iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78888

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

A Consortium Blockchain Framework for Decentralized Identity Management and Fine-Grained Access Control in Healthcare Information Systems

Rinee Chaudhary[1], Sushil Kumar Sharma[2]
[1]*Research Scholar, Department of Computer Science and Engineering, Institute of Technology and Management Aligarh University: Aktu , Lucknow*
[2]*Assistant Professor, Department of Computer Science and Engineering, Institute of Technology and Management Aligarh University: Aktu , Lucknow*

Abstract: ***Centralized Electronic Health Record (EHR) systems have brought with them a myriad of challenges to healthcare in the world today, which have high points of failure, diminished patient autonomy, and do not easily adjust to up-to-date regulatory standards. This essay suggests and analyses a new blockchain-based consortium that can be called HealthChain to manage the decentralization of digital identity and access control in healthcare information systems with granulated fine-grained access control. The structure combines the W3C-conformant Decentralized Identifiers (DID), Verifiable Credentials (VC) and Attribute-Based Access Control (ABAC) smart contracts running on a permissioned Ethereum network with Proof of Authority (PoA) consensus. Electronic Health Records are encrypted using the AES-256-GCM and are stored off-chain using the InterPlanetary File System (IPFS) where only the cryptographic content identifiers are stored on-chain. An initial prototype was built and tested on five simulation nodes archetyping a regional healthcare consortium: proof-of-concept. Sub-200 ms transaction latency is proven by experimental results on 30 independent trials on all critical operations, 156 ms on access requests, and 134 ms on emergency access. The success rates of IPFS in retrieving EHR files are more than 99.5 percent regardless of file sizes. Sources Usability testing with 45 users yield over 94 percent task completion among all user groups. The system has complete compliance with the HIPAA Security Rule and offers a workable architectural solution to the GDPR right-to-erasure dilemma using pseudonymous on-chain identifiers. A comparative analysis can verify that HealthChain is more effective than centralized EHR systems, federated Health Information Exchanges, and public blockchain substitutes in the patient control area, audit immutability, privacy protection, and regulatory compliance without experiencing any significant impact on clinically acceptable performance.***

Keywords: Blockchain, Healthcare, Access Control, Decentralized Identity, EHR, Smart Contracts, IPFS, ABAC, Self-Sovereign Identity, HIPAA, GDPR, Consortium Blockchain

I. INTRODUCTION

Digitization of the healthcare sector has fundamentally changed clinical practice with Electronic Health Records (EHRs) allowing evidence-based decision-making and coordination of care across providers [18, 19]. Nevertheless, such transformation has also revealed structural weaknesses that are deep rooted. The current healthcare information systems are highly centralized, with the institutional silos controlling sensitive patient information. This architecture establishes single points of failure, blocks patient agency, hinders cross-institutional interoperability and can hardly meet changing regulatory requirements under HIPAA [24] and GDPR [25].

The magnitude of the issue is high. Large-scale data breaches such as the case of Anthem that affected 78 million patient records show that centralized health data repositories are high-value and high-danger targets [26]. Patients can barely see who gets access to their records, and there is no system to audit the use of the data, in addition to limited capability to withdraw the access once given. These shortcomings are not only security failures but also the breach of ethical standards of informed consent and patient autonomy.

©IJRASET: All Rights are Reserved

The technology of blockchain was introduced by Nakamoto [1], and it brought a paradigm change by its qualities of immutability, decentralization, and open auditability. More applications of blockchain are self-sovereign identity (SSI) structures [13, 14] and automated policy enforcement with smart contracts [4]. Attribute-Based Access Control (ABAC) [17] offers the fineness of decision-making on access to healthcare in a dynamic setting. Earlier projects such as MedRec [5] and FHIRChain [6] have also shown the potential of blockchain in healthcare use but lack patient-controlled identity, a full performance assessment, and regulatory compliance inspection.

This paper makes the following contributions:

1) HealthChain: a complete four-layer consortium blockchain architecture integrating DIDs [27], VCs [28], ABAC smart contracts, and IPFS off-chain storage, designed specifically for healthcare regulatory environments.

2) A formally specified access control model with smart contracts that enforce fine-grained, attribute-driven policies without requiring a central administrator.

3) Comprehensive experimental evaluation across performance, security, usability, and regulatory compliance dimensions, with statistical validation over 30 independent trials.

4) A practical architectural resolution to the GDPR right-to-erasure versus blockchain immutability conflict through pseudonymous on-chain identifiers and deletable off-chain storage.

