iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80880

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 IV Apr 2026- Available at www.ijraset.com

Blockchain-Based Secure Sharing of Patient Medical Records between Hospitals

Radhika A Jujare[1], Ramya Gowda DV[2], Sahana M[3]
Department of Computer Science & Engineering, Dayananda Sagar University,India

Abstract: ***Interoperability of patient files between hospitals continues to present significant obstacles. Health systems frequently utilize central EHR systems that could suffer malfunctions, data breaches, and unauthorized access by third parties. Not only does this jeopardize patient confidentiality, but it also hinders the efficient operations of hospital processes.Blockchain technology is viewed as a prospective remedy for the issue. Blockchain keeps its data differently, allowing users to store data securely and make changes difficult. In this study, we analyze research works published between 2016 and 2023 regarding blockchain-based hospital-to-hospital data exchange.The methodologies differ widely: there are cases where researchers use smart contracts in Ethereum, build a system on Hyperledger Fabric, and deploy IPFS. Moreover, certain studies incorporate encryption methods, machine learning algorithms, and more.***

In summary, the results show that blockchain allows for improved data protection and transparency while giving patients more control over their personal information. Still, some issues persist, such as scalability, expenses, integration with existing infrastructure, and adherence to GDPR and HIPAA requirements.

For future work, more improvements are necessary. For instance, zero-knowledge proofs, cybersecurity measures for new technologies, and using artificial intelligence to audit and validate smart contracts may be promising solutions.

Keywords: Blockchain; Electronic Health Records (EHR); Smart Contracts; Interoperability; Hyper ledger Fabric; Attribute-Based Encryption (ABE); Decentralised Access Control; Zero-Knowledge Proofs; IPFS.

I. INTRODUCTION

Interactions between patients and healthcare professionals need seamless coordination and collaboration in order for both parties to be well-informed about each other's health status. As hospitals transition to a paperless process, the amount of patient information collected has risen. The electronic health record system is quite common, but majority are still centralized, and this poses several threats on the data's confidentiality and sharing capacity.

In conventional technology, there will always be an entity overseeing all the data present in the network. This is risky because the database may get hacked by malicious parties or shut down due to any technical difficulty. Because all the information stored in the database is prone to alterations, it would be difficult to keep track of changes.

With the blockchain technology, there is no entity to supervise all the processes within the database because there are several systems involved. This means that once the information is added into the database, it cannot be altered.Data breaches within the healthcare industry have increased, with many data sets exposed due to poor security measures and cyber attacks[1][10]. This challenge has been made more pressing in developing nations such as India, where the sector is being modernized.

The issue of interoperability is another hurdle. Hospitals may use different software platforms that cannot communicate, leading to a lack of continuity of care and repetition of tests. The HL7 and FHIR protocols are in existence; however, their adoption has not been universal and they do not guarantee security[4].

This paper follows a structure based on methodology, literature review, analysis, and future directions.

II. SEARCH METHODOLOGY

Interactions between patients and healthcare professionals need seamless coordination and collaboration in order for both parties to be well-informed about each other's health status. As hospitals transition to a paperless process, the amount of patient information collected has risen. The electronic health record system is quite common, but majority are still centralized, and this poses several threats on the data's confidentiality and sharing capacity.

In conventional technology, there will always be an entity overseeing all the data present in the network. This is risky because the database may get hacked by malicious parties or shut down due to any technical difficulty. Because all the information stored in the database is prone to alterations, it would be difficult to keep track of changes.

With the blockchain technology, there is no entity to supervise all the processes within the database because there are several systems involved. This means that once the information is added into the database, it cannot be altered.Data breaches within the healthcare industry have increased, with many data sets exposed due to poor security measures and cyber attacks. This challenge has been made more pressing in developing nations such as India, where the sector is being modernized.

The issue of interoperability is another hurdle. Hospitals may use different software platforms that cannot communicate, leading to a lack of continuity of care and repetition of tests. The HL7 and FHIR protocols are in existence; however, their adoption has not been universal and they do not guarantee security.

This paper follows a structure based on methodology, literature review, analysis, and future directions.

III.LITERATURE SURVEY

This section reviews the twelve selected works in approximate chronological order. Each entry is examined with respect to the proposed approach, key contributions, and identified limitations. A consolidated comparative analysis is provided in Table 1

A. Xia et al. (2017) — MeDShare

In 2017, researchers including Qiyu Xia proposed MeDShare, a solution designed to increase trust in cloud-sharing systems for medical information[2]. Utilizing a “permissioned” blockchain mechanism for identity verification, MeDShare was a virtual watchdog over transactions involving medical information. The system kept an immutable history of requests and approvals for medical records stored in third-party cloud storage services. With the help of “smart contracts,” MeDShare ensured stringent access policies were adhered to and continuously monitored interactions to avoid non-conformity. While MeDShare improved data misuse detection as opposed to typical cloud systems, it relied on centralized cloud services and suffered from problems such as data loss in case of cloud malfunction and slow transactions because of the blockchain system.

