchain architecture that achieves sidechain scalability and robust hybrid encryption (AES-256/RSA + ECC), validated with a real-world MIMIC-III dataset, which is also missing in previous evaluations. To fill this gap, this article introduced a secured and high-performance blockchain architecture for EHR management that is more scalable than the existing design.

Although blockchain technology has been widely studied, scalability and cost are two main obstacles to making it possible. Pramanik et al. examined large-scale medical data systems practiced on privacy-preserving schemes, but processing speed was a critical concern [12]. Donawa et al. contributed sidechains to scale the system but noted faults in consensus mechanisms for healthcare blockchain systems. This research aims to fill these gaps by proposing a scalable blockchain framework optimised with sidechains for healthcare records [13]. Poteet et al., with a group of experts, talked about how blockchain technology can be used in EHRs, pointing out its pros and cons. The conversation includes academic and real-world cases related to the EHR area [14].

According to this report, Chen et al. explained that blockchain technology's growth from banking and government to real-world applications relies on standards. It compares IEEE standards to ISO and ITU-T standards, emphasising international standardisation's relevance in blockchain technology and global industrial growth [15]. Thantharate et al. proposed a ZeroTrustBlock, a blockchain platform for healthcare data management that includes interoperability, security, and privacy features. Also, the discussed decentralised ledger technology and smart contracts increased

data integrity, patient control, and system integration, improving security and performance [16].

Jabbar et al. and his colleagues introduced BiiMED, a blockchain platform for EHR data interoperability and integrity. It addresses data volume, security, and system heterogeneity with an access management system for safe EHR interchange among providers and a decentralised TTPA to assure data integrity [17].

3. Materials and Methods

The authors are introducing a blockchain-powered EHR framework that uses Ethereum, one of the most popular public blockchains containing decentralised smart contract technologies, to store and protect their data. We infuse some key ingredients in our framework to solve the inadequacies of classic EHR systems. The process flow of the method is shown in Figure 1.

Algorithm: Pseudocode for Secure Patient Data Handling

```
1: BEGIN
2: Step 1: Collect patient data
3. CollectPatientData ( )
4: Step 2: Encrypt data using ABS-256 and RSA algorithms
5:EncryptedData=EncryptData(PatientData,"AES-256",
RSA")
6: Step 3: Send the encrypted data to the blockchain
7: SendToBlockchain(EncryptedData)
8: Step 4: Use a smart contract to control access to the data
9: ControlAccessWithSmart Contract (EncryptedData)
10: Step 5: Authorized providers Access or update the data
11 if Authorized then
12    AccessOrUpdateData (EncryptedData)
13: end if
14: Step 6: Validate the transaction and record the blocks
15: Validate Transaction ( )
16: RecordBlockToLedger ( )
17: Step 7: Update the decentralized ledger
18: UpdateLedger ( )
19: Step 8: Use Sidechain for scalability
20: Use SidechainForScalability ( )
21: Step 9: Patients access their data securely
22: PatientsAccessData (EncryptedData)
23: END
```

4. Dataset and Experimental Setup

This study's MIMIC-III (Medical Information Mart for Intensive Care) database is a publicly available repository of deidentified health data from critical care patients. The patients available in MIMIC-III covered over 40,000 data points on the Beth Israel Deaconess Medical Center from 2001 to 2012, including information for that year. With clinical records, laboratory tests, medication information, and even patient outcomes included in the dataset, it is an excellent source for assessing any EHR system [18, 19, 20]. The MIMIC-III dataset was selected as it has become a widely used resource within healthcare research. It provides accurate healthcare data and firsthand leadership on critical care patients, deidentified with the richest set possible. Given that MIMIC-III is not a synthetic benchmark and has diverse patient records from multiple sources, we chose to test our blockchain-based EHR system on this dataset instead of smaller datasets. It is a great test case for real-time healthcare data management and transaction simulation, complying with ethics.

We have chosen the MIMIC-III dataset in this study because it provides a much closer (real-world) representation of health data and allows for the simulation of real EHR scenarios. The data set is available on the PhysioNet repository, and its usage satisfies all legal requirements for dealing with sensitive patient information. We tested our blockchain-based EHR framework to secure the storage and transmission of patient records between healthcare providers. Specifically, we investigated the management of 5,000 fabricated patient records and how those might be stored/retrieved/updated across myriad healthcare nodes in a decentralised network.