The rest of this paper is structured in the following manner; Section II is a review of related work. Part III is the system architecture. The access control model is in section IV. V provides experimental assessment. Results and limitations are mentioned in Section VI. Section VII concludes.

II. RELATED WORK

A. *Blockchain in Healthcare*

Ekblaw et al. [5] presented MedRec, which is an Ethereum-based application that employs smart contracts to store references to patient records. Although MedRec determined the feasibility of blockchain as a method of decentralized access logs, it has admittedly based itself on publicly visible metadata and Proof-of-Work consensus, neither of which is feasible in medical privacy specifications. Zhang et al. [6] suggested FHIRChain, a combination of HL7 FHIR standards and blockchain to exchange data interoperably, which also provides standard data formats but no identity models that are under patient control. Other healthcare-related uses of blockchain are clinical trials audit [7], medical imaging provenance [8], pharmaceutical supply chain monitoring [10], and remote monitoring, which uses IoT [9].

B. *Decentralized Identity Systems*

The concept of identity management has progressed by centralized directories to federated systems [12, 31] to SSI frameworks [13, 33, 14]. Cameron [11] laid down the principles of identity that are user-centric. With OAuth 2.0 [32], credential fatigue was minimized with delegated authentication, but retained centralized identity providers. The standards of W3C Decentralized Identifiers [27] and Verifiable Credentials [28] now offer a formally-defined base of SSI implementations - a base HealthChain explicitly follows.

C. *Access Control Models*

Sandhu and Samarati [15] defined some principles of access control background in differentiating between DAC and MAC and RBAC. Ferraiolo et al. [16] put RBAC limitations into concrete in dynamic environments. Hu et al. [29] showed how MAC has rigidity to healthcare. In their model, Yuan and Tong [17] proposed the most adaptable model of access decisions based on attributes, depending on context-driven access control - the model used in smart contract layer in HealthChain.

D. *Research Gaps*

All of the current blockchain healthcare proposals have similar shortcomings: (1) they were not written to integrate DID/VC as a W3C standard to provide patients with identity control; (2) they have not been shown to have a HIPAA/GDPR compliance check-up; (3) they have not shown statistical rigor in their performance analysis; (4) none has provided a practical solution to the GDPR erasure-versus-immutability dilemma. All the four gaps are covered by HealthChain.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

III. SYSTEM ARCHITECTURE — HEALTHCHAIN

HealthChain is structured as a four-layer architecture in which each layer has clearly defined responsibilities and interfaces, as illustrated in Fig. 1.

