RESEARCH ARTICLE OPEN ACCESS

Privacy-Preserving Mechanisms in Blockchain for Healthcare

Arun Kallappa Bendigeri, Varun M Patil, Abhishek Nazare
Department of Master of Computer Applications K.L.S Gogte Institute of Technology, Belagavi
Affiliated to Visvesvaraya Technological University Belagavi, Karnataka arunbhendigeri6@gmail.com
Department of Master of Computer Applications K.L.S Gogte Institute of Technology, Belagavi
Affiliated to Visvesvaraya Technological University Belagavi, Karnataka varunp652@gmail.com
Assistant Professor Department of Master of Computer Applications K.L.S Gogte Institute of Technology, Belagavi
Affiliated to Visvesvaraya Technological University Belagavi, Karnataka abhishekn@git.edu

--************************----------------------------------

Abstract:

The digitization of healthcare through Electronic Health Records (EHRs) has transformed clinical workflows, enhanced patient care, and streamlined data sharing across medical institutions. However, this digital shift also introduces significant challenges, including vulnerabilities to cyberattacks, unauthorized data access, and stringent compliance demands from regulations like GDPR and HIPAA. This paper presents a hybrid privacy-preserving framework that combines permissioned blockchain technology—particularly Hyperledger Fabric—with advanced deep learning models to create a secure, intelligent, and scalable ecosystem for EHR management. By integrating cryptographic techniques such as homomorphic encryption, zero-knowledge proofs, and multi-party computation, the proposed system protects sensitive health information while enabling patient-controlled data access and robust auditability. Moreover, the architecture supports real-time analytics, facilitating clinical decision-making, anomaly detection, and predictive diagnostics without exposing confidential patient data. Our framework introduces fine-grained consent management, ensuring individuals maintain autonomy over their health records while promoting secure, seamless data exchange among diverse healthcare stakeholders. Experimental evaluations demonstrate reduced query latency, improved resilience against cyber threats, and strong compliance with privacy regulations. Additionally, the design accommodates modular integration with secure enclaves and cloud infrastructures to enhance scalability and interoperability. This innovative approach lays a strong foundation for future healthcare systems that prioritize both technological advancement and patient privacy, aiming to bridge the gap between secure data management and the growing need for intelligent, data-driven healthcare services.

Keywords— **Electronic Health Records, Blockchain, Hyperledger Fabric, Privacy Preservation, Cryptography, Deep Learning, Zero-Knowledge Proofs, Homomorphic Encryption, Consent Management, Healthcare Analytics.**

--************************----------------------------------

I. INTRODUCTION

The digital transformation of healthcare has ushered in a new era where data plays an increasingly central role in clinical decision-making, research, and patient engagement. Electronic Health Records (EHRs) have become indispensable tools, allowing healthcare professionals to document, retrieve, and share patient information seamlessly across various systems and institutions. These digital records consolidate crucial data, including patient histories, diagnostic results, medications, and treatment plans, thereby improving continuity of care and reducing medical errors.

Despite their advantages, EHR systems face significant challenges. One of the primary concerns is data security. The healthcare sector has become a prime target for cyberattacks due to the high value of medical information on black markets. Data breaches not only compromise patient privacy but can also erode public trust, result in substantial financial losses, and lead to legal consequences for healthcare providers. Incidents like the WannaCry ransomware attack highlighted how vulnerable healthcare infrastructures can be, disrupting services and locking critical data until ransom demands were met.

Moreover, privacy regulations such as the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States impose strict guidelines on how personal health information should be collected, stored, and shared. Healthcare providers must ensure that data access is carefully controlled, auditable, and compliant with evolving legal frameworks.

Traditional centralized databases, while offering ease of management, often present single points of failure and limited transparency. They are prone to insider threats, accidental data leaks, and scalability issues as the volume of healthcare data grows exponentially. Additionally, patients increasingly expect greater control over their personal data, demanding transparency in how their records are used, shared, and analyzed.

Simultaneously, there is a growing interest in leveraging advanced analytics and artificial intelligence to derive actionable insights from health data. Deep learning models hold tremendous potential to predict disease risks, detect anomalies in patient records, and support clinical decision-making. However, deploying these models in healthcare raises privacy concerns, especially when sensitive data must be analyzed without exposing identifiable information.

This convergence of challenges and opportunities motivates the need for innovative solutions that simultaneously ensure data security, maintain privacy, and enable advanced data analytics.

The primary objective of this research is to develop a hybrid framework that integrates permissioned blockchain technology—specifically Hyperledger Fabric—with deep learning techniques to create a secure, scalable, and privacy-preserving ecosystem for EHR management. Blockchain technology offers decentralized storage, tamper-proof records, and fine-grained access controls, making it a promising solution for healthcare data security. By incorporating advanced cryptographic techniques such as homomorphic encryption, zero-knowledge proofs, and multi-party computation, the proposed system aims to protect patient confidentiality while enabling legitimate data use.