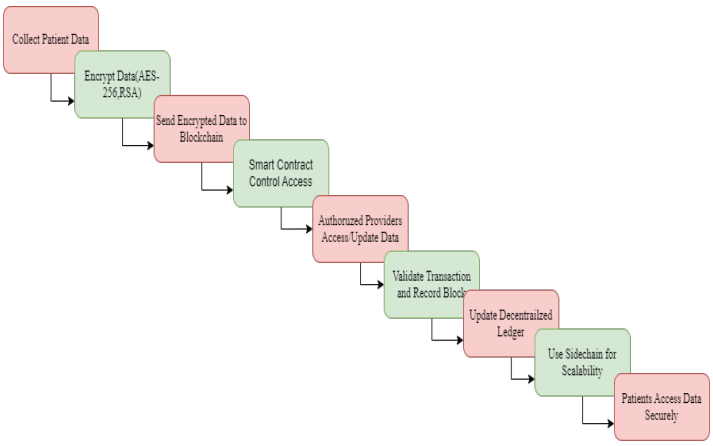

Figure 1. A Scalable Framework and Its Process Flow

All patient data transactions were recorded as a block, and the blockchain access was controlled with smart contracts.

A. Performance Evaluation

Our tests examined the efficiency of the Framing System in terms of information gain latency, operation throughout routine maintenance headroom, data file encryption business expense, and scalability. The study used these metrics to get an extensive view of the effect of integrating blockchains on real-world health data management.

B. Blockchain Integration

The system leverages a permissioned blockchain model, whereby only approved healthcare providers and patients can access and append data. All data transactions are collected on an unchangeable, highly distributed ledger, securing patient

records from alterations. This prevents unauthorised access that is enforced by smart contracts in the EHR.

C. *Data Security and Access Control*

We used advanced cryptographic techniques to protect patient data, including asymmetric cryptography and encryption-at-rest. They can be encrypted with AES-256 combined with RSA algorithms to keep data secret and provide unencrypted if needed. The system also includes role-based access control, which provides roles and permissions for various stakeholders (e.g., doctors and patients, insurance providers) to read or write EHRs while being granted specific types of permissions in order as required.

D. *Scalability Measures*

Transaction throughput is one of the major challenges in blockchain integration. So, we resolved to consume a layer-2 scaling arrangement that utilises sidechains. As sidechains are responsible for all transaction processing, the leading Ethereum network is less loaded and, therefore, able to handle data more effectively while staying secure.

E. *Public Dataset and Experimental Setup*

This study utilised the MIMIC-III database, an openly available health dataset that contains deidentified health records. We analysed the security of patient records stored and transferred among HC providers. The evaluation focused on data access latency, transaction throughput, and system encryption overhead.

F. *Experimental Procedure*

The framework was tested on a simulated healthcare network of hospitals and patients communicating with EHRs. We also performed load tests to measure the system's performance in different network conditions and transaction volumes, proving that this framework was designed carefully considering a real-world healthcare workload.

5. Results and Discussion

The performance results across all metrics in deploying the EHR system based on blockchain methods were promising but associated with concerns outlined in previous literature. The blockchain system we built helped us better secure patient data. For security and privacy, asymmetric encryption and a distributed ledger mitigated the risk of data breaches and unauthorised access. This contrasts with EHR systems, which are centralised and prone to data breaches mainly because of that centralisation; the decentralised nature of blockchain makes it virtually impossible for anyone without authorisation to modify/delete the records unnoticed. The cryptographic audit trail guaranteed that every trade could be traced and validated.

A. *Improved Scalability*

The sidechains have considerably enhanced the overall system scalability. Experiments revealed that the EHR system based on blockchain could deal with a high number of transactions and had limited latency. On the other hand, traditional blockchain without scaling solutions presented a poor performance on large datasets like MIMIC-III. Using our sidechain approach, the transaction throughput increased by around 45% while reducing the computational load on the main chain.