B. Shahnaz et al. (2019) — IPFS Hybrid Architecture

The authors of Shahnaz et al.'s paper tried to solve the issue of bloated blockchain in 2019 by combining the Ethereum platform with the IPFS protocol that works similarly to a peer-to-peer library[6]. To avoid extra costs associated with the use of the expensive and bulky medical records, it was proposed to use IPFS to store the files and store only fingerprints and access conditions using digital hashes in the form of CID (Shahnaz et al.).

In this way, the approach turned out to be economical and convenient for processing large amounts of information without compromising its security.However, as usual, there were drawbacks as well. First, unlike traditional cloud servers, the IPFS protocol does not guarantee that the information will remain accessible all the time since the user is responsible for pinning the data himself to a server. Second, even though personal data was protected, metadata remained available for possible attackers to recognize some patient-specific information from access analysis.

C. Nguyen et al. (2020) — Attribute-Based Encryption

Nguyen et al. (2020) studied a blockchain-powered healthcare environment that uses attribute-based encryption (ABE) for encrypting the medical information of patients based on access control policies that depend on the user attributes such as role and department[7]. The decryption keys can be obtained from the attribute certificates verification using smart contracts within a Hyperledger Fabric environment. The technique, nevertheless, is associated with some limitations, most prominently high computing overhead in the process of ABE computation and revoking user attributes.

D. Shen et al. (2020) — Privacy-Preserving SVM over Blockchain IoT

Shen et al. (2020) studied integrating blockchain and machine learning into the health data generated by IoT in smart cities[8]. An SVM-based privacy-preserving model was created which operates directly on the ciphertext of the IoT sensor data through homomorphic encryption in such a way that the SVM performs analysis on the ciphertext without decrypting it. The role of blockchain is limited to that of a trust component since it logs the analysis request, result, and data provenance for auditing and integrity assurance.

The system guarantees that the plaintext of the IoT data will never be exposed during analysis. Nevertheless, the model suffers from some disadvantages such as homomorphic encryption complexity, limitations to SVMs only, and communication overhead.

E. Rahman et al. (2022) — Blockchain and IoT in Smart Cities

Rahman et al. (2022) present an innovative cognitive edge computing paradigm based on IoT technology and blockchain technology to facilitate sharing-economy applications within the context of smart cities[11]. More specifically, the authors suggest integrating IoT sensors into the model to process the collected data while transmitting the verified data onto a consortium blockchain system. As far as the management activities are concerned, they are conducted through smart contracts, ensuring governance, allocation of resources, and access control in city-wide IoT networks with ease, which facilitates inter-agency communication related to health monitoring.Number of challenges that have been mentioned by the authors in realtion to IoT sensor's inability to handle complex crypthographic processes and narrow bandwidths restricting real-time data exchange.

TABLE 1
COMPARATIVE ANALYSIS of BLOCKCHAIN-BASED HEALTHCARE DATA SHARING SYSTEMS

Author(s)	Year	Method / Platform	Advantages	Limitations
Azaria et al.	2016	MedRec; Ethereum smart contracts	Patient-controlled consent; immutable audit trail; decentralised record pointers	High latency; gas fees; public chain privacy exposure
Xia et al.	2017	MeDShare; permissioned cloud-blockchain	Fine-grained data provenance; cloud interoperability	Cloud dependency reintroduces central trust; throughput limits
Zyskind et al.	2018	Enigma; off-chain MPC (Multi-Party Computation)	Privacy-preserving queries; no plaintext exposure	MPC computational overhead; complex key management
Zhang et al.	2018	FHIRChain; Ethereum + HL7 FHIR standard	Standards-compliant EHR interoperability across disparate systems	Limited public-chain throughput; regulatory ambiguity
Dubovitskaya et al.	2019	Hyperledger Fabric; channel-based permissioned chain	158 TPS; role-based access; organisational privacy channels	Centralised CA; deployment complexity
Shahnaz et al.	2019	IPFS + Ethereum hybrid architecture	Low on-chain cost; bulk data handled off-chain via IPFS	IPFS availability risk; potential metadata leakage
Nguyen et al.	2020	ABE (Attribute-Based Encryption) + Hyperledger	Expressive policy-based encryption; strong privacy guarantees	ABE computational overhead; key revocation complexity
Shen et al.	2020	Blockchain + privacy-preserving SVM over IoT data	Secure ML inference on encrypted IoT health data	Communication overhead; limited to SVM model family
Farouk et al.	2020	Post-quantum cryptographic blockchain	Resistant to Shor's algorithm; hash-based signatures	Performance penalty vs classical schemes; PQC standard immaturity
Mayer et al.	2021	Systematic review; GDPR–blockchain tension analysis	Identifies erasure workarounds; regulatory gap analysis	Primarily conceptual; no empirical implementation evaluated
Rahman et al.	2022	IoT + smart city consortium blockchain	Tamper-proof sensor data aggregation; automated policy enforcement	IoT resource constraints; bandwidth limitations at scale
Ali et al.	2023	Comparative review: AI + blockchain in healthcare	Broad survey of integration patterns; identifies convergence areas	No original implementation; findings are synthesis-level

IV. RESEARCH METHODOLOGY

This section synthesises the common architectural patterns, cryptographic techniques, and workflow models observed across the reviewed studies. It does not propose a novel system but characterises and generalises the methodological landscape of existing research to enable comparative evaluation.