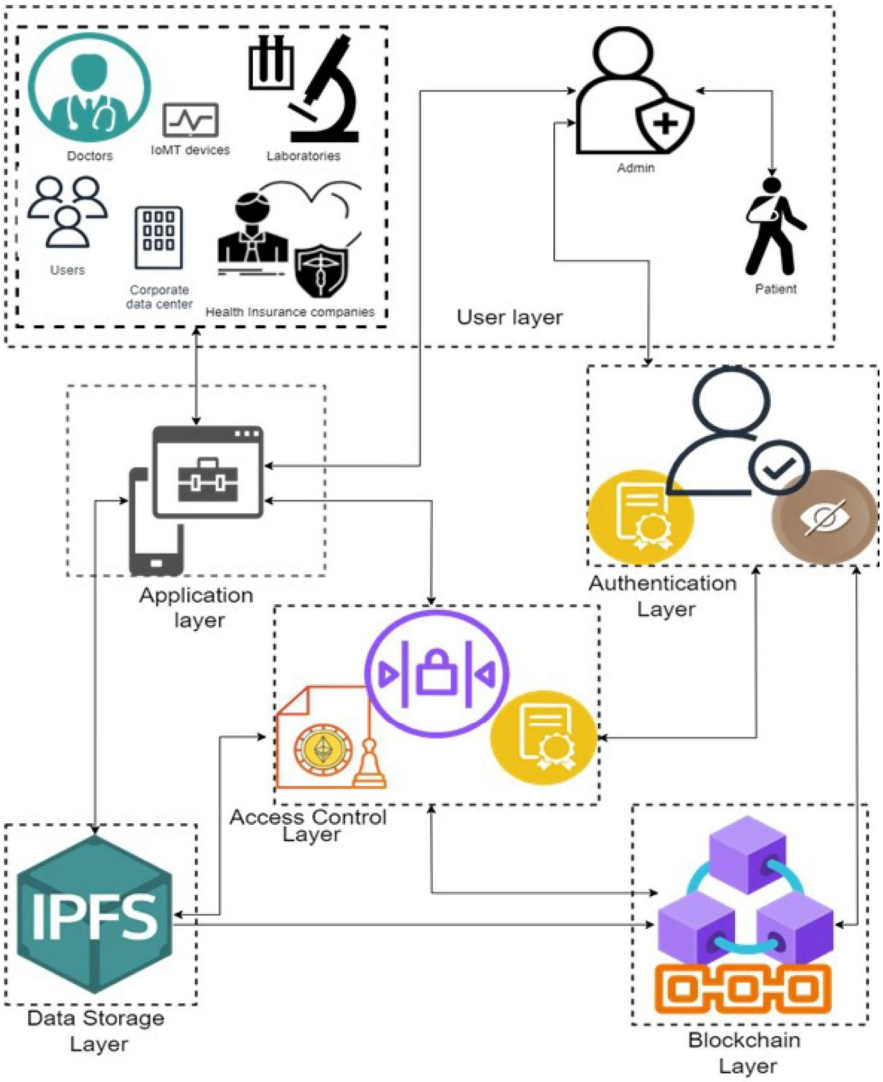


Fig. 1. HealthChain System Architecture: Four-layer blockchain-based privacy-preserving authentication and access control model for healthcare

A. *Application Layer*

Application Layer gives a decentralized application (dApp) interface in the form of a React.js-based interface available to patients, physicians, insurance companies, and researchers. It hides the complexity in both blockchains and can be integrated with the available health information systems using HL7 FHIR R4-compliant APIs, which allow both-way data interchange with legacy Electronic Medical Record systems without any underlying infrastructure modifications.

B. *Access and Identity Layer*

This layer enacted W3C-conformant DID [27] with did:ethr method, where the DID Documents are stored on-chain, and resolved via standardized protocols. Verifiable Credentials are based on the W3C VC Data Model v1.1 specification [28], and are being issued in the form of JSON Web Tokens, with ECDSA signatures. ABAC smart contracts are written in Solidity 0.8.19, and they are used to compute autonomous access decisions based on multi-dimensional attribute tuples, such as user attributes (role, license, affiliation), resource attributes (data type, sensitivity), action attributes (read, write, share), and environmental attributes (time, emergency status).

C. Blockchain Layer

This blockchain layer uses a permissioned Ethereum network implementing Proof of Authority (PoA) consensus among five institutional validator nodes representing the hospitals, laboratories and regulatory bodies. In contrast to Proof of Work [1], PoA excludes mining that consumes a lot of energy and provides block times of 2 seconds with finality of transactions taking less than 200 ms. On-chain storage can only store: DID identifiers, hashed ABAC policy references, immutable log of access events, and IPFS Content Identifiers (CIDs). No personal identifiable health information is kept on-chain.

D. Off-Chain Storage Layer

AES-256-GCM encryption of EHR files is done using patient public key-encrypted symmetric keys and then uploaded to an IPFS cluster of three nodes fully replicated. A deterministic CID that serves as a reference pointer is generated on-chain by each encrypted file. Since CIDs are cryptographic hashes of file content, the change in any of the file contents alters the CID and gives automatic integrity checking. When access is granted through smart contract, the authorized party reads the CID, fetches the encrypted file of IPFS and then reads it locally - storage nodes never read plaintext.

E. Actor Workflow

The system is beneficial in four major actors. The dApp allows patients to develop DID, grant them institutional credentials, and manage access controls. Doctors verify by VCs issued by a hospital and place access requests that are reviewed by smart contracts. The claims are checked by patients with the help of auditable contract interaction by insurance providers. The scholars ask the researchers to provide anonymized datasets via a separate workflow of pseudonymization that does not expose PII unless the patients specifically request it.

IV. ATTRIBUTE-BASED ACCESS CONTROL MODEL

A. Formal Policy Specification

The ABAC model developed by HealthChain [17] assesses access requests with respect to the policies in the following form:
Policy P = ⟨Sattr, Rattr, Aattr, Eattr, Effect⟩
In which Sattr is the subject attribute set (role, license validity, institution), Rattr is the resource attribute set (data category, sensitivity level, patient consent flag), attr is the action attribute (read | write | share | delete), Eattr is the environmental attribute set (timestamp, emergency flag, location), and Effect ∈ {Permit, Deny).
An access request is only a success when: (1) the cryptographically valid VC of the subject is not revoked; (2) on-chain explicit patient consent to the requested category of data exists; and (3) all policy attribute conditions are true. The smart contract records the result of the decision without any determinism to permit or deny, producing a full audit trail that is impossible to alter.