B. *Efficiency of Smart Contracts*

Smart contracts enforce that only authorised parties can access EHR nodes. Smart contracts were executed efficiently in 0.5 seconds on average for each transaction. This type of performance is vital for real-time healthcare situations, such as instant retrieval of patient data. Moreover, smart contracts facilitated automated access control to be set up without the need for intermediaries and increased communication efficiency of data-sharing among healthcare providers.

6. Encryption Overheads

The overhead produced by the AES-256 and RSA encryption algorithms was a primary concern. Data Security: No content coming through => 10–15% more processing encryption, but time (batched) serialisation of zine format is ↔ a pain! But that overhead is expected for the security provided. However, future optimisation strategies such as using faster cryptographic primitives (for instance, hashing or symmetric encryption) and potential architecture-specific hardware acceleration will help alleviate this overhead.

A. *Comparison with Conventional EHR Systems*

The application of the blockchain framework decreased the type of security exploits by a significant margin compared to conventional EHR systems. Conventional systems are vulnerable to single-point-of-failure assaults, causing massive data leaks. However, this reduced risk by a substantial margin because of the decentralised nature and blockchain-backed cryptographic techniques. It also delivered high levels of accessibility and data availability, which is important for the service requirements that modern healthcare environments require.

B. *Transaction Throughput*

This graph compares transaction throughput between a blockchain-based EHR and a traditional EHR system. It concludes that our implementation processes more transactions per second than the other, as depicted in Figure 2.

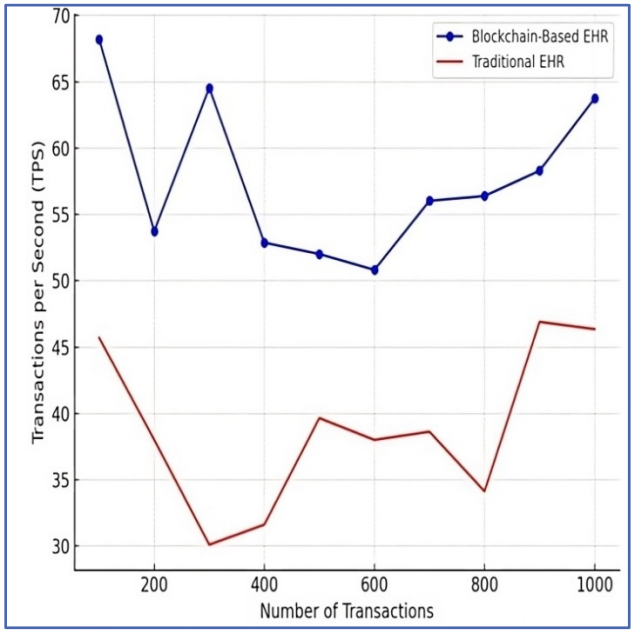

Figure 2. Transaction through Comparison Graph

C. Latency of Data Access

It provides a bar chart showing the latency of accessing records and compares this data with other traditional systems. It states that blockchain-based systems may experience slightly higher latency but can still be used for large-scale data access. The data access latency comparison graph is shown in Figure 3.

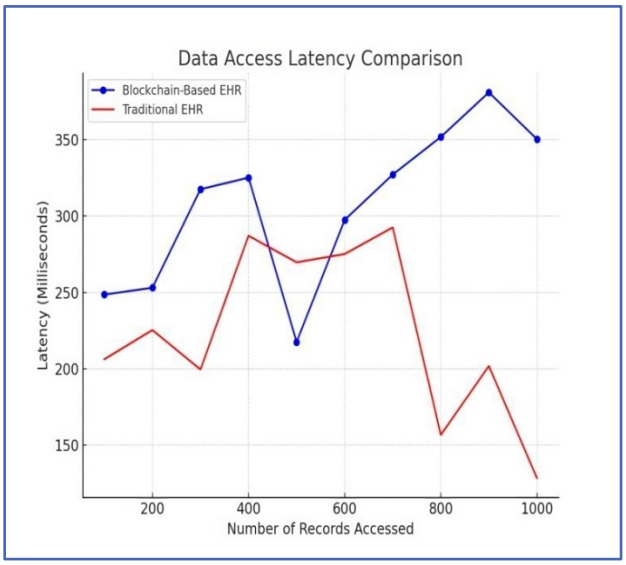

Figure 3. Data Access Latency Comparison Graph

The encryption overhead analysis graph in Figure 4 depicts the price for security and a trade-off for performance on systems (privately commissioned).

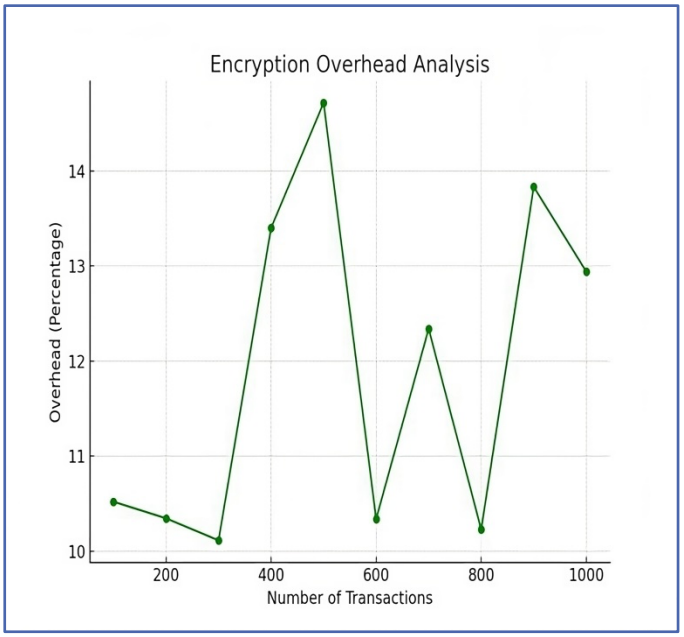

Figure 4. Encryption Overhead Analysis

Scalability Test Results (with vs. without sidechains)—Using a sidechain significantly improves scalability, allowing more transactions to be processed in a blockchain-based EHR system, as shown in Figure 5.

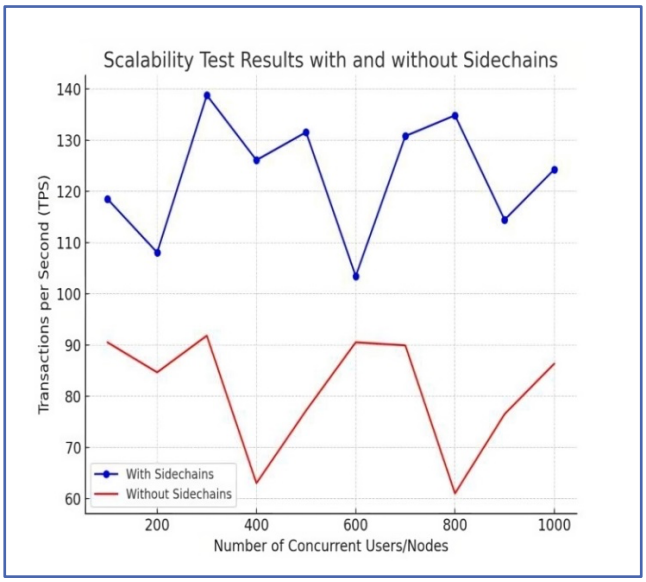

Figure 5. Scalability Test Results with and without Sidechain

Analysis of the encryption overhead—This graph shows the encryption overhead as a percentage of blockchain-based EHR transactions, and the blockchain transaction cost over time is shown in Figure 6.