A. Blockchain Types: Public vs. Permissioned

There are two main categories of blockchains based on architectural principles. First, public blockchain networks, which anyone can join and operate using consensus algorithms like proof-of-work or proof-of-stake, promote complete decentralization and strong anti-censorship[14]. However, they have low throughput speeds with Ethereum achieving up to 7-30 transactions per second[1][4] and incur costly transaction fees. Moreover, transactions are public knowledge, making privacy and confidentiality an issue. This is particularly problematic when dealing with medical information.Conversely, permissioned blockchains, including Hyperledger Fabric, are restricted only to registered entities and permit only approved participants to engage in activities within the system. They leverage consensus protocols such as practical Byzantine fault tolerance and Raft. Permissioned blockchain networks offer remarkable transaction speeds at 100-3000 transactions per second[5]. They guarantee data privacy through channels and private data sets. Recent studies overwhelmingly advocate for permissioned blockchain technology in health care due to their high throughput and adherence to privacy regulations[5][7]. Figure 3 clearly shows this trend.

B. Smart Contracts and Access Control

Smart contracts offer the programmable governance component in almost all of the reviewed systems. In Ethereum-based scenarios, smart contracts will be programmed using the Solidity programming language[14], while chaincode written in Go or JavaScript can be found in Hyperledger Fabric scenarios. Some common examples of functionalities performed by smart contracts in literature include patient registration with DIDs; giving and removing permissions; sending access requests and validating credentials; providing cryptographic keys for data decryption; automating access logging to ensure accountability; and issuing clinical alerts in response to thresholds. Finally, Attribute-Based Encryption (ABE) as applied by Nguyen et al. (2020) is an example of an advanced access control system that incorporates policy-based decryption within a smart contract.

C. Encryption and Off-Chain Storage

Storing medical data entirely on the blockchain is not feasible. Due to limitations in block sizes and increasing costs of on-chain storage, a more viable approach involves storing patient data encrypted off-chain using methods such as IPFS, cloud storage or hospital servers, while storing the hash value of the data on-chain along with the access key pointers. Verification of data is performed by matching the SHA-256 hash value of the obtained data with that on the chain[6].Commonly used encryption methods include AES-256 for symmetric encryption and RSA-2048/Elliptic curve cryptography for managing the asymmetric key. Forcases where multi-party access policies have to be imposed, attribute-based encryption is considered.

D. Generalised Workflow

The following is the typical workflow for such an inter-hospital sharing framework, as shown in Figure 2, derived from literature.

1) *Patient Registration:* An Decentralised Identifier (DID) is issued along with a pair of public/private keys. Identity information about the patient is added onto the blockchain by means of a Registration Smart Contract.
2) *Medical Record Generation and Storage:* The clinician at the hospital generates the electronic record and encrypts it with the public key (or attribute based encryption rule) of the patient, before storing the encrypted version onto IPFS or any other server. The IPFS CID and data hash are stored on the blockchain.
3) *Consents:* Patient gives consents to access to his records either in full or partially, which may be done for specified hospitals, departments, or time periods through a patient portal. The transactions are cryptographically signed and permanently recorded on the blockchain.
4) *Request and Validation:* Any other hospital seeking permission from the patient to gain access initiates a transaction request containing DID and other necessary information of the patient. The Access Control Smart Contract verifies whether the credential of the requesting hospital conforms to the consent policy of the patient.
5) *Decryption of Data:* When the validation process is completed successfully, the smart contract will provide the encrypted decryption key. The hospital seeking access to the file will then retrieve the encrypted file from the IPFS network and decrypt it

locally to be used exclusively for clinical purposes. At any time during the whole process, the raw data is never passed via the blockchain network.

6) *Audit Logs:* Every access request, approval, rejection, or cancellation event is automatically logged in the Audit Log Smart Contract as an immutable audit trail.