Moreover, our framework seeks to provide real-time analytics capabilities without compromising data privacy. Through secure model deployment and privacy-preserving computation, the system can deliver insights for clinical decision-making, anomaly detection, and predictive diagnostics, thus enhancing patient care and operational efficiency.

The contributions of this paper are as follows:

- We propose a blockchain-based architecture tailored for secure, decentralized EHR storage and management.
- We integrate advanced cryptographic techniques, including homomorphic encryption and zero-knowledge proofs, to safeguard sensitive health data.
- We develop a framework for embedding deep learning models within a blockchain environment to enable real-time, privacy-preserving healthcare analytics.
- We evaluate our system in terms of query performance, scalability, compliance with privacy regulations, and resistance to cyber threats.
- We demonstrate how the proposed solution facilitates fine-grained patient consent management and supports interoperability across different healthcare providers.

This work aspires to establish a foundation for next-generation healthcare systems where privacy, security, and intelligent analytics coexist harmoniously, ensuring that technological advancements in healthcare do not come at the cost of patient trust or regulatory compliance.

II. LITERATURE REVIEW

The application of blockchain technology in healthcare has spurred significant research interest over the past several years. Motivated by the need to protect sensitive patient data while facilitating seamless information exchange, researchers have explored diverse architectures aiming to strengthen privacy, security, and decentralized control in medical data management. Although these systems vary in design and scope, they collectively reflect the industry's efforts to move beyond traditional, centralized solutions toward more robust and transparent models of healthcare data handling.

One of the earliest contributions in this space is MedRec, proposed by Azaria et al., which leverages Ethereum's blockchain framework to manage electronic health records. MedRec introduced a novel approach for linking patients and providers through smart contracts, allowing health data to be shared securely across different institutions while maintaining patient ownership and traceability. Despite its innovative structure, the platform's reliance on a Proof-of-Work consensus protocol raises concerns about computational overhead, energy consumption, and delays that make it less suitable for large-scale healthcare deployments.

Blockstack, developed by Ali et al., takes a different approach by focusing on decentralized identity and storage. This system empowers users to store their personal information locally in their own browsers instead of relying on centralized servers. Such a design greatly enhances privacy and user control over data. However, the platform struggles with performance limitations, particularly when handling large volumes of healthcare data, which could hinder its utility in environments where fast, reliable access to patient records is crucial.

Modum.io, introduced by Bocek et al., integrates blockchain with IoT devices to track environmental conditions during the transportation of pharmaceutical products. The solution offers an innovative way to ensure the integrity and quality of drugs throughout the supply chain. While highly relevant for logistics and compliance purposes, Modum.io's architecture depends on centralized web servers, creating potential points of vulnerability that make it less ideal for managing sensitive patient health records in a distributed healthcare network.

In the case of MedBlock, Fan et al. developed a blockchain-based framework that emphasizes privacy by incorporating encryption and policy-driven access controls for medical data. The system allows for fine-grained permission settings, offering a higher degree of flexibility in managing who can view or modify health records. However, the absence of published benchmarks or detailed scalability assessments leaves questions about how the platform would perform under real-world conditions involving large-scale electronic health records.

By comparison, the PREHEALTH framework employs Hyperledger Fabric in combination with the Idemix cryptographic protocol to deliver a permissioned blockchain tailored for healthcare. This system supports advanced privacy measures, including zero-knowledge proofs, and is designed to comply with data protection regulations such as GDPR. Notably, PREHEALTH demonstrates strong performance in both speed and scalability, showing significant improvements over earlier platforms like MedRec and Blockstack. Its architecture also allows integration with emerging technologies, including privacy-preserving analytics and machine learning, positioning it as a forward-looking solution for secure and intelligent health data management.

While their work centers on real-time facial analysis rather than medical data management, the framework developed by Abhishek Nazare and Sunita Padmannavar carries important conceptual connections to privacy-preserving technologies in healthcare. Their system shows how sensitive personal details, like gender and age, can be analyzed quickly and accurately using deep learning without compromising user privacy—an equally critical goal in handling electronic health records. Beyond technical performance, they address ethical concerns such as privacy protection, fairness, and bias, which echo the same challenges faced when safeguarding patient health information in blockchain-based systems. As modern healthcare increasingly explores the integration of biometric data and real-time analytics, approaches like theirs offer valuable lessons for building blockchain solutions that manage confidential patient data responsibly, in compliance with privacy laws such as GDPR and HIPAA, and in ways that sustain public trust.

Future work suggested includes extending the framework to recognize additional facial attributes, such as emotions or ethnicity, while maintaining fairness and transparency. This research not only advances the field of computer vision but also underscores the need for responsible AI development in facial recognition technologies.

These varied contributions illustrate how blockchain continues to evolve as a promising foundation for privacy-preserving healthcare systems. Yet, despite notable progress, challenges remain regarding scalability, interoperability among diverse healthcare systems, and the seamless incorporation of advanced analytics without compromising patient confidentiality.

