Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 09 Issue 02
2025

Research Article
https://doi.org/10.56979/902/2025

Privacy-Aware E-Health Data Sharing via Decentralized Blockchain System

Usama Ahmed[1*], Afzaal Hussain[2], Muhammad Ziad Nayyer[3], Adil Rasheed[4], Sharaiz Shahid[5], and Muhammad Adeel Zahid[4]

[1]Department of Software Engineering, Government College University, Faisalabad, Pakistan.
[2]Department of Information Technology, Government College University, Faisalabad, Pakistan.
[3]Department of Computer Science, GIFT University, Gujranwala, Pakistan.
[4]Center for Data Science, Government College University, Faisalabad, Pakistan.
[5]Institute of Computing, MNS University of Agriculture Multan, Pakistan.
[*]Corresponding Author: Usama Ahmed. Email: usamaahmed@gcuf.edu.pk

Received: June 12, 2025 **Accepted:** August 11, 2025

Abstract: With the growing sensitivity of personal health information (PHI), ensuring secure and privacy-preserving mechanisms for data exchange has become a critical challenge. Blockchain technology, with its inherent properties of immutability, decentralization, and transparency, shows significant promise in reshaping healthcare data management. Unlike existing single-layer approaches, this paper presents a decentralized blockchain-based multi-layer architecture with trapdoor based searchable encryption, designed to enable secure, scalable, and privacy-aware sharing of electronic health records (EHR), consisting of data generation, storage, service, and super service layers. It leverages private and consortium blockchains to preserve data confidentiality and enforce access control through smart contracts. Trapdoor-based searchable encryption enables privacy-preserving queries on encrypted records, ensuring sensitive PHI remains protected yet discoverable by authorized users. Experimental evaluation demonstrates improved access efficiency, reduced cost, and compliance with data privacy regulations. This work highlights blockchain's transformative role in healthcare by ensuring trust, security, and accessibility.

Keywords: Blockchain; Electronic Health Record; Privacy; Smart Contract; Decentralized Systems; Searchable Encryption; e-Health

1. Introduction

Blockchain, commonly known as Distributed Ledger Technology (DLT), provides a tamper-evident and transparent framework for recording digital transactions [1]. It operates as a decentralized and timestamped chain of immutable data blocks, each secured by cryptographic algorithms and maintained by a peer-to-peer network without a central authority [2]. The decentralized nature of blockchain enables trustless participants to exchange sensitive information securely, as all transactions are verifiable and transparent [3].

The term "blockchain technology" is often used broadly, encompassing platforms like Bitcoin, Ethereum, and other decentralized systems, tokens, and smart contracts. Each transaction in blockchain is validated using a consensus algorithm e.g., Proof-of-Work (PoW) or Proof-of-Authority (PoA) and added to the distributed ledger, forming a chronological, immutable chain of records accessible across the network [4]. This structure ensures data integrity, traceability, non-repudiation, and resistance to tampering, making it highly suitable for scenarios where security and transparency are paramount [5]. A simple yet illustrative application is in a ticketing system, where each issued ticket is recorded as a transaction or block. This creates an immutable ledger of sales and transfers, drastically reducing fraud, eliminating the need for intermediaries, and ensuring end-to-end auditability [6, 7]. Key features of the blockchain include:

- Immutability – Once data is recorded on the blockchain, it cannot be altered or deleted, ensuring the integrity of transaction records.
- Decentralization – There is no single point of control; transactions are validated by a distributed network of nodes, enhancing system resilience and trust.
- Transparency – All network participants can view transaction history, which promotes auditability and reduces fraud.
- Security – Cryptographic algorithms secure transactions and user identities, protecting against unauthorized access and data tampering.
- Smart Contracts – Self-executing code that automatically enforces rules and conditions encoded into the blockchain, eliminating the need for intermediaries.

Blockchain applications span multiple industries including finance, supply chains, the Internet of Things (IoT), and healthcare [8, 9]. In the context of healthcare, blockchain is particularly promising for providing data consistency, security, and interoperability among disparate health information systems [10, 11]. Medical records today are often fragmented, inconsistently formatted, and vulnerable to unauthorized access, leading to inefficiencies and risks in clinical decision-making.

The emergence of smart contracts in blockchain 2.0 platforms (e.g., Ethereum) has further enhanced automation and conditional execution of agreements. Despite these advancements, challenges remain in areas such as scalability, compliance, and privacy [2] [9] [12]. E-health involves the use of digital communication systems to support healthcare delivery, including data generation, storage, sharing, and disposal. With the transition from paper-based records to Electronic Health Records (EHRs), concerns around privacy, security, and data accessibility have intensified. Traditional centralized systems are susceptible to unauthorized access, data loss, and integrity compromise [5, 13].