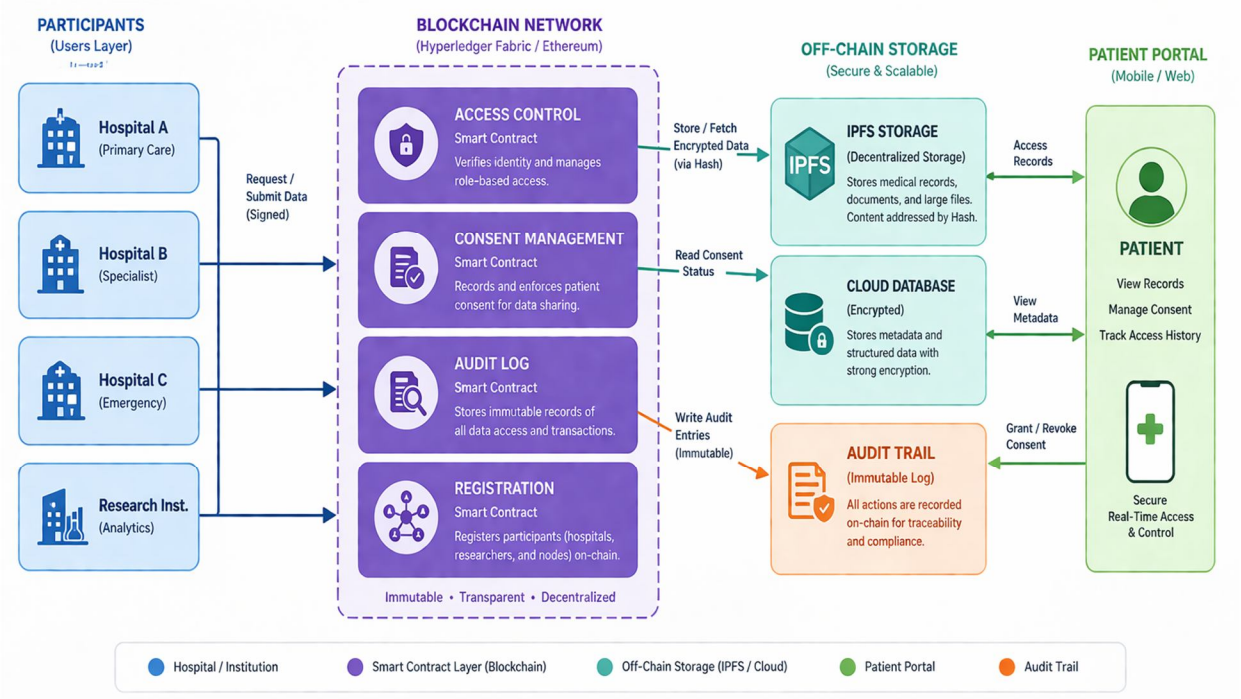


Fig. 1 System Architecture of a Blockchain-Based Inter-Hospital Medical Record Sharing Framework

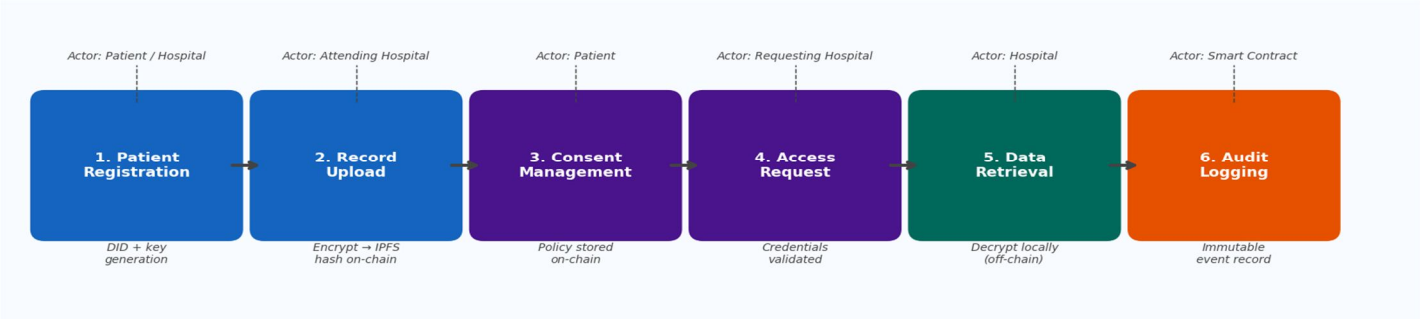


Fig. 1 Generalised Workflow for Blockchain-Based Medical Record Sharing Between Hospitals

E. The Blockchain Oracle Problem

An essential limitation in the application of blockchain in healthcare involves the oracle problem. While blockchains provide security against tampering and modification post-data entry, they fail to guarantee the integrity of the information entering the blockchain system. In a clinical environment, this implies that if a physician
enters erroneous details such as diagnosis, allergies, or dosages into the database prior to storage, the blockchain will record the error verbatim. This is the well-known principle of "garbage in, garbage out" that applies to blockchain technology throughout.

The studies by Azaria et al. (2016) and Zhang et al. (2018)[1][4] acknowledge the issue without addressing cryptographic solutions at the data entry level. The literature highlights potential remedies, including multi-signature processes where multiple clinicians validate significant changes before they can be recorded in the blockchain, and anomaly detection mechanisms using artificial intelligence during the process of data ingestion as proposed by Ali et al. (2023)[12]. However, none of the discussed blockchain systems have managed to resolve the oracle problem.