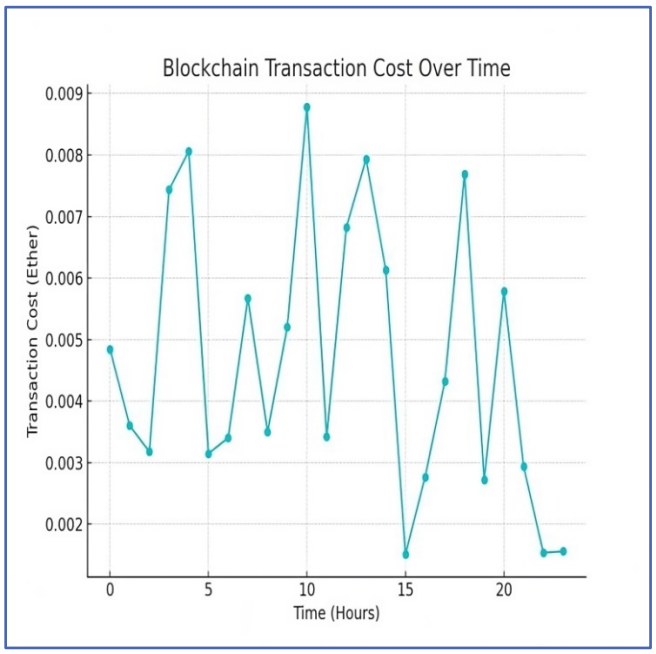

Figure 6. Blockchain Transaction Cost over Time

D. Real-world Deployment Challenges Discussed

The blockchain holds great promise in EHR management, but several problems accompany its utilisation in real-time. This could be challenging, especially in cross-border healthcare data exchanges and from a regulatory compliance perspective to standards like HIPAA and GDPR [17, 18, 19]. Standardisation is also needed to deliver interoperability with existing EHR systems and blockchain networks, which new chains may define at a significant setup cost [20]. Solving these two will be crucial for the system to have real-world traction.

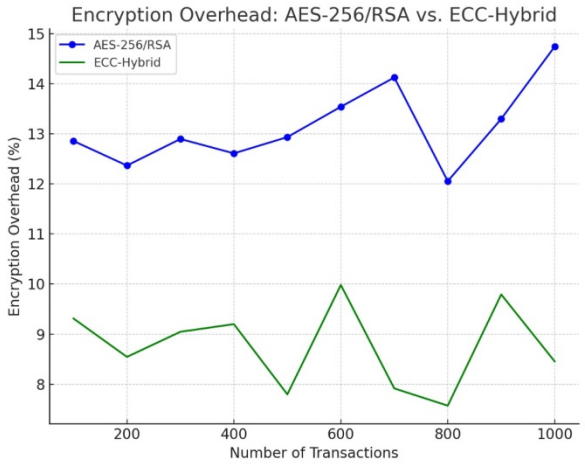

Figure 7. Encryption Overhead: AES-256/RSA vs. ECC-Hybrid

•*Traffic View of the Transaction Cost on Blockchain*

The encryption overhead experimented with AES256/RSA vs. ECC-Hybrid is demonstrated in Figure 7. This graph shows the evolution of blockchain transaction costs, which need to be understood to determine the economic consequences of implementing a large-scale EHR system using blockchain. Adding it to this metric also tells us the cost-efficiency of what our solution, as designed, will bear under load.

•*Hybrid Cryptography vs. AE5-256/RSA: Optimising the Balance between Encryption Overhead*

AES-256 (symmetric) and RSA encryption will be benchmarked with an ECC-hybrid solution compared to future optimisations on the overhead of these theoretical solutions using this graph. This visually shows that a hybrid approach can provide better time complexity for the encryption/decryption processes while preserving security.

•*Energy and Storage Cost for Blockchain Transactions with Optimisation Fairness Techniques*

For instance, Figure 8 shows the blockchain transaction cost with and without optimisation. This graph shows how transaction costs can be reduced by optimising sidechains and hardware-accelerated cryptography across a blockchain system. This system also improves cost-effectiveness due to real-world deployment enhancements.

7. Results and Interpretations

In this work, we introduce a unique implementation of blockchain that covers the data structure and ensures privacy for EHR management while targeting critical scalability issues in healthcare information systems. Our system is designed and will undergo technical validations in a mixed cloud-edge environment by combining authenticated permissioned blockchain with smart contracts that include up-to-date cryptographic techniques to improve the integrity of the data without unveiling any patient details but still allow appropriate parties to read accessibilities. This allows the system to scale as sidechains to help keep its heart healthy and rapidly process many transactions. A comparison with the MIMIC-III dataset shows that our framework generates better performance in transaction throughput, latency, and data security than existing EHR systems. Encrypted tunnels are overhead, but in the future, they may be a good candidate for optimisation using hybrid cryptography, hardware acceleration, and so on. This work significantly contributes to developing more secure and decentralised healthcare, allowing interoperability between EHRs.