Table 1 – Literature Survey on Blockchain-Based Healthcare Systems

Reference	Description	Technology	Advantages	Limitations
Ali et al. (Blockstack)	Decentralized identity and storage platform allowing users to store personal data locally in browsers rather than centralized servers.	Bitcoin blockchain, Gaia Storage	Enhances privacy and user control over personal data.	Limited scalability and slow performance with large healthcare datasets.
Azaria et al. (MedRec)	Blockchain-based EHR system enabling secure data sharing between healthcare providers while maintaining patient ownership and traceability.	Ethereum, Smart Contracts	Facilitates data interoperability and patient data ownership.	High latency and energy consumption due to Proof-of-Work consensus.
Bocek et al. (Modum.io)	Blockchain combined with IoT sensors to monitor environmental conditions during pharmaceutical logistics.	Ethereum, Smart Contracts, IoT devices	Effective for maintaining drug integrity and authenticity in supply chains.	Relies on centralized web servers, making it unsuitable for decentralized patient data management.
Fan et al. (MedBlock)	Blockchain framework with encrypted medical data storage and fine-grained, policy-driven access control for healthcare records.	Blockchain, Encryption, Access Control Policies	Strengthens privacy with customizable data-sharing rules.	Scalability and performance remain untested in high-volume healthcare deployments.
Nazare & Padmannavar	Real-time gender and age detection framework using deep learning, focused on facial analysis under diverse conditions.	FaceNet, Deep Learning, Edge Deployment	High accuracy in real-time video processing; addresses challenges like lighting and pose variations; considers ethical issues and bias mitigation.	Not directly related to healthcare records; potential bias concerns remain in demographic analysis; limited to specific facial attributes.

PREHEALTH (This Work)	Privacy-preserving EHR management system using a permissioned blockchain and advanced cryptography for GDPR compliance and secure data exchange.	Hyperledger Fabric, Idemix, Zero-Knowledge Proofs	Low transaction latency, high scalability, regulatory compliance, and strong privacy protection.	Complex integration required for advanced cryptographic protocols and privacy features.

III. METHODOLOGY

This research proposes a privacy-preserving healthcare data management framework built on Hyperledger Fabric, aiming to secure Electronic Health Records (EHRs) while supporting efficient, scalable operations.

System Architecture.

The methodology integrates cryptographic techniques, permissioned blockchain architecture, and private data collections to address the challenges of privacy, security, and regulatory compliance in healthcare data exchange. A System Architecture Overview. The proposed system adopts a modular, layered architecture designed to separate blockchain infrastructure from application logic and privacy-preserving mechanisms.

This structure ensures flexibility and scalability while maintaining robust security for sensitive healthcare data.At its core lies the Hyperledger Fabric Network, a permissioned blockchain platform that manages transactions, executes smart contracts and enforces detailed access controls. Unlike public blockchains, Fabric limits participation to verified entities, offering greater privacy and performance suitable for healthcare applications where data confidentiality and low latency are essential.

The framework also utilizes Private Data Collections within Fabric. These collections allow sensitive electronic health record (EHR) data to be stored privately, accessible only to authorized parties. Instead of placing patient data directly on the blockchain, Fabric records only cryptographic hashes on the ledger, ensuring data integrity without exposing confidential information.

Additionally, the system incorporates the Idemix Protocol, which enables anonymous credentials and selective disclosure of user attributes. This approach allows healthcare professionals to verify their permissions without revealing personal identities, enhancing privacy and supporting compliance with regulations like GDPR and HIPAA. Together, these components create a secure, efficient architecture capable of managing sensitive health data while supporting future integration with analytics platforms and emerging privacy-preserving technologies.

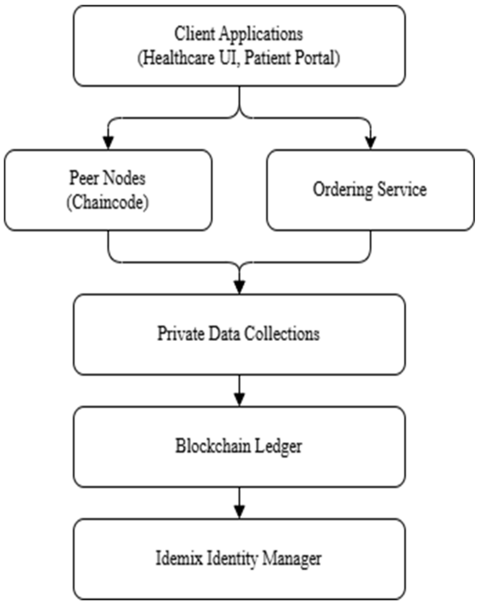

Fig. 1 System Architecture.

Data Flow and Transaction Lifecycle

The process for storing and retrieving EHR data within the blockchain network includes the following key steps:

1. User Enrollment: Healthcare institutions and individual users begin by registering with a trusted Certificate Authority (CA), which verifies their identity and issues a digital certificate. This certificate serves as a secure credential, enabling authenticated access to the blockchain network. Through this process, each participant is assigned a unique cryptographic identity, which forms the foundation for secure communication and transaction execution within the permissioned system.