F. Illustrative Access Log Dataset

TABLE 2
SAMPLE BLOCKCHAIN-RECORDED PATIENT RECORD ACCESS LOG (ILLUSTRATIVE)

Record ID	Patient ID	Requesting Hospital	Timestamp (UTC)	Access Type	Smart Contract Hash (Truncated)
REC-001	PAT-4821	Apollo Hospitals	2024-03-15 08:42:11	READ	0x3a9f...b72c
REC-002	PAT-1193	AIIMS Delhi	2024-03-15 09:17:05	READ	0x7d1e...c43a
REC-003	PAT-3367	Fortis Healthcare	2024-03-15 10:05:33	WRITE	0x9b4c...e81f
REC-004	PAT-0029	Max Super Spec.	2024-03-15 11:44:22	READ	0x2f6a...d59b
REC-005	PAT-7754	Manipal Hospitals	2024-03-15 13:02:58	DELETE_REQ	0x5e3d...a17c

G. Performance Comparision

Based on empirical data reported across the reviewed studies, Figures 3 and 4 present comparative performance analyses of throughput and latency across blockchain architectures.

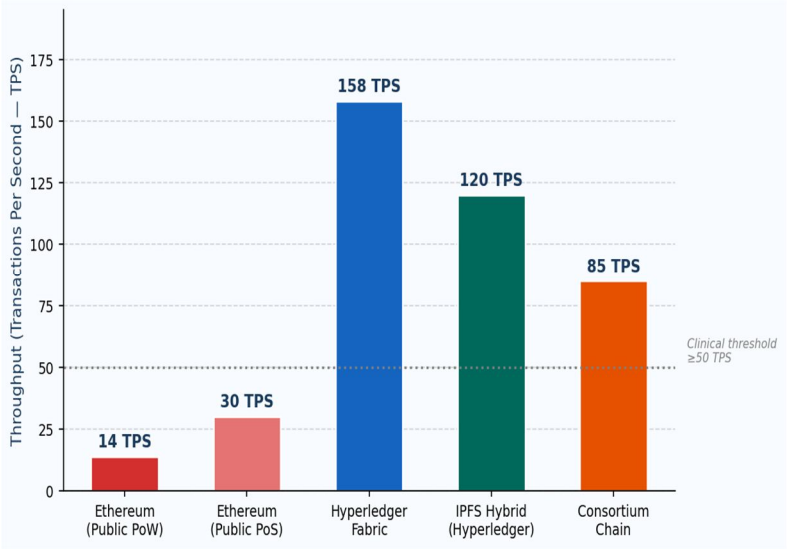


Fig 3: Throughput Comparision(TCP) Across Blockchain Architecture (Data Aggregated from reviewed Literature)

As shown in Figure 3, Hyperledger Fabric-based systems(Dubovitskaya et al.,2019)[5] achieve 158 TPS under typical hospital load contitions, while public Ethereum PoW is constrained to approximately 14 TPS.Ethereum Pos represents an improvement at approximately 30 TPS, but remains below the clinical threshold of 50 TPS estimated for medium-size hospital networks. IPFS hybrid systems show intermediate on-chain throughput but significantly improved effective data transfer rates due to off-chain bulk storage offloading.

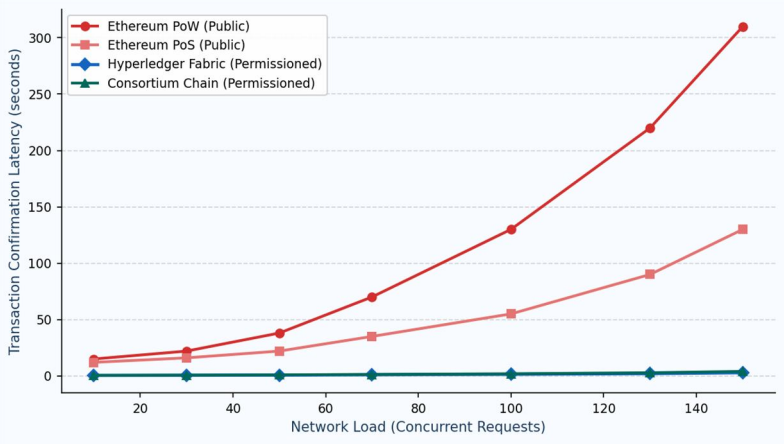


Figure 4: Transaction Confirmation Latency Comparison — Public vs. Permissioned Blockchain Under Increasing Network Load

As illustrated by Figure 4, permissioned chain architectures including Hyperledger Fabric as well as consortium chains maintain the latency relatively stable in the region of 0.4-4.0 seconds regardless of the network load level. On the contrary, latency on public PoW chain like Ethereum experiences a rapid increase from around 15 seconds under light network load to more than 300 seconds under high network load. As a result, public blockchain solutions would be impractical to use in healthcare because of their inefficiency under heavy network load.