As the healthcare industry continues to adopt digital tools, blockchain provides a robust foundation for building secure, interoperable, and privacy-preserving e-health systems. Unlike physical records stored at disparate locations, EHRs are indexed with metadata, making them easier to search and retrieve, provided they are securely maintained. However, with shared electronic platforms like Shared Electronic Health Records (SEHR), ensuring confidentiality becomes complex as data is no longer confined to a single institution. Legal, technical, and organizational mechanisms must work in unison to enforce data protection policies across distributed systems.

Key requirements for a secure e-health data system include: 1) End-to-end encryption during data transmission and storage, 2) Strict access control mechanisms, 3) Data anonymization and auditability and 4) Protection from insider threats and unauthorized third parties. Blockchain enhances these capabilities by ensuring that each health record is securely stored, timestamped, and verifiable. When healthcare providers exchange information over a blockchain network, every transaction is logged and traceable. This reduces the risk of data loss, unauthorized sharing, or use of outdated information. Moreover, with blockchain, patients retain control over their health data through cryptographic keys, enabling selective sharing and revocation of access.

Existing blockchain-based healthcare solutions have primarily focused on either private or consortium blockchains, often emphasizing access control, selective encryption, or hybrid storage to enhance privacy and scalability. While these approaches provide useful mechanisms, they are generally limited to a single-layer structure and struggle to balance strict privacy requirements with cross-institutional interoperability and regulatory oversight. In contrast, the proposed work introduces a multi-layered hybrid architecture that integrates private, consortium, and super-consortium blockchains. This design ensures that sensitive PHI remains confined within private chains, while searchable indexes in consortium chains enable secure data sharing across institutions, and a super-consortium layer provides global governance and auditing. Additionally, the incorporation of trapdoor-based searchable encryption allows privacy-preserving queries on encrypted records, offering stronger guarantees of confidentiality and lower latency in healthcare applications than prior models. Overall, this paper makes the following contributions,

1. A privacy-preserving protocol has been designed using private and consortium blockchains to securely share electronic health records, integrating public key encryption and keyword search for controlled access.

2. A comprehensive analysis has been conducted to evaluate blockchain's impact on various healthcare domains, supported by literature review and real-world use case analysis.
3. The protocol has been deployed on Ethereum using PoW and PoA consensus mechanisms, with results showing that PoA offers superior performance and scalability for healthcare environments.

Following this section, the entire paper is divided into five more sections, with section 2 presenting state-of-the art in blockchain based e-health care systems, section 3 presenting the basic concepts, section 4 presenting the proposed framework, section 5 presenting the result and discussion followed by conclusions in section 6.

2. Literature Review

Tahir et al. [14] propose a blockchain-based healthcare records management framework addressing interoperability, privacy, and security. The design is decentralized, enabling patients and providers to access shared data without central authority. Tamper resistance is assured through immutable ledgers, while privacy protection is strengthened via cryptographic access control. Consensus is realized through permissioned blockchain protocols, reducing transaction overhead but slightly limiting scalability. The framework avoids main-chain congestion by using hybrid off-chain storage for heavy data. Implementation complexity lies in integrating legacy systems and ensuring compliance with healthcare regulations. Overall, the contribution demonstrates a practical step toward secure, interoperable EHRs.

A Zero-Trust permissioned blockchain framework has been introduced in [15] to enhance privacy and interoperability in healthcare. Unlike public decentralized models, decentralization here is semi-restricted, offering accountability within controlled networks. Tamper-resistance remains strong due to distributed validation. Privacy is emphasized via Zero-Trust identity verification, minimizing insider threats. Consensus is optimized using lightweight permissioned protocols, ensuring efficiency in clinical settings. The model relieves pressure on the main chain by restricting transactions to authorized parties, but scalability for cross-institutional deployment is challenging. Implementation is complex due to rigorous identity management integration. This work highlights Zero-Trust as a robust approach for sensitive medical ecosystems.

Reegu et al. [16] develop a blockchain framework for interoperable electronic health records. The system is decentralized, supporting peer-to-peer medical data sharing while ensuring tamper resistance via cryptographic validation. Privacy is maintained through controlled access layers, though broader multi-stakeholder environments present challenges. Consensus relies on a Proof-of-Authority (PoA)-like mechanism, which is faster but somewhat centralized. The framework minimizes pressure on the main chain by relying on smart contracts for access requests. Implementation difficulty is moderate, especially around ensuring compliance with healthcare interoperability standards such as HL7-FHIR. The paper's contribution lies in combining blockchain with established EHR standards for real-world adoption.