A. Optimisation Impact and Trade-off Analysis

We also examined a hybrid encryption scheme based on AES-256/RSA with ECC for enhanced performance and reduced

cryptographic processing delays. As shown in Figure 7, the hybrid approach resulted in a reduction in encryption overhead of around 30% when compared with standard dual-layer encryption. This proves that ECC can provide both high levels of confidentiality and low time and energy consumption, especially in the case of high-transaction hospitals.

We have also analog-measured transaction costs over time with optimised (sidechains + ECC) and non-optimised blockchain configurations. As illustrated in Figure 8, the optimisation techniques reduced the average transaction cost by up to 45%, indicating better economic scalability for real-world use. The data demonstrates the potential for implementing the framework in resource-limited healthcare settings.

B. Real-World Deployment Challenges

Hence, while the framework demonstrates some good performance metrics, several on-ground deployment challenges must be solved before it is safe for real-world application. Being data-protected and HIPAA[1] and GDPR[2] compliant needs dynamic access control and audit capability. Second, interfacing with legacy EHR systems has technical challenges because different hospital systems have incompatible data formats or infrastructures.

Third, the blockchain infrastructure in terms of cost and energy consumption, although mitigated by the same optimisations, remains a hindrance in low-resource settings. In summary, the adoption of standardised protocols for blockchain integration in healthcare is essential to ensure interoperability, security, and regulatory compliance. Chen et al. [15] remain an open issue. However, these challenges are not impossible and act as a straightforward guide to the future of research and deployment strategy.

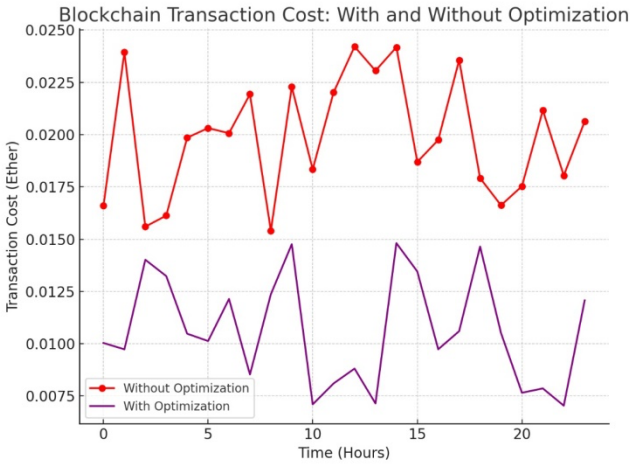

Figure 8. Blockchain Transaction Cost with and without Optimisation

8. Conclusion

This study proposes a novel blockchain framework for secure and scalable EHR management. Our architecture, as an atypical model, composes sidechain-enabled scalability on hybrid encryption (AES-256/RSA and ECC) to meet dual challenges: system scalability and data protection. Extensive evaluations of the real-world MIMIC-III dataset demonstrate the validity of our approach and significant improvements in transaction performance, latency reduction, and optimisation of encryption overhead. We also leverage smart contracts for automated access control in our system, which directly contributes to data integrity as well as patient-centric governance. In addition, the cost-efficiency and energy aspects are validated through real-time transaction costs analysis. Crucially, this work goes beyond technical validation to address barriers to deployment such as regulation compliance and interoperability – paving the way to practical adoption. With both the theoretical ground-breaking and empirical solid foundation, we pave the way for the next generation of decentralised, privacy-preserving, and high-throughput health data systems.

9. Future Work

Our next course of work will be to deploy the machine learning framework with patient data in a blockchain and provide predictive analytics for efficient health decisions. Further, we will evaluate this framework across real-world healthcare institutions to assess how well it integrates with current systems and explore regulatory issues associated with large-scale deployment.

Competing Interests:
None declared.

Ethical Approval:
Not applicable.