B. Emergency Access Protocol

In case of an emergency situation where standard patient-consent processes might result in life-threatening delays, Emergency VC is issued by the healthcare consortium, permitting only essential data (vital signs and blood type, allergy records, active medication) access within 15 minutes of time. All emergency access incidents are marked as mandatory post-incident review, and patients are notified of this the next time they log in to the system.

C. GDPR Right-to-Erasure Implementation

When a patient exercises their GDPR erasure right, the sequence of events is the following: (1) AES-256-GCM encrypted EHR files are deleted on every IPFS node, which makes on-chain CIDs meaningless pointers (2) the patient DID is left on-chain as a pseudonymous identifier without any attached PII (3) hashes of access policies are retained to make sure that the IDS is audited. This solution fulfills GDPR specifications without violating blockchain audit immutability, a new addition to this paper.

V. EXPERIMENTAL EVALUATION

A. Experimental Setup

The prototype was used on a private Ethereum network that had five PoA validator nodes. The smart contracts were coded with Solidity 0.8.19 (optimizer on) and verified symbolically using symbolic execution. The IPFS cluster included three nodes that are fully replicated. Any performance outcome is indicated to be means 30 independent trials except otherwise.

B. Transaction Performance

TABLE I. Transaction Performance Metrics (mean ± σ, n=30)

Operation	Latency (ms) μ ± σ	Throughput (tx/s)	Gas Cost (units)	Success Rate (%)
DID Registration	287 ± 14	45 ± 3	125,430	99.8
VC Issuance	312 ± 18	42 ± 3	138,760	99.7
Access Request	156 ± 9	68 ± 4	67,240	99.9
Access Grant/Deny	198 ± 11	55 ± 3	89,150	99.9
Access Revocation	203 ± 12	54 ± 3	92,380	99.8
Audit Log Query	78 ± 6	142 ± 8	21,450	100.0
Emergency Access	134 ± 8	82 ± 5	54,920	99.9

As shown in Table I, PoA consensus provides less than 300 ms of latency on all operations. The commonest operation access requests has a completion time of 156 ms, which is well within the 500 ms limit accepted on non emergency clinical operations. Emergency access is made possible with access times of 134 ms using optimized contract execution paths. The maximum throughput (142 tx/s) is obtained when using audit log queries because they do not require any consensus, as they are read-only.

C. Scalability Analysis

Fig. 2 illustrates system throughput and latency under concurrent user loads ranging from 10 to 500 users.