Rashid et al. [17] address healthcare supply chains using blockchain, smart contracts, and decentralized storage. Decentralization ensures traceability of medical goods across suppliers. Tamper resistance is achieved through immutable chain-of-custody records. Privacy protection is less emphasized since supply chain transparency is prioritized over confidentiality. Consensus protocols are simplified, designed to accommodate multiple stakeholders without high computational cost. The main-chain pressure is alleviated using decentralized storage (e.g., IPFS), separating data from the core blockchain. Implementation challenges include interoperability with existing logistics systems and industry adoption resistance. The contribution demonstrates blockchain's ability to improve trust and accountability in healthcare logistics.

Authors in [18] presents a distributed blockchain platform for accountable medical data sharing. Decentralization enables patients and institutions to exchange medical data transparently. Tamper resistance is inherent in blockchain's immutability, while privacy is addressed through selective encryption and access policies. Consensus mechanisms are optimized for performance, balancing trust and latency, though not explicitly addressing energy efficiency. The design does impose some pressure on the main chain due to extensive data auditing, which could become bottlenecked at scale. Implementation complexity arises from integrating policy-driven data sharing with blockchain transactions. The work contributes a clear architecture for traceable, auditable medical data exchange.

Our proposed solution addresses these gaps by designing a patient-centric, blockchain-based PHI (Protected Health Information) sharing protocol using private and consortium blockchains. It integrates public-key encryption, keyword-searchable access, and smart contracts for automating consent and enforcing time-limited data permissions. The platform uses a Proof-of-Authority (PoA) consensus mechanism to ensure high throughput, low gas fees, and scalable transaction validation—making it well-suited for real-time clinical use cases [13]. Furthermore, the system supports access revocation, auditable history tracking, and reputation-based governance among participating institutions. By eliminating centralized intermediaries and aligning with healthcare compliance requirements, our framework enhances data integrity, privacy protection, and operational transparency being the key requirements for next-generation eHealth ecosystems [6]. A comparative analysis of the most prominent works with the proposed approach is given in Table 1.

Table 1. Comparative analysis of available literature

Ref	Decentralized	Tamper-resistant	Privacy Protection	Consensus	Pressure on Main Chain	Implementation Difficulty
[14]	Yes (permissioned)	Strong	Cryptographic access control	Permissioned consensus	Low (hybrid storage)	High (legacy integration)
[15]	Semi-decentralized	Strong	Zero-Trust identity management	Lightweight permissioned	Low	High (identity integration)
[16]	Yes	Strong	Controlled access layers	PoA-like	Low (smart contracts)	Moderate (EHR standards)
[17]	Yes	Strong	Limited (focus on transparency)	Simplified consensus	Very Low (IPFS storage)	Moderate–High (logistics integration)
[18]	Yes	Strong	Selective encryption	Optimized consensus	Moderate (data auditing)	High (policy integration)
Proposed Work	Multi-level (private autonomy + consortium collaboration + super-consortium governance)	Strong (immutable records at each layer)	Very strong (encrypted PHI in private chains + searchable indexes)	Mixed (local BFT/PoA in private, permissioned in consortium, federated at super-consortium)	Very Low (indexes shared, not raw PHI)	Moderate–High (multi-layer orchestration + cross-chain query handling)

3. Basic Concepts

3.1. Overview of Blockchain

Blockchain technology refers to a decentralized and distributed digital ledger system that enables secure, transparent, and tamper-proof data exchanges across networks using public key cryptography and consensus algorithms. Unlike traditional centralized systems controlled by banks, corporations, or governments, blockchain operates via peer-to-peer (P2P) validation, ensuring transparency and resistance to data manipulation. The larger the network, the more secure the system becomes.

Although blockchain is often associated with Bitcoin, its application extends to various sectors including finance, supply chain, healthcare, and e-commerce. According to industry reports, major technology firms such as IBM leverage blockchain for supply chain optimization. Blockchain integrates seamlessly with modern digital infrastructures by enabling real-time data handling and enhancing existing IT architectures.

A blockchain consists of blocks linked in a chronological chain, each stamped with a cryptographic hash containing transaction data and the hash of the preceding block. This structure ensures data immutability and integrity. When a new block is generated, it must be verified by multiple nodes before being added to the chain, reinforcing its distributed trust model.