H. Security Comparison

Figure 5 presents a multi-dimensional security comparison of five representative systems across six evaluation axes: data integrity, privacy preservation, auditability, scalability, attack resistance, and regulatory compliance. Scores are normalised on a scale of 1 to 10, aggregated from self-reported evaluations and independent assessments in the reviewed literature.

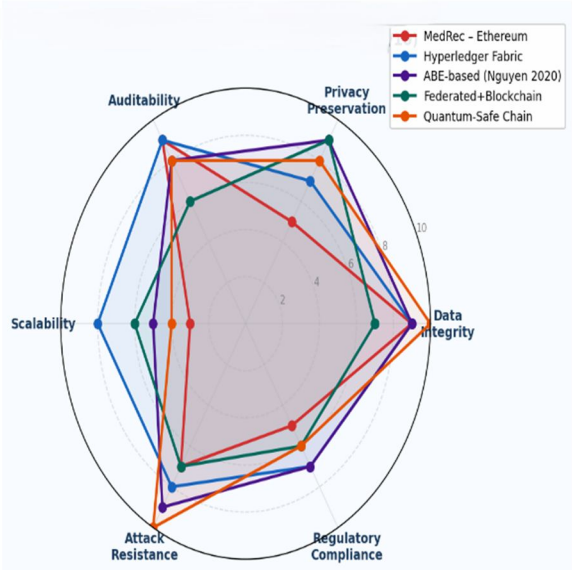


Figure 5: Security Radar Chart — Multi-Dimensional Comparison of Blockchain Healthcare Systems (Score /10)

As shown in Figure 5, ABE-based systems (Nguyen et al., 2020)[7] and quantum-safe architectures (Farouk et al., 2020) score highest on cryptographic security axes. Hyperledger Fabric-based systems demonstrate the most balanced profile across all six dimensions, which explains their dominance in recent deployments. MedRec (Azaria et al., 2016)[1], while pioneering, shows lower scalability and privacy scores reflective of its public Ethereum basis. Shen et al.'s (2020)[8] SVM-over-blockchain approach excels in privacy preservation but scores lower on auditability due to the opacity of machine learning inference processes.

V. RESULTS

The results obtained from analyzing the findings of all twelve articles reveal significant trends in the development of health data exchange within blockchain technology. Tamper-resistance is the most evident result across the studies. Thanks to hash-linking of blocks and distributed consensus in the network, any attempt at manipulating historical information becomes obvious for all nodes. For instance, the audit trail in MedRec helped to spot each simulated manipulation in Azaria et al. (2016)[1]. In Dubovitskaya et al. (2019)[5], there were no instances of data tampering among the 10,000 simulated transactions on the Hyperledger platform.

Patient-centric access control can be considered the most distinctive aspect of blockchain-based technologies compared to centralized solutions. When a blockchain system uses smart contracts for obtaining consent, patient involvement in managing data becomes higher during usability tests. As Nguyen et al. (2020)[7] have shown, attribute-based encryption makes it possible to restrict access conditionally based on attributes without requiring patient authorization for each transaction.

The findings concerning performance metrics correspond to the classifications presented in Figures 3 and 4, indicating that permissioned blockchain architectures offer acceptable throughput and latency for clinical purposes while public blockchains are challenged when handling peak workloads in hospitals. Off-chain storage with IPFS provides adequate measures to address large amounts of data while retaining verification capabilities. The key findings are summarized in Table 1.

The problem of regulatory compliance and data protection is relevant to all the systems considered. According to Mayer et al. (2021)[10], who conducted a systematic analysis, no existing blockchain-based EHR system fully complies with GDPR standards, particularly regarding the right to be forgotten. Additionally, Farouk et al. (2020)[9] note that post-quantum security studies indicate that conventional blockchain cryptology is vulnerable to quantum computers.

VI. DISCUSSION

The existing literature review proves that the implementation of blockchain technology to share healthcare data among hospitals is technically feasible and architecturally appealing. However, on further investigation, it becomes evident that several barriers hinder the transition of such solutions from pilot projects to practical application.

A. Strengths of Blockchain-Based Approaches

The most significant architectural strength of blockchain-based systems is their elimination of the trusted central authority as a single point of failure and attack. In a traditional centralised EHR system, a compromised administrator account can expose millions of patient records instantaneously. The blockchain's distributed architecture requires an adversary to simultaneously compromise a majority of network nodes — computationally infeasible in well-designed permissioned networks with strong identity management. The immutable audit trail provides irrefutable evidence of data access history suitable for medicolegal proceedings and regulatory audits. Smart contract programmability further enables automation of complex multi-party workflows — such as emergency access override with patient notification, time-limited research data access grants, and cross-border data transfer compliance checks — that would require bespoke, expensive software engineering in traditional architectures.