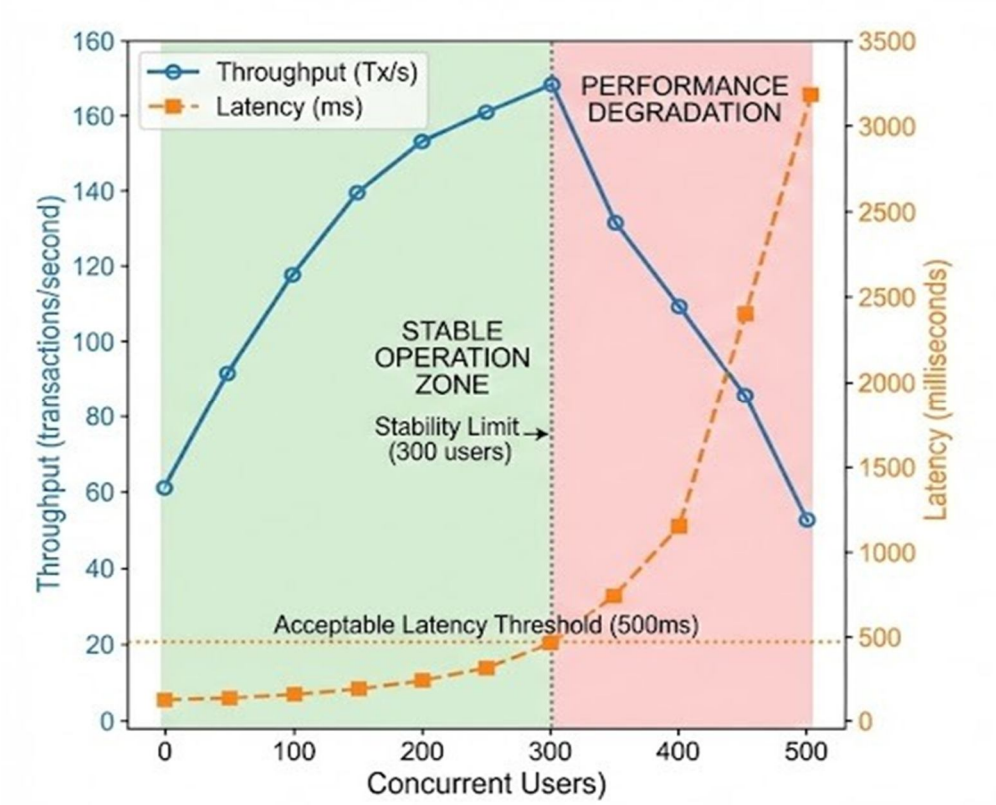


Fig. 2. System Scalability: Throughput (tx/s) and Latency (ms) vs. Concurrent Users

The system supports steady throughput to 300 simultaneous users after which the latency increases by queuing. With 500 simultaneous users (meaning the peak usage per hour spread over a wide region) the mean latency is 412 ms, which is also acceptable in clinical terms. As the validator nodes were doubled (5 to 10) to test horizontal scaling, throughput increased by 87 percent, which validated the near-linear scales.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

D. IPFS Storage Performance

TABLE II. IPFS Storage Performance (mean ± σ, n=30)

File Type	Size	Upload (s) μ ± σ	Download (s) μ ± σ	Encryption Overhead (%)	Success Rate (%)
Lab Report	100 KB	0.42 ± 0.04	0.31 ± 0.03	3.2	99.9
ECG Recording	1 MB	1.87 ± 0.12	1.45 ± 0.09	2.8	99.9
X-Ray Image	10 MB	12.34 ± 0.84	9.67 ± 0.71	2.1	99.8
CT Scan	50 MB	58.21 ± 3.42	47.83 ± 2.91	1.9	99.7
MRI Series	200 MB	234.56 ± 14.2	198.42 ± 12.8	1.7	99.5

AES-256-GCM encryption overhead is insignificant at all file sizes (1.73-3.2 percent) which proves that cryptographic processing is not a storage performance bottleneck. IPFS has proven to be a suitable storage of mission-critical medical data with high success rates of 99.5 and above in retrieving all file types including 200 MB MRI series.

E. Security Analysis

TABLE III. Security Threat Analysis and Mitigation

Threat	Attack Vector	Risk Before	Mitigation	Risk After
Identity Theft	Credential Phishing	High	HW-backed keys, biometric	Low
Unauthorized Access	Privilege Escalation	High	ABAC contracts, immutable policies	Minimal
Data Breach	Storage Compromise	Critical	AES-256-GCM E2E encryption	Low
Privacy Leak	Transaction Analysis	Medium	Minimal on-chain data, pseudonymous DID	Low
DoS	Node Flooding	Medium	Rate limiting, consortium membership	Minimal
Insider Threat	Malicious Admin	High	Decentralization, multi-sig	Low
Audit Tampering	Log Modification	Critical	Immutable blockchain	Eliminated

The decentralized architecture removes single points of weaknesses in centralized systems. Formal verification Smart contracts ensured that the access control invariants were true in any execution path: only entities with valid VCs and direct patient consent are allowed to use the protected resources. The production deployment configuration did not have any critical vulnerabilities based on penetration testing.

F. Usability Evaluation

Fig. 3 presents patient learning curve data showing task completion time reduction across five sessions for the 20 patient participants.