Key components of blockchain architecture include:

- *Node*: A computer within the network
- *Transaction*: The smallest unit of blockchain data
- *Block*: A container for transaction data
- *Chain*: Sequentially linked blocks
- *Miners*: Nodes responsible for validating and adding new blocks
- *Consensus*: Protocol governing agreement among nodes

3.2. Types of Blockchain Networks

- *Public Blockchain:* is a fully decentralized, permissionless network where anyone can join without needing approval from a central authority [3, 19]. Participants can read, write, validate transactions, and even contribute computational power to mine or confirm blocks. This open architecture supports maximum transparency and global accessibility, making it ideal for applications such as cryptocurrencies, with Bitcoin [1] and Ethereum [4] being the most well-known examples. While public blockchains are generally secure due to their large and distributed validator base, their safety relies heavily on user practices—including proper key management and adherence to strict cryptographic security protocols to prevent unauthorized access or exploitation.
- *Private Blockchain*: is a permissioned network where access is limited to pre-approved participants, typically within a single organization or a consortium of trusted entities as depicted in Figure 1. Unlike public blockchains, private blockchains are centrally managed, meaning only designated nodes can read, write, or validate transactions.

  This restricted access model provides enhanced control over governance, scalability, and data privacy, making it particularly suitable for enterprise applications that require regulatory compliance and strict access controls. Private Blockchains also support faster transaction throughput due to fewer nodes and streamlined consensus mechanisms. Prominent examples include Hyperledger Fabric, which is widely used in supply chain and healthcare, and Corda, designed specifically for financial institutions and contractual workflows [20-22].
- *Consortium Blockchain:* is a semi-decentralized, permissioned system governed collectively by a group of pre-selected organizations rather than a single central authority as depicted in

  Figure . In this model, the consensus process is controlled by a consortium, which could include multiple companies, institutions, or government agencies that work together under a shared governance framework.

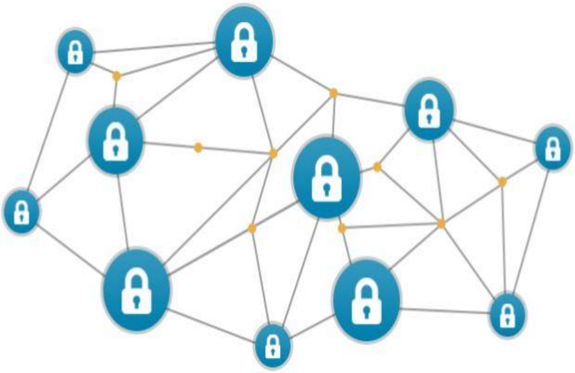


Figure 1. Private Blockchain

- Consortium blockchains strike a balance between the transparency of public networks and the access control of private blockchains, allowing for trusted collaboration among known participants while maintaining a degree of decentralization. This makes them particularly suitable for inter-organizational use cases in sectors such as banking, supply chain, energy, and public administration, where multiple stakeholders need to share, validate, and audit data securely. Examples include Quorum and Hyperledger Besu, which are commonly used in finance and regulatory environments [23, 24].

- *Hybrid Blockchain:* combine features of public and private chains as shown in Figure . They allow selective data access while maintaining transparency. This model is adaptable and suitable for enterprises balancing privacy with accountability [25].