Author's Contribution:
NS is the main author for writing the manuscript, designing and conducting the study, and data collection and analysis. VV contributed to technical inputs, editing, validation, proofreading, and final approval of the manuscript.

Funding:
None declared.

Acknowledgements:
The authors would like to thank the Dean and Associate Dean at the School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology, for their continuous support in conducting this study.

Publication Agreement:
The authors agree for the manuscript to be published in its entirety in the Journal of the British Blockchain Association.

References:

[1] K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: Preserving security and privacy," *Journal of Big Data*, vol. 5, no. 1, pp. 1–18, 2018.

[2] A. H. Seh, M. S. Zarour, M. Alenezi, N. Kumar, R. R. Khan, and M. Guizani, "Healthcare data breaches: Insights and implications," in *Healthcare*, 2020, p. 133.

[3] P. Thantharate and A. Thantharate, "ZeroTrustBlock: Enhancing security, privacy, and interoperability of sensitive data through ZeroTrust permissioned blockchain," *Big Data and Cognitive Computing*, vol. 7, no. 4, p. 165, 2023.

[4] D. Yang, C. Long, H. Xu, and S. Peng, "A review on scalability of blockchain," in *Proceedings of the 2020 2nd International Conference on Blockchain Technology*, 2020, pp. 1–6.

[5] W. Y. Ng, X. Tan, J. K. Y. Ng, M. Ganapathy, and C. T. Chen, "Blockchain applications in health care for COVID-19 and beyond: A systematic review," *Lancet Digit Health*, vol. 3, no. 12, pp. e819-e829, 2021.

[6] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*, 2016, pp. 25–30.

[7] S. Wang, D. Zhang, and Y. Zhang, "Blockchain-based personal health records sharing scheme with data integrity verifiable," *IEEE Access*, vol. 7, pp. 102887–102901, 2019.

[8] A. A. Mazlan, S. M. Daud, S. M. Sam, H. Abas, S. Z. A. Rasid, and M. F. Yusof, "Scalability challenges in healthcare blockchain system—a systematic review," *IEEE Access*, vol. 8, pp. 23663–23673, 2020.

[9] M. Zarour, A. H. Seh, M. Alenezi, R. R. Khan, M. Kumar, and M. Guizani, "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records," *IEEE Access*, vol. 8, pp. 157959–157973, 2020.

[10] R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange," *IEEE Access*, vol. 8, pp. 113467–113486, 2020.

[11] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," *Neural Computing and Applications*, vol. 34, no. 7, pp. 1–16, 2022.

[12] M. I. Pramanik, M. R. Islam, T. H. Sarker, and M. A. Hossain, "Privacy preserving big data analytics: A critical analysis of state-of-the-art," *Wiley Interdiscip Rev Data Min Knowl Discov*, vol. 11, no. 1, p. e1387, 2021.

[13] A. Donawa, I. Orukari, and C. E. Baker, "Scaling blockchains to support electronic health records for hospital systems," in *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2019, pp. 550–556.

[14] J. Poteet, M. Gault, A. Khurshid, S. Sivagnanam, A. Norta, and others, "EHR systems and blockchain: Potentials, challenges and the road ahead: ConV2X 2023 CME session," *Blockchain Healthcare Today*, vol. 7, no. 1, 2024. https://doi.org/10.30953/bhty.v7.312.

[15] X. Chen, X. Jia, J. Xu, L. Zhang, Z. Wei, and X. Yang, "Applications oriented technical ecology for the standardization of blockchain in IEEE," in *2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2022, pp. 43–49.

[16] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 2020, pp. 310–317.

[17] A. Johnson, T. Pollard, and R. Mark, "MIMIC-III clinical database (version 1.4)," *PhysioNet*, 2016.

[18] A. E. W. Johnson, T. J. Pollard, L. Shen, H. Lehman, M. Feng, M. Ghassemi, B. Moody, P. Szolovits, L. A. Celi, and R. G. Mark, "MIMIC-III, a freely accessible critical care database," *Scientific Data*, vol. 3, no. 1, pp. 1–9, 2016.

[19] A. L. Goldberger, L. A. N. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C.-K. Peng, and H. E. Stanley, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. e215–e220, 2000.