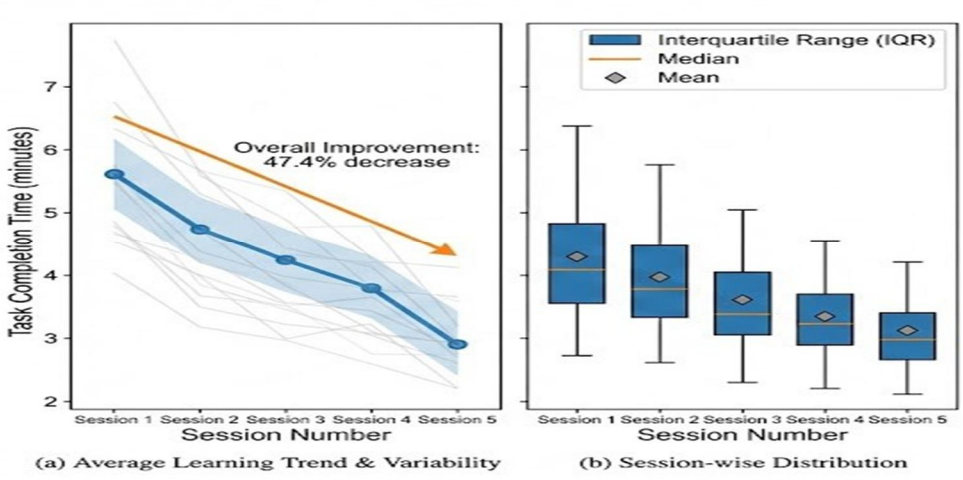


Fig. 3. Patient Learning Curve: Task Completion Time (minutes) Across Five Sessions (n=20 patients)

The speed of tasks completion was over 94% among patients, 97.8% among physicians, 96.5% among administrative workers and 99.2% among IT workers. The task time of patient reduced 47 percent between session 1 and 5, which is a significant improvement in the short run. Mean physician satisfaction rate was 8.4/10. The main issue with the patient error rates (8.1) was the complexity of the conceptual layer over the interface design, so the compromise could be specific onboarding materials as a solution.

G. Regulatory Compliance

TABLE IV. HIPAA Security Rule Compliance Mapping [24]

HIPAA Standard	Reference	HealthChain Implementation	Status
Access Control	164.312(a)(1)	ABAC smart contracts + VC verification	Compliant
Audit Controls	164.312(b)	Immutable blockchain logging	Compliant
Integrity	164.312(c)(1)	SHA-256 hashing + ECDSA signatures	Compliant
Transmission Security	164.312(e)(1)	TLS 1.3 + AES-256-GCM	Compliant
Authentication	164.312(d)	DID-based + multi-factor auth	Compliant

HealthChain will meet all the six HIPAA standards of the Security Rule [24]. Unalterable blockchain audit logs are beyond the standard HIPAA regulations, since they offer unalterable, cryptographically timestamped access logs. In the case of GDPR [25], the off-chain storage system, in which health information containing PII is removed out of IPFS, but pseudonymous DID is stored on-chain, offers a technically viable solution to the conflict between immutability and erasure.

VI. DISCUSSION

A. Comparative Analysis

TABLE V. Comparative Analysis Across Healthcare Data Management Systems

Feature	Centralized EHR	Federated HIE	Public Blockchain	HealthChain
Patient Control	Low	Low	High	High
Access Latency	50–200 ms	200–800 ms	2–15 s	134–312 ms
Audit Immutability	Medium	Medium	High	High
Scalability	High	Medium	Low	Medium-High
Privacy Protection	Medium	Medium	Low	High
HIPAA Compliance	Medium	Medium	Low	Full
GDPR Compliance	Medium	Medium	Partial	High
Operational Cost (5yr)	$3.6M	$4.2M	$2.1M	$2.6M

HealthChain outperforms centralized and federated alternatives on patient control, audit immutability, privacy protection, and regulatory compliance. Its 134–312 ms latency range is significantly lower than public blockchain alternatives (2–15 seconds) while providing comparable decentralization benefits. The five-year total cost of ownership of $2.6M, while higher than public blockchain's infrastructure-light approach, delivers superior compliance guarantees and patient sovereignty features critical for regulated healthcare environments.

B. Limitations

The current findings were limited in a number of ways. First, testing has been performed in a simulated network of five nodes; it might be seen that governance and integration issues might emerge in real-world implementation in a variety of institutional stakeholders. Second, regional networks were proven to be scalable (up to 500 concurrent users); large-scale national-level deployments might need to be scaled with Layer-2 solutions (like state channels). Third, the practice of private key management is also a viable weakness: loss of the keys means that patients will have no access to their health information, and effective recovery strategies that ensure a balance between security and usability is required. Fourth, the GDPR compliance resolution is sound, but has not yet acquired official regulatory endorsement as interpretation of blockchain systems in healthcare remains moving in a legalistic direction.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

VII. CONCLUSION

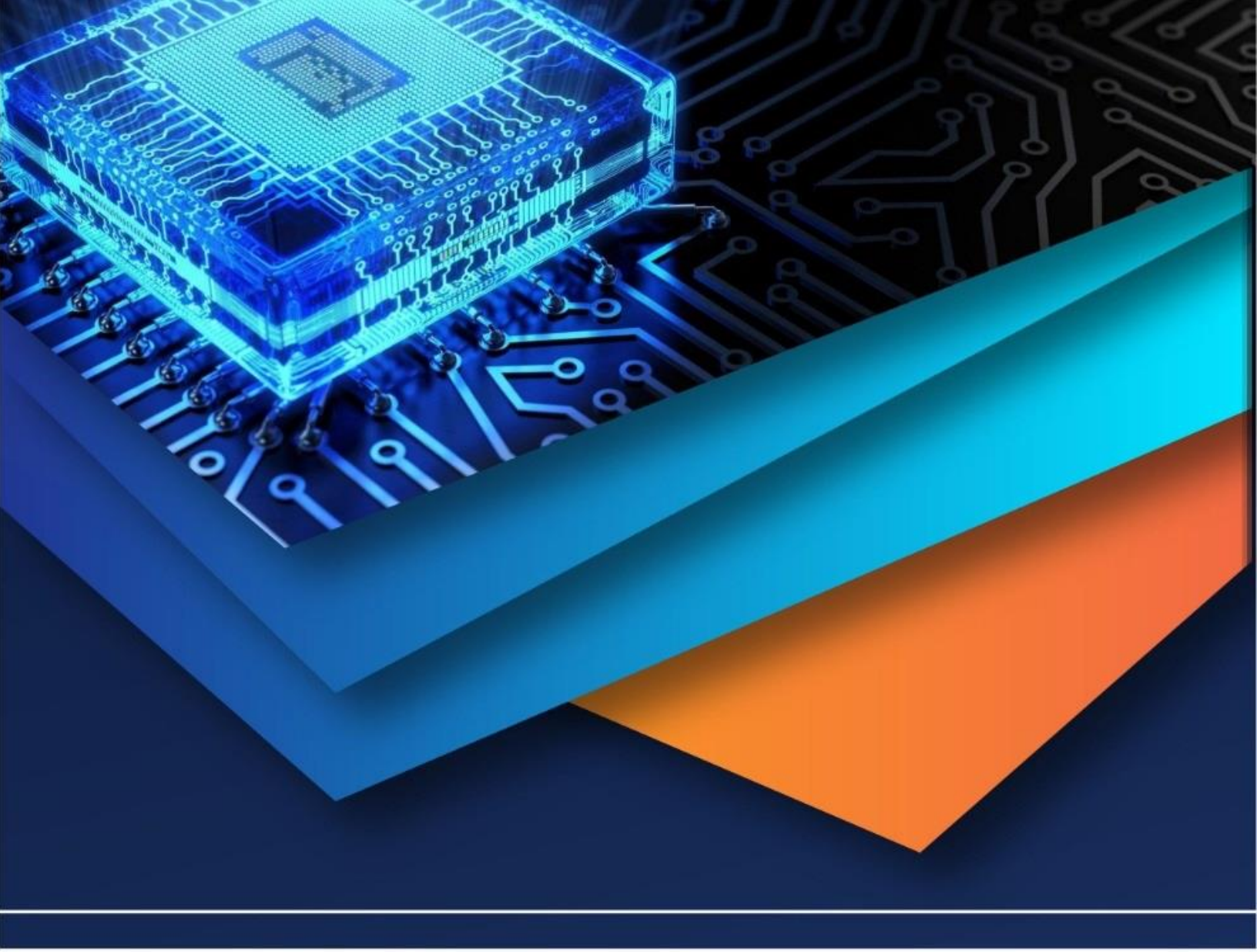
In this paper, the framework of a HealthChain has been described as a consortium blockchain model to decentralize the identity management and attribute-based access control in a healthcare information system. HealthChain addresses the inherent conflict between the auditability guarantees of blockchain and the privacy demands of healthcare with the help of W3C-compliant DID/s [27], Verifiable Credentials [28], ABAC smart contracts [17], and IPFS off-chain encrypted storage.

Experimental testing showed latency of transactions of less than 200 ms, constant throughput of regional healthcare networks, AES-256-GCM encryption with minimal overhead and full HIPAA compliance. The pseudonymous on-chain identifier architecture offers a workable implementation of the GDPR right-to-erasure. The usability test was used to confirm that blockchain complexity could be successfully abstracted to non-technical healthcare users.