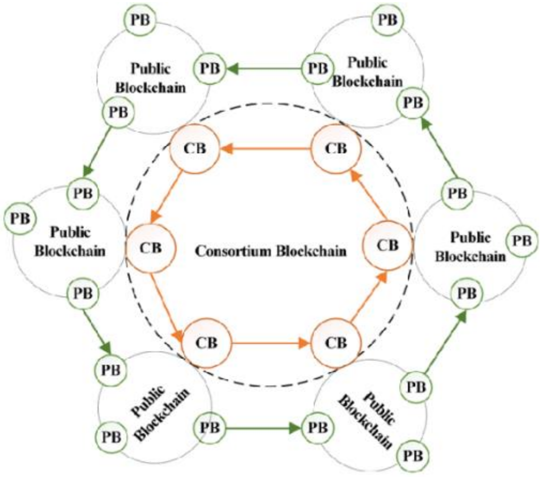


Figure 2. Consortium Blockchain

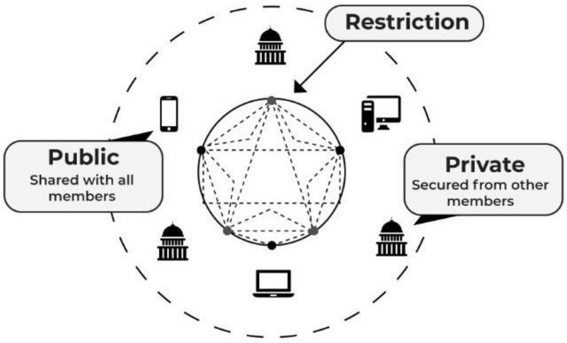


Figure 3. Hybrid Blockchain

- *Decentralization*: In decentralized systems, data is stored across multiple nodes, eliminating reliance on a central authority. This architecture enhances security, reduces bottlenecks, and enables peer-to-peer transactions without intermediaries
- *Transparency*: Blockchain offers pseudonymous transparency. Transactions are visible via public addresses, enabling auditing without revealing personal identities. This accountability is crucial for public institutions and financial systems.
- *Immutability*: Data recorded on a blockchain cannot be altered retroactively due to the cryptographic linkage of blocks. Hash functions ensure that any change in a block would invalidate the entire chain, securing data integrity.

a. Support Functions

- *Merkle Trees:* enhance data verification by aggregating hash values of transactions into a hierarchical structure. Each non-leaf node contains the hash of its children, enabling efficient and secure verification of data integrity. This structure is fundamental to blockchain systems like Bitcoin [26].

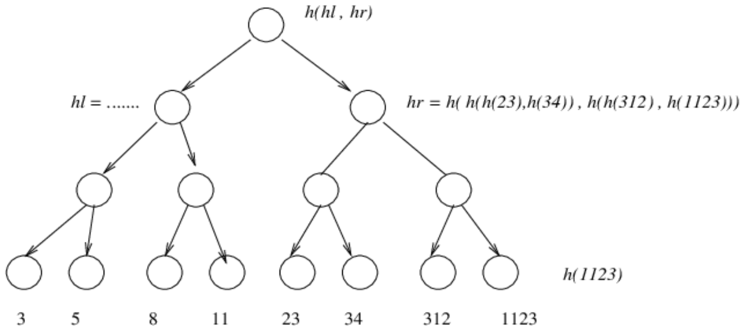


Figure 4. A binary Merkle tree

- *Smart Contracts:* are self-executing digital agreements encoded on the blockchain. These contracts automate processes without intermediaries, reducing cost, time, and fraud risk. First introduced by Nick Szabo in 1997 [27], smart contracts are particularly useful for decentralized applications like crowdfunding platforms and healthcare data sharing.
- *Hash Functions:* Hash functions transform input data of any size into a fixed-length string, ensuring data integrity and consistency. Cryptographic hash functions (e.g., SHA-256) are irreversible, producing a unique digest for each input. Even minor changes in input drastically alter the output, a property known as the avalanche effect.

b. Deployment Architectures

- *Local Deployment:* In traditional on-premise deployments, organizations manage infrastructure, software updates, and security internally. While secure, this model is resource-intensive.
- *Cloud-based PaaS Deployment:* Cloud-based Platform-as-a-Service (PaaS) provides scalability and cost efficiency. It allows institutions to deploy blockchain applications without managing hardware, while maintaining control over their networks.
- *Cloud-based IaaS Deployment:* Infrastructure-as-a-Service (IaaS) further reduces capital expenditure by outsourcing hardware and network services to cloud providers. This model supports rapid deployment and ensures high availability.