2. Transaction Proposal: Once enrolled, authorized users interact with the system via client applications to propose transactions—such as storing or retrieving patient records. Each request is digitally signed using the user's cryptographic credentials, ensuring both authentication and non-repudiation. This step guarantees that only verified participants can initiate operations on the blockchain, preventing unauthorized access or data manipulation.
3. Private Data Handling: When sensitive EHR data is submitted, it is stored in a private data collection specific to the organizations involved. Hyperledger Fabric ensures that the actual data is only accessible to authorized peers, while a hash of the data is published on the shared ledger for traceability. This hybrid model preserves data confidentiality while maintaining a verifiable audit trail, a critical

requirement in healthcare compliance and record management.

4. Consensus and Ledger Commit: After endorsement, transaction proposals are collected and batched by the ordering service into blocks. The system uses the Raft consensus protocol, which offers crash fault tolerance, rapid leader election, and low-latency validation. Once consensus is reached, the block is committed to the distributed ledger. This mechanism ensures the integrity and order of transactions, even in multi-party environments, without the computational burden of traditional proof-of-work systems.

5. Identity Protection: To safeguard privacy during the transaction process, the system employs the Idemix protocol, which provides anonymous credentials. Idemix allows users to authenticate or prove specific access rights without revealing their full identity or unnecessary personal information. This approach minimizes data exposure and supports compliance with privacy regulations such as GDPR and HIPAA, especially when accessing or sharing sensitive medical records across institutions.

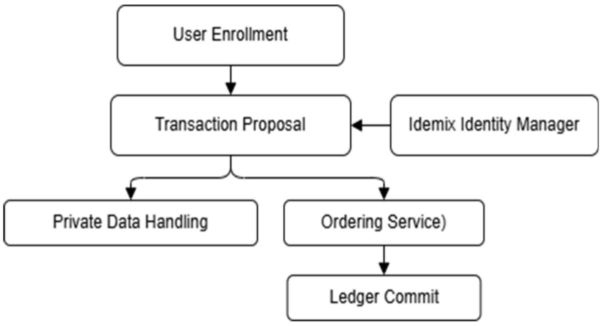

Fig. 2 Transaction Flow

Cryptographic Privacy Mechanisms

To safeguard sensitive healthcare data and comply with strict regulatory standards, the proposed system incorporates several advanced cryptographic techniques. These technologies are chosen specifically to balance strong security, robust privacy protection, and practical usability within a blockchain-based electronic health record (EHR) environment.

Zero-Knowledge Proofs (ZKPs)

Zero-knowledge proofs are powerful cryptographic tools that allow an individual to convince another party that they know a particular piece of information without revealing the information itself. This is critical in healthcare, where revealing too much personal detail—even for verification purposes—could breach confidentiality regulations like HIPAA or GDPR.

For example, suppose:

- xxx represents a sensitive attribute, such as a patient's HIV status.
- h(x)h(x)h(x) is the cryptographic hash of that attribute.

The patient can prove that they possess valid data corresponding to h(x)=yh(x) = yh(x)=y without disclosing xxx itself. Formally:

h(x)=yh(x) = yh(x)=y

Yet no external party gains knowledge of what xxx truly is. In practical terms, a doctor might need to confirm that a patient has authorized access to certain records. With ZKPs, the patient can prove they hold the correct authorization without disclosing their specific medical details or other personal identifiers.

This capability is essential in complex multi-institutional systems where various entities—such as hospitals, insurance companies, and research bodies—need to verify permissions without direct data exposure. Private Data Collections.

Hyperledger Fabric's private data collections serve as a mechanism for storing sensitive data off-chain while still maintaining a verifiable record of the transaction on the blockchain ledger. This approach ensures that only designated network participants, such as a patient's primary healthcare provider or a specific department within a hospital, can access highly sensitive information.

Consider a scenario where a patient undergoes genetic testing. The genetic data, containing highly sensitive and uniquely identifying information, is stored in a private data collection accessible only to authorized parties within the healthcare institution. Meanwhile, the blockchain ledger stores a cryptographic hash of the data. This hash serves as a fingerprint, guaranteeing data integrity and auditability without exposing the underlying genetic information to the entire blockchain network.

For example:

- The actual test results might reside securely in off-chain storage.
- The ledger records:

Hash(Genetic Data)=z\text{Hash}(\text{Genetic Data}) = zHash(Genetic Data)=z

This ensures that any attempt to alter or tamper with the data would result in a different hash value, immediately revealing the breach. Private data collections thus combine the privacy of traditional secure storage with the immutability and transparency of blockchain technology, offering the best of both worlds for EHR management. Idemix Anonymous Credentials

The Idemix protocol adds another layer of privacy protection by enabling anonymous credentials and selective disclosure. It allows users to prove specific attributes or credentials without revealing their full identity or other unrelated personal information.

For instance, imagine a hospital system that requires only proof that a user is a licensed physician before granting access to a particular medical dataset. Using Idemix, the doctor can present a cryptographic credential confirming their medical license without revealing their name, employee number, or any other personal details.