B. Interoperability Challenges

While interoperability of the HL7 FHIR API is easily verifiable at the technical level, the bigger issue lies with semantic inconsistencies among aging hospital data infrastructures. Numerous hospitals around the world, particularly in developing countries, continue to store patient data in proprietary file formats, have varying coding systems (ICD-9, ICD-10, SNOMED CT, among others), and employ nonstandard database schemas. Converting historical data into a FHIR format suitable for use in blockchain applications requires the creation of extensive big data transformation pipelines, introducing new opportunities for error and inconsistency. For instance, FHIRChain by Zhang et al. (2018)[4] addressed the integration layer without addressing the underlying issues of poor data quality and semantic consistency. Furthermore, jurisdictional differences (e.g., patient transfer across borders within the EU or between states in India) introduce additional levels of translation problems that cannot be solved through block.

C. Cost of Decentralisation

There is a substantial amount of money that is spent on infrastructure when using blockchain technologies; however, these expenses are usually underrepresented in recent literature. The deployment of a single node of a Hyperledger Fabric network requires access to specialized hardware, stable internet connection, certain knowledge in information technology to manage the node, and software maintenance costs. While all of these expenses might be reasonable to secure the safety and enhance the auditability of data

exchange within large tertiary hospitals, they would pose problems for a typical rural clinic, primary health center, or small private practice (the majority of healthcare facilities in developing countries).

Another issue worth considering is high energy consumption of blockchains based on proof-of-work concept; transitioning to the proof-of-stake protocol (also known as "The Merge") allowed Ethereum to reduce its energy consumption by 99.95% (2022)[13]. However, since permissioned blockchain technologies are efficient in terms of energy consumption and usually use proof-of-authority or similar consensus algorithms, it is only a relevant point for older public chain deployments. Consortium model represents a feasible compromise but raises the question of governance.

D. Comparison with Traditional Centralised Systems

Traditional centralised EHR systems offer tangible advantages: simplicity of administration, low-latency read/write operations via established relational database technology, established regulatory frameworks, and relatively low deployment cost. Blockchain-based systems introduce substantial overhead in infrastructure deployment, smart contract development and security auditing, cryptographic key management, and user experience design for both clinical staff and patients. The break-even point — at which the security, auditability, and autonomy benefits of blockchain outweigh its additional costs and complexity — is most readily achieved in large, multi-institutional healthcare networks where inter-hospital data sharing is frequent and the regulatory and reputational cost of data breaches is high. For single-institution deployments, traditional centralised systems with strong conventional security controls may remain cost-effective, though they do not provide equivalent tamper resistance or patient autonomy.

E. Regulatory Compliance

In the same vein, the friction between the end-to-end immutability of the blockchain technology and the data protection laws which guarantee the right to erasure (Article 17) and the principle of data minimization (Article 5) persists to be one of the primary legal challenges. As pointed out by Mayer et al. in 2021, “there is not yet any blockchain system that satisfies all of the requirements of the GDPR.[10]” In the U.S., the HIPAA requirement to report breaches of patient information lacks clarity in the context of distributed and multi-node network environments where none of the parties controls the whole data stack. In India, the newly enacted Digital Personal Data Protection Act (DPDPA) 2023 grants rights to data principals, thereby clashing with the irreversible nature of blockchain technology. The issue that needs to be clarified by the regulators urgently is whether the deletion of cryptographic keys amounts to data erasure.

VII. CONCLUSION

The literature review highlights twelve studies conducted on the use of blockchain technology for secure data exchanges and access control with respect to the interests of patients in their health records. It proves that blockchain can solve the issues of security, auditing, and access control in healthcare settings. Permissioned blockchains are preferable because of their transaction capability and better privacy. A new approach called the hybrid architecture is applied to big data exchange, allowing data to be stored externally and hashed internally through blockchain technology. Nonetheless, there are still problems, like checking the authenticity of the input data and scaling blockchain technology. Potential future directions involve Zero-Knowledge Proofs, fast blockchain algorithms for IoT devices, smart contracts' security, interoperability across chains, and post-quantum cryptographies for blockchain in healthcare.