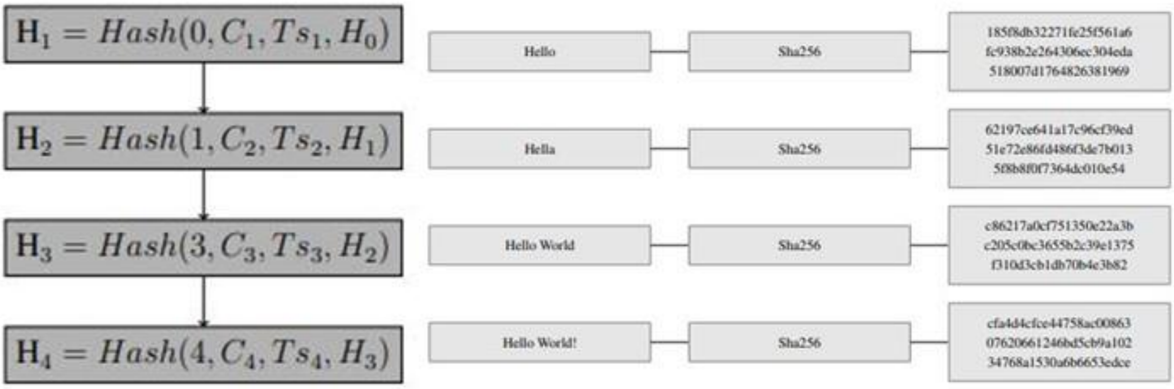

$H_1 = Hash(0, C_1, Ts_1, H_0)$
$H_2 = Hash(1, C_2, Ts_2, H_1)$
$H_3 = Hash(3, C_3, Ts_3, H_2)$
$H_4 = Hash(4, C_4, Ts_4, H_3)$
Hello
Sha256
185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969
Hella
Sha256
62197ce641a17c96cf39ed51e72e86fd486f3de7b0135f8b8f0f7364dc010e54
Hello World
Sha256
c86217a0cf751350e22a3bc205c0bc3655b2c39e1375f310d3cb1db70b4e3b82
Hello World!
Sha256
cfa4d4cfce44758ac0086307620661246bd5cb9a10234768a1530a6b6653edce

Figure 5. Effect of one-way hash functions using Sha256 algorithm

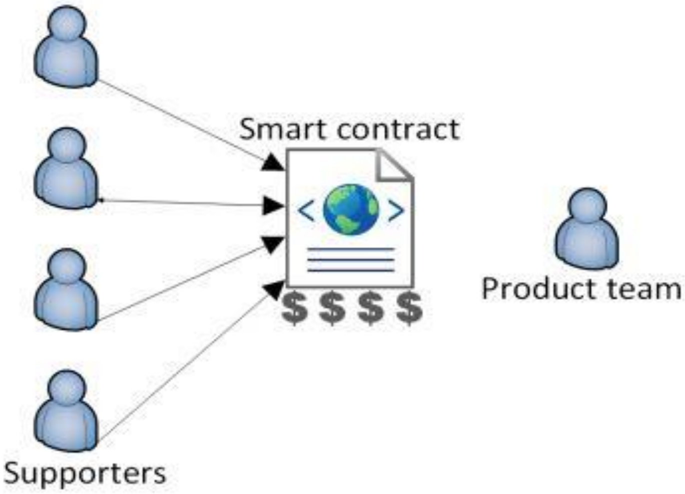


Figure 2. A typical smart contract in Blockchain

4. Proposed Methodology

This section presents the proposed methodology for enabling secure management, sharing, and accessibility of Electronic Health Records (EHRs) central to the modernization of healthcare.

a. System Architecture

The proposed system considers a consortium of hospitals collaborating to securely share patient data using a hybrid blockchain framework. It incorporates both private blockchains for individual hospitals and a consortium blockchain shared among authorized medical entities. Each hospital's private blockchain stores the original Personal Health Information (PHI) of its patients, while authorized external doctors interact through the consortium blockchain to access patient records with appropriate permissions. The architecture emphasizes data protection, access control, confidentiality, secure search, revocation, and role-based system access. Figure 3 illustrates the proposed blockchain-enabled EHR architecture consisting of four-layer namely *i) Data Generation Layer, ii) Data Storage Layer, iii) Service Layer* and *iv) Super Service Layer* described in details as follows.

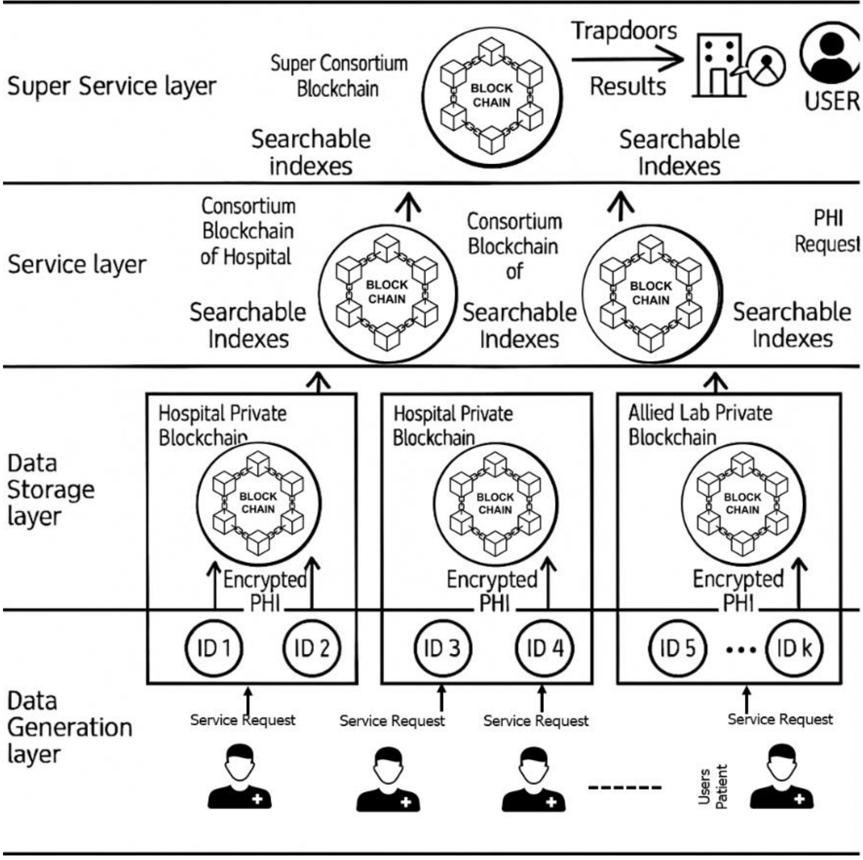


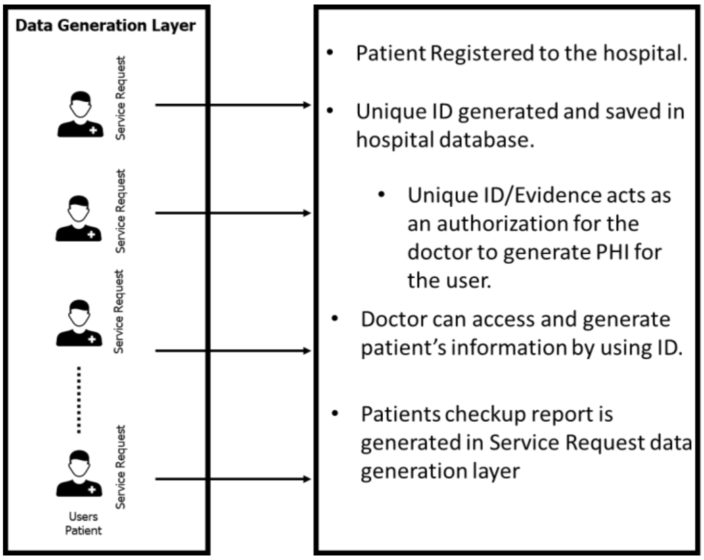
Figure 3. Proposed architecture

i. Data Generation Layer

This is the foundational layer where patients interact with healthcare entities (hospitals, labs, or clinics), generating personally identifiable health information (PHI). Each patient is assigned a unique ID (e.g., ID1, ID2, ... IDk) to tag and manage the corresponding service requests.

- Service requests from users trigger clinical actions and data creation.

- Information includes diagnosis, prescriptions, imaging results, and lab reports.



- Patient Registered to the hospital.
- Unique ID generated and saved in hospital database.
    - Unique ID/Evidence acts as an authorization for the doctor to generate PHI for the user.
- Doctor can access and generate patient’s information by using ID.
- Patients checkup report is generated in Service Request data generation layer

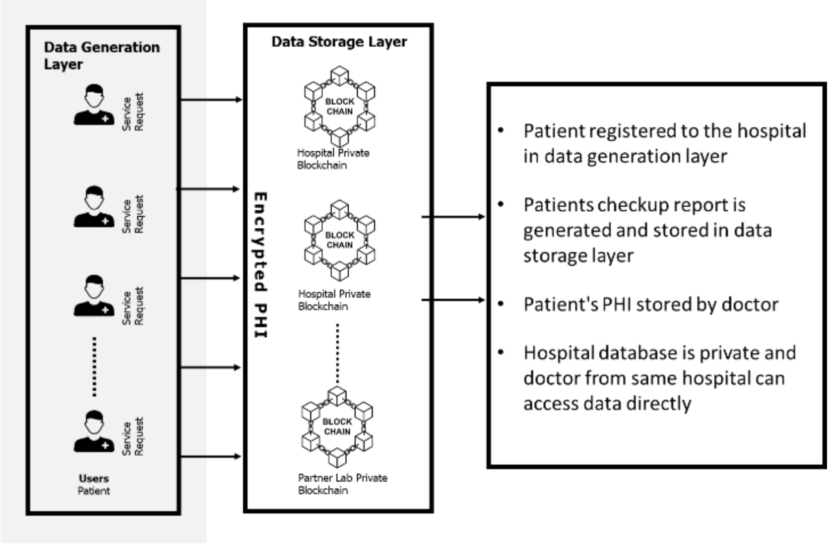
Figure 4. Data Generation layer

ii. *Data Storage Layer*

Encrypted PHI and metadata are stored in Private Blockchains managed by individual healthcare providers (e.g., Hospital A, Hospital B, Allied Labs). This layer ensures that:

- Encrypted PHI is securely stored.
- Access control and audit logs are enforced at the institutional level.