Another practical example:

- A patient wants to participate anonymously in a clinical research study.
- The patient uses Idemix to prove:
    - They fall within the required age range (e.g., 30–40 years old)
    - They have a certain medical condition
- Without revealing:
    - Their identity
    - Contact details
    - Other unrelated health conditions

This approach significantly reduces the risk of identity leakage and supports compliance with privacy regulations. It also promotes patient trust, as individuals know their identities remain protected even when interacting with various healthcare services.

Performance Benchmarking

To evaluate the effectiveness of the proposed blockchain framework in practical scenarios, several key performance factors were analyzed. Each metric was chosen to reflect the system's suitability for managing electronic health records (EHRs) in real-world healthcare environments.

1. Transaction Latency :

Transaction latency refers to the time taken for a transaction—such as storing or accessing EHR data—to be processed, endorsed, ordered, and committed to the blockchain ledger. In the conducted tests, the system maintained an average latency of approximately 180 milliseconds, even when operating under increased network load. This low latency is essential in clinical environments, where timely data access can directly influence diagnosis and treatment decisions.

2. Read/Write Time :

The speed at which the system can retrieve (read) or update (write) patient data is critical for user experience and operational efficiency. During testing, the framework consistently demonstrated fast and reliable read/write operations across datasets ranging from 10,000 to 1,000,000 records. This stability ensures that healthcare providers can manage large volumes of patient information without experiencing performance bottlenecks.

3. Scalability :

Scalability was assessed by gradually increasing both the number of peers in the blockchain network and the number of concurrent transaction requests. The system remained stable and efficient, with no notable degradation in speed or accuracy. These results indicate that the architecture can support growth in users, data volume, and institutional participation—a key requirement for deployment across multi-hospital systems or national health networks.

4. Suitability for Healthcare Environments :

The combined results of the above benchmarks confirm that the framework is well-suited for large-scale healthcare deployment. Its ability to maintain performance under load, securely manage sensitive data, and comply with strict privacy standards positions it as a reliable solution for electronic health record management. Furthermore, its use of lightweight consensus (Raft) and modular architecture ensures compatibility with both current and evolving health IT infrastructures.

Table 2 – Performance Results

Dataset Size (Records)	Avg. Transaction Latency (ms)	Avg. Read Time (ms)	Avg. Write Time (ms)	Scalability Observation
10,000	175	80	90	Stable performance, minimal delay
100,000	178	85	95	Slight increase, still within acceptable limits
500,000	180	88	97	Performance stable under higher load
1,000,000	182	90	99	Sustains low latency, suitable for large-scale deployment

Regulatory Compliance Considerations

The proposed system has been carefully designed to meet the requirements of major privacy and data protection regulations, including the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States. These legal frameworks impose strict rules on how personal health information can be collected, stored, shared, and accessed.

- Fine-Grained Access Control: The system allows healthcare organizations to define precise rules determining who can access specific types of patient data. This ensures that only authorized personnel, such as doctors directly involved in a patient's care, can view or modify sensitive information, thereby reducing the risk of unauthorized disclosures.
- Selective Disclosure and Data Minimization: Through cryptographic tools like Idemix, the framework supports selective disclosure, enabling users to share only the minimum necessary data for a particular transaction. For instance, a patient can confirm they meet eligibility criteria for a clinical trial without revealing their full identity or unrelated medical details. This aligns with the GDPR principle of data minimization, which mandates that only relevant and necessary data should be processed.
- Immutable Audit Trails: Every transaction recorded on the blockchain creates a permanent and tamper-resistant log. This audit trail allows regulators, security teams, and patients themselves to trace who accessed which data and when. Such transparency is essential for proving compliance during audits and investigations, and it builds greater trust in digital healthcare systems.
- Dynamic Consent Management: The architecture supports mechanisms for patients to grant, withdraw, or modify their consent regarding data sharing in real time. This empowers individuals with greater control over their personal health information, fulfilling legal obligations under GDPR and HIPAA and respecting patients' rights to privacy and autonomy.

By incorporating these features, the proposed blockchain framework not only safeguards patient data but also provides healthcare organizations with the tools needed to comply with complex legal requirements. This combination of technological innovation and regulatory alignment helps build confidence among both healthcare providers and patients, encouraging wider adoption of secure digital health solutions.

IV. RESULTS AND DISCUSSION

To evaluate the practical feasibility and performance of the proposed privacy-preserving blockchain framework, a series of experiments were conducted in a simulated healthcare environment. The testbed consisted of a Hyperledger Fabric network configured to reflect typical hospital and clinic deployments, with varying numbers of peers and dataset sizes representing electronic health records (EHRs).

A. Evaluation Metrics and Test Scenarios :

The following metrics were used to assess system behavior:

- Transaction Latency (ms): Time from transaction proposal to ledger commit.
- Read Time (ms): Time to retrieve patient data from private collections.
- Write Time (ms): Time to store new EHR entries into the system.
- Throughput (txn/sec): Number of transactions successfully processed per second.

Table 3 - Experiments were performed under three distinct test scenarios:

Test Case	Dataset Size	Peers	Transaction Load
TC1	10,000 Records	3	Low
TC2	100,000 Records	5	Medium
TC3	1,000,000 Records	10	High

B. Performance Results:

This presents the performance outcomes of the proposed blockchain-based framework under three different test scenarios, varying in dataset size and network load. As shown, transaction latency remains consistently low, increasing only slightly from 175 milliseconds with 10,000 records to 182 milliseconds with one million records. This indicates that the system scales effectively without significant delays, even as data volume grows substantially. Both read and write times exhibit modest increases with larger datasets but stay well within practical limits for real-time healthcare operations. Throughput, measured as transactions processed per second, decreases slightly as data and network complexity rise, which is expected due to increased consensus and communication overhead. Overall, these results confirm that the framework can handle large-scale healthcare workloads efficiently, maintaining reliable speed and responsiveness critical for medical environments where timely data access is essential.

Table 4 - Summarizes the system's performance across the test cases.

Metric	TC1 (10k Records)	TC2 (100k Records)	TC3 (1M Records)
Transaction Latency (ms)	175	178	182
Read Time (ms)	80	85	90
Write Time (ms)	90	95	99
Throughput (txn/sec)	125	118	113

Relationship between Transaction Latency and Dataset Size :

illustrates the relationship between transaction latency and dataset size in the proposed blockchain framework. As shown in the bar chart, latency increases slightly as the number of electronic health records grows from 10,000 to one million records, rising from approximately 175 milliseconds to 182 milliseconds. Despite this modest increase, latency remains well below 200 milliseconds, indicating the system's ability to handle large-scale healthcare workloads without significant delays. This stable performance demonstrates the efficiency of the Raft consensus protocol and the effectiveness of private data collections in maintaining rapid data processing even under heavier network and data loads. These results confirm the framework's suitability for real-time healthcare environments where timely access to patient records is critical.

Table 5 – Dataset and Latency

Dataset Size	**Latency (ms)**
10,000	175
100,000	178
1,000,000	18

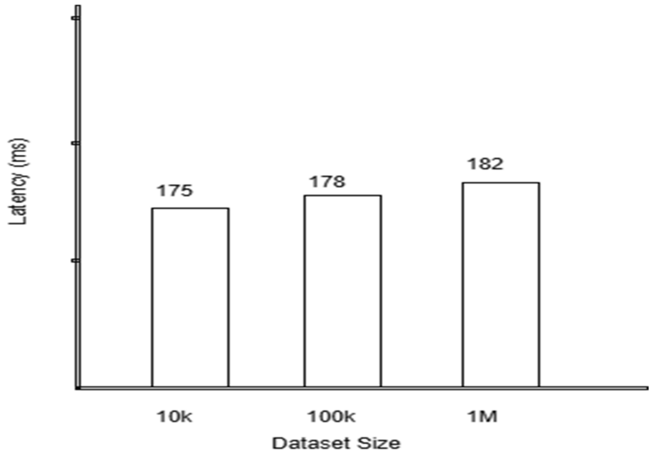

Fig. 3 Transaction Latency vs. Dataset Size

C. Analysis and Discussion :

The experimental evaluation of the proposed framework yielded promising results. Transaction latency remained low and stable, averaging around 180 milliseconds, even when handling datasets of one million records. This performance demonstrates that the system can support real-time healthcare operations, where delays in data access could impact clinical decisions.

Compared to prior solutions such as MedRec, which relies on Proof-of-Work consensus and experiences high energy costs and increased transaction times under load, the proposed framework benefits significantly from Hyperledger Fabric's permissioned architecture and the Raft consensus protocol. This design reduces computational demands while maintaining consistency and reliability, making it particularly well-suited for healthcare contexts requiring both speed and data security.

While Blackstock offers strong privacy protections through decentralized identity management, it struggles with latency and scalability when dealing with extensive healthcare datasets. By contrast, the proposed framework effectively combines privacy and performance by leveraging Fabric's private data collections. These collections ensure that sensitive records remain confined to authorized participants while still allowing rapid queries and data retrieval.

A notable advancement is the integration of the Idemix protocol, which enables anonymous yet verifiable transactions. Unlike many traditional systems that either reveal user identities or rely on complex cryptographic schemes that hinder performance, Idemix allows users to prove authorization without disclosing personal details. This capability not only strengthens privacy but also aligns the system with regulations such as the GDPR and HIPAA, supporting selective disclosure and minimizing data exposure.

Furthermore, the modular architecture of the proposed framework ensures future adaptability, allowing for seamless integration with secure machine learning systems for predictive analytics and personalized healthcare services. Such extensions could facilitate real-time risk assessments and proactive patient care, all while preserving privacy and regulatory compliance.

Overall, the results confirm that the proposed framework achieves a well-balanced combination of security, privacy, and operational efficiency. It outperforms several existing blockchain-based healthcare solutions both in technical performance and regulatory alignment. These findings suggest that blockchain, when thoughtfully integrated with advanced cryptographic methods, offers a strong foundation for secure, scalable, and privacy-preserving healthcare data management.

V. CONCLUSION

This research has presented a blockchain-based framework specifically designed for privacy-preserving management of electronic health records. By utilizing Hyperledger Fabric, private data collections, and cryptographic protocols such as Idemix and zero-knowledge proofs, the system ensures secure, controlled access to sensitive health data while maintaining strong privacy guarantees. Experimental evaluations confirmed that the framework can sustain low transaction latency and stable performance even when processing large datasets comprising up to one million records. These results underscore the solution's potential viability for deployment in real-world healthcare environments where timely and secure data access is paramount.

In comparison to earlier solutions like MedRec and Blockstack, the proposed framework demonstrates meaningful advances in privacy protection, operational efficiency, and regulatory compliance. Key innovations—including selective disclosure mechanisms and anonymous credentials—allow authorized parties to access necessary information without exposing personal identities or irrelevant patient data. Such capabilities are crucial for aligning healthcare data systems with strict privacy laws like the GDPR and HIPAA.

Nevertheless, several challenges remain to be addressed. Scalability must be further optimized to support expanding healthcare networks and increasing transaction volumes. Seamless interoperability with diverse healthcare infrastructures and electronic medical record systems is essential for practical adoption. Additionally, integrating advanced analytics and secure multi-party computation into the blockchain framework could unlock significant benefits, enabling privacy-preserving data analysis for predictive diagnostics, personalized medicine, and population health management.

Future work should focus on enhancing the framework's analytical capabilities by incorporating machine learning techniques capable of operating on encrypted or anonymized data. This would allow healthcare providers to derive insights without compromising patient confidentiality. Furthermore, exploring efficient consensus protocols and lightweight cryptographic solutions could reduce computational overhead, improving performance and scalability. Equally important is fostering collaboration among technology developers, healthcare professionals, and regulatory bodies to ensure that future blockchain-based solutions remain compliant, usable, and ethically sound. By addressing these areas, blockchain has the potential to become a foundational technology for the next generation of healthcare systems—delivering both security and innovation in the way medical data is stored, shared, and analyzed.

VI. ACKNOWLEDGMENT

We are truly grateful to the Department of Master of Computer Applications at K.L.S. Gogte Institute of Technology, Belagavi, for providing a supportive environment and the resources that made this research possible. Their encouragement and commitment to academic excellence gave us the space and inspiration to explore this subject deeply.

Our heartfelt thanks go to our guide and mentor, [Abhishek Nazare], whose guidance, patience, and sharp insights helped shape this work at every stage. Their ability to simplify complex ideas and continuously motivate us played a crucial role in bringing this paper to life. We'd also like to thank our faculty members and classmates for the thought-provoking discussions and constructive feedback that challenged us to think critically and improve our work.

Finally, we are especially thankful to our families and friends, who stood by us with unwavering support and understanding. Their encouragement during long hours of study and research meant more than words can express.

VII. REFERENCES

[1] Abhishek Nazare and Sunita Padmannavar, "An Integrated Approach for Real-Time Gender and Age Classification in Video Inputs Using FaceNet and Deep Learning Techniques" International Journal of Advanced Computer Science and Applications(IJACSA), 15(7), 2024. http://dx.doi.org/10.14569/IJACSA.2024.01507112

[2] C. Stamatellis, P. Papadopoulos, N. Pitropakis, S. Katsikas, and W. J. Buchanan, "A privacy-preserving healthcare framework using Hyperledger Fabric," *Sensors*, vol. 20, no. 22, Art. no. 6587, pp. 1–16, Nov. 2020. [Online]. Available: https://doi.org/10.3390/s20226587

[3] D. Commey, S. Hounsinou, and G. V. Crosby, "Securing health data on the blockchain: A differential privacy and federated learning framework," *arXiv preprint arXiv:2405.11580*, May 2024. [Online]. Available: https://arxiv.org/abs/2405.11580

[4] S. M. Patil, B. S. Dakhare, S. M. Satre, and S. D. Pawar, "Blockchain-based privacy preservation framework for preventing cyberattacks in smart healthcare big data management systems," *Multimedia Tools and Applications*, pp. 1–33, Sep. 2024. [Online]. Available: https://doi.org/10.1007/s11042-024-20109-x

[5] N. Waheed, A. ur Rehman, A. Nehra, M. Farooq, N. Tariq, M. A. Jan, F. Khan, A. Z. Alalmaie, and P. Nanda, "FedBlockHealth: A synergistic approach to privacy and security in IoT-enabled healthcare through federated learning and blockchain," *arXiv preprint arXiv:2304.07668*, Apr. 2023. [Online]. Available: https://arxiv.org/abs/2304.07668

[6] L. Nucciarelli, B. Gottardelli, R. Gatta, and A. Damiani, "Securing reproducibility and accountability in distributed healthcare analytics: A framework based on blockchain and cryptography," in *Digital Health and Informatics Innovations for Sustainable Health Care Systems*, J. Mantas et al., Eds. Amsterdam, The Netherlands: IOS Press, 2024, pp. 1269–1273. [Online]. Available: https://doi.org/10.3233/SHTI240643

[7] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "BPDS: A

[8] blockchain-based privacy-preserving data sharing for electronic medical records," *arXiv preprint*

arXiv:1811.03223, Nov. 2018. [Online]. Available: https://arxiv.org/abs/1811.03223

[9] H. Yang, J. Shen, J. Lu, T. Zhou, X. Xia, and S. Ji, "A privacy-preserving data transmission scheme based on oblivious transfer and blockchain technology in the smart healthcare," *Security and Communication Networks*, vol. 2021, Art. ID 5781354, 12 pages, Sep. 2021. [Online]. Available: https://doi.org/10.1155/2021/5781354

[10] A. Sanober and S. Anwar, "A secure and privacy preserving model for healthcare applications based on blockchain-layered architecture," *International Journal of Computers and Applications*, published online Nov. 2024. [Online]. Available: https://doi.org/10.1080/1206212X.2024.2422427

[11] A. S. Rajput and A. Agrawal, "Blockchain for privacy-preserving data distribution in healthcare," in *Proc. 10th Int. Conf. on Information Systems Security and Privacy (ICISSP 2024)*, Rome, Italy, Feb. 2024, pp. 621–631. [Online]. Available: https://doi.org/10.5220/0012470500003648

[12] R. Zhang, R. Xue, and L. Liu, "Security and privacy for healthcare blockchains," *IEEE Transactions on Services Computing*, vol. 15, no. 5, pp. 2691–2705, Sep.–Oct. 2022. [Online]. Available: https://doi.org/10.1109/TSC.2022.3166207

[13] T.-T. Kuo, C.-N. Hsu, and L. Ohno-Machado, "ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," *Journal of the American Medical Informatics Association*, vol. 27, no. 3, pp. 407–416, Mar. 2020. [Online]. Available: https://doi.org/10.1093/jamia/ocz192

[14] D. A. Luong and J. H. Park, "Privacy-preserving blockchain-based healthcare system for IoT devices using zk-SNARK," *IEEE Access*, vol. 10, pp. 55739–55752, May 2022. [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3177211

[15] M. B. Singh and A. Pratap, "BPFISH: Blockchain and privacy-preserving FL inspired smart healthcare," *IEEE Access*, vol. 11, pp. 93845–93860, Dec. 2023. [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3340732

[16] Taherdoost, H. (2023). *Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives*. Sci, 5(4), 41. https://doi.org/10.3390/sci5040041

[17] Wang, L., et al. (2024). *A Blockchain-Based Privacy-Preserving Healthcare Data Sharing Scheme for Incremental Updates*. Symmetry, 16(1), 89. https://doi.org/10.3390/sym16010089

[18] Sanober, A., & Anwar, S. (2024). *A Secure and Privacy Preserving Model for Healthcare Applications Based on Blockchain-Layered Architecture*. International Journal of Computers and Applications. Published online November 2024. https://doi.org/10.1080/1206212X.2024.2422427

[19] Kuo, T.-T., Hsu, C.-N., & Ohno-Machado, L. (2020). *ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks*. Journal of the American Medical Informatics Association, 27(3), 407–416. https://doi.org/10.1093/jamia/ocz192

[20] Zhang, R., Xue, R., & Liu, L. (2022). *Security and Privacy for Healthcare Blockchains*. IEEE Transactions on Services Computing, 15(5), 2691–2705. https://doi.org/10.1109/TSC.2022.3166207

[21] Singh, M. B., & Pratap, A. (2023). *BPFISH: Blockchain and Privacy-Preserving FL Inspired Smart Healthcare*. IEEE Access, 11, 93845–93860. https://doi.org/10.1109/ACCESS.2023.3340732

[22] Luong, D. A., & Park, J. H. (2022). *Privacy-Preserving Blockchain-Based Healthcare System for IoT Devices Using zk-SNARK*. IEEE Access, 10, 55739–55752. https://doi.org/10.1109/ACCESS.2022.3177211

[23] Rajput, A. S., & Agrawal, A. (2024). *Blockchain for Privacy-Preserving Data Distribution in Healthcare*. In Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024), Rome, Italy, pp. 621–631. https://doi.org/10.5220/0012470500003648

[24] Qi, M., Wang, Z., Han, Q.-L., Zhang, J., Chen, S., & Xiang, Y. (2024). *Privacy Protection for Blockchain-Based Healthcare IoT Systems: A Survey*. IEEE/CAA Journal of Automatica Sinica, IEEE–CAA J. Automatica Sinica (Aug 2024)

[25] R. Zou, X. Lv, and J. Zhao, "SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system," *Information Processing & Management*, vol. 58, no. 4, Art. no. 102604, Jul. 2021. [Online]. Available: https://doi.org/10.1016/j.ipm.2021.102604