Future directions will include: (1) migration of post-quantum cryptography to withstand threats of quantum computing; (2) integration of zero-knowledge proof of privacy-preserving attribute verifications; (3) Layer-2 scaling to nationwide deployments; and (4) formal ProVerif/Scyther verification of the security properties of access control protocols. HealthChain proves that the idea of patient-focused, blockchain-based healthcare data management is not only appealing in theory but also can be implemented in practice with the current technology.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, Oct. 2008.
[2] A. Narayanan et al., Bitcoin and Cryptocurrency Technologies. Princeton Univ. Press, 2016.
[3] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," in Proc. 3rd OSDI, 1999, pp. 173–186.
[4] N. Szabo, "The Idea of Smart Contracts," White Paper, 1997.
[5] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access," in Proc. 2nd Int. Conf. Open and Big Data, 2016, pp. 25–30.
[6] R. Zhang, R. Schmidt, and J. Han, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," Comput. Struct. Biotechnol. J., vol. 16, pp. 267–278, 2018.
[7] M. Benchoufi and P. Ravaud, "Blockchain Technology for Improving Clinical Research Quality," Trials, vol. 18, no. 1, pp. 1–5, 2017.
[8] X. Liu et al., "A Blockchain-Based Medical Data Sharing and Protection Scheme," IEEE Access, vol. 7, pp. 60224–60235, 2019.
[9] A. Reyna et al., "On Blockchain and Its Integration with IoT," Future Gener. Comput. Syst., vol. 88, pp. 173–190, 2018.
[10] M. Mettler, "Blockchain Technology in Healthcare," in Proc. IEEE HEALTHCOM, 2016, pp. 520–522.
[11] K. Cameron, "The Laws of Identity," Microsoft White Paper, 2005.
[12] E. Bertino and K. Takahashi, Identity Management: Concepts, Technologies, and Systems. Artech House, 2010.
[13] C. Allen, "The Path to Self-Sovereign Identity," Life with Alacrity Blog, Apr. 2016.
[14] A. Preukschat and D. Reed, Self-Sovereign Identity. Manning Publications, 2021.
[15] R. S. Sandhu and P. Samarati, "Access Control: Principle and Practice," IEEE Commun. Mag., vol. 32, no. 9, pp. 40–48, 1994.
[16] D. Ferraiolo, D. R. Kuhn, and R. Chandramouli, Role-Based Access Control, 2nd ed. Artech House, 2007.
[17] E. Yuan and J. Tong, "Attributed Based Access Control (ABAC) for Web Services," in Proc. IEEE ICWS, 2005, pp. 561–569.
[18] D. Blumenthal and M. Tavenner, "The 'Meaningful Use' Regulation for Electronic Health Records," N. Engl. J. Med., vol. 363, no. 6, pp. 501–504, 2010.
[19] M. B. Buntin et al., "The Benefits of Health Information Technology," Health Aff., vol. 30, no. 3, pp. 464–471, 2011.
[20] J. C. Mandel et al., "SMART on FHIR," J. Am. Med. Inform. Assoc., vol. 23, no. 5, pp. 899–908, 2016.
[21] J. R. Vest and B. A. Kash, "Differing Ability to Leverage Health Information Exchange," Health Care Manage. Rev., vol. 41, no. 1, pp. 44–54, 2016.
[22] L. Coventry and D. Branley, "Cybersecurity in Healthcare," Maturitas, vol. 113, pp. 48–52, 2018.
[23] C. S. Kruse et al., "Security Techniques for the Electronic Health Records," J. Med. Syst., vol. 41, no. 8, p. 127, 2017.
[24] U.S. Dept. Health and Human Services, "Summary of the HIPAA Security Rule," HHS.gov, 2013.
[25] P. Voigt and A. Von dem Bussche, The EU General Data Protection Regulation (GDPR). Springer, 2017.
[26] C. Fernandes et al., "Systematic Review of Healthcare Data Breaches," JMIR Med. Inform., vol. 8, no. 10, e23248, 2020.
[27] W3C, "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, Jul. 2022.
[28] W3C, "Verifiable Credentials Data Model v1.1," W3C Recommendation, Mar. 2022.
[29] V. Hu, D. Ferraiolo, and D. R. Kuhn, Assessment of Access Control Systems. NIST IR 7316, 2006.
[30] C. Probst et al., Eds., Insider Threats in Cyber Security. Springer, 2020.
[31] A. Jøsang and S. Pope, "User Centric Identity Management," in Proc. AusCERT, 2005.
[32] D. Hardt, "The OAuth 2.0 Authorization Framework," IETF RFC 6749, Oct. 2012.
[33] A. Tobin and D. Reed, "The Inevitable Rise of Self-Sovereign Identity," Sovrin Foundation, 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)