Each institution maintains a local blockchain that stores only their patient records in encrypted form, ensuring data sovereignty and compliance with privacy laws like HIPAA or GDPR. Validated blocks are shared with the consortium blockchain using pseudonymized patient identities and keyword indicators.



- Patient registered to the hospital in data generation layer
- Patients checkup report is generated and stored in data storage layer
- Patient's PHI stored by doctor
- Hospital database is private and doctor from same hospital can access data directly

Figure 5. Data Storage layer

iii. Service Layer

This layer establishes consortium blockchains to enable cross-institutional interoperability. It stores only indexed references of PHI, allowing authorized users to query encrypted records via trapdoor mechanisms. Smart contracts enforce access rights and log activity, while institutions retain data ownership. Through tamper-proof indexing and encrypted request protocols, hospitals and labs can securely collaborate without centralization.

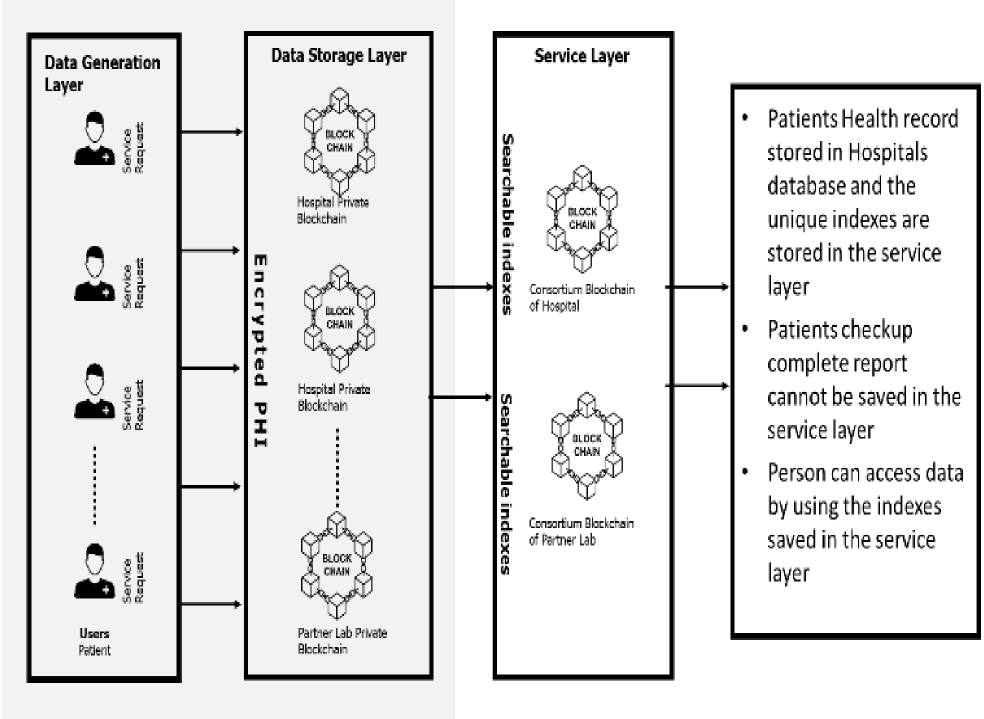

Data Generation Layer
Service Request
Service Request
Service Request
Service Request
Users
Patient
Data Storage Layer
Encrypted PHI
BLOCK CHAIN
Hospital Private Blockchain
BLOCK CHAIN
Hospital Private Blockchain
BLOCK CHAIN
Partner Lab Private Blockchain
Service Layer
Searchable indexes
Searchable indexes
BLOCK CHAIN
Consortium Blockchain of Hospital
BLOCK CHAIN
Consortium Blockchain of Partner Lab
• Patients Health record stored in Hospitals database and the unique indexes are stored in the service layer
• Patients checkup complete report cannot be saved in the service layer
• Person can access data by using the indexes saved in the service layer

Figure 6. Service Layer

iv. Super Service Layer