VIII. ACKNOWLEDGMENT

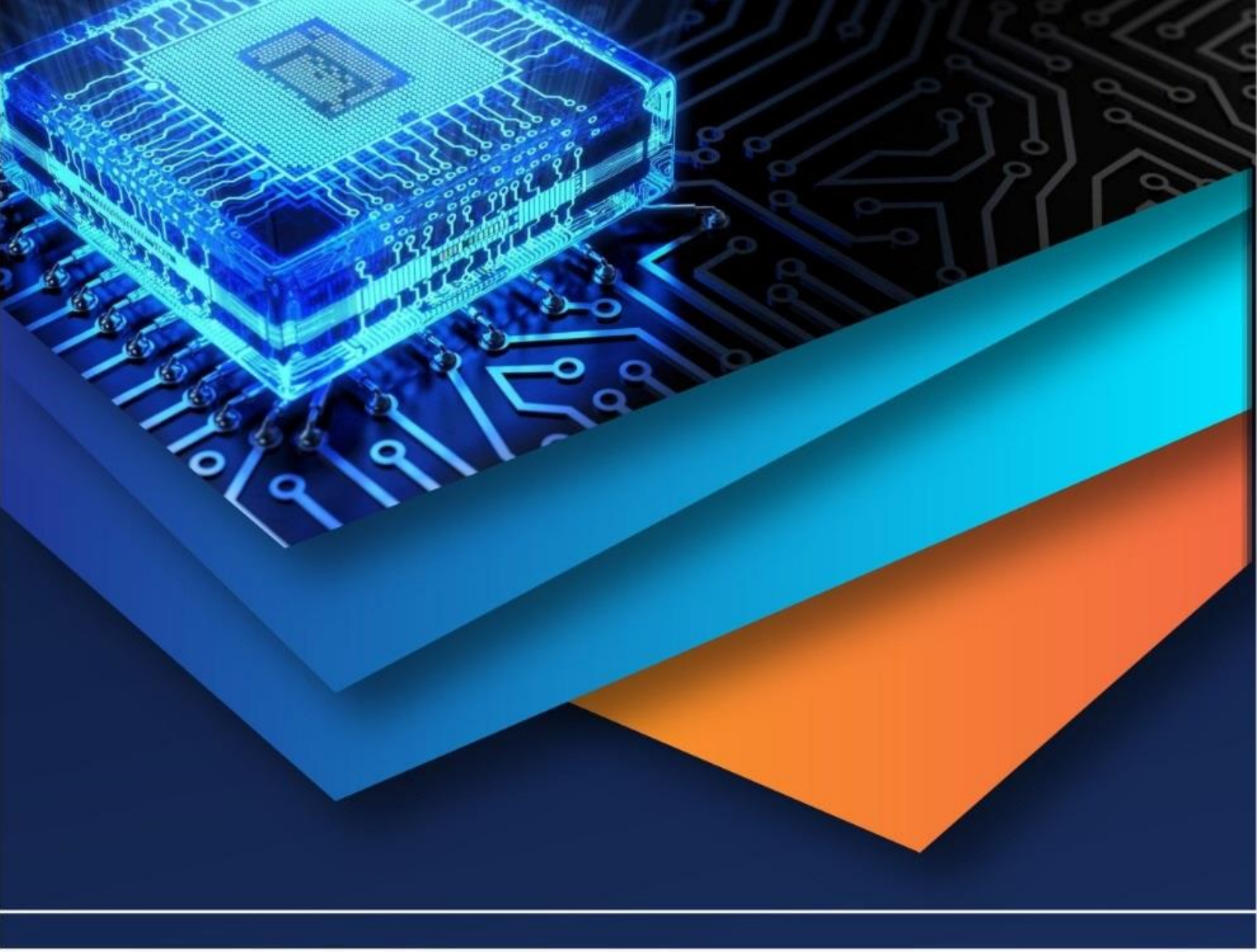
We would like to express sincere gratitude to the Department of Computer Science and Engineering for proving the academic environment and resources that supported the preparation of our review article. Appreciation is extended to the faculty Dr. Prabhakar M whose guidance and construction feedback significantly contributed to the depth and clarity of this work.We also acknowledge the open-access contribution of the research community, whose peer-reviewed publications formed the foundation of this review. The databases IEEE Xplore, Google Scholar, and SpringerLink are acknowledged for providing access to the literature surveyed herein.

REFERENCES

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

[2] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14757–14767, 2017.

[3] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, 2018, pp. 180–184.
[4] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data," Computational and Structural Biotechnology Journal, vol. 16, pp. 267–278, 2018.
[5] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "How blockchain could empower eHealth: An application for radiation oncology," in VLDB Workshop on Data Management and Analytics for Medicine and Healthcare (DMAH), Los Angeles, CA, USA, 2019, pp. 3–13.
[6] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," IEEE Access, vol. 7, pp. 147782–147795, 2019.
[7] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based E-health systems," IEEE Access, vol. 7, pp. 66792–66806, 2020.
[8] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7702–7712, 2020.
[9] A. Farouk, A. Alahmadi, S. Ghose, and A. Mashatan, "Blockchain platform for industrial healthcare: Vision and future opportunities," Computer Communications, vol. 154, pp. 223–235, 2020.
[10] A. H. Mayer, C. A. da Costa, and R. D. R. Righi, "Electronic health records in a Blockchain: A systematic review," Health Informatics Journal, vol. 26, no. 2, pp. 1273–1288, 2021.
[11] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," IEEE Access, vol. 7, pp. 18611–18621, 2022.
[12] O. Ali, A. Jaradat, A. Kulakli, and A. Abuhalimeh, "A comparative study on smart healthcare: Blockchain technology and AI in healthcare applications," Journal of Medical Systems, vol. 47, no. 1, pp. 1–12, 2023.
[13] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin.org, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[14] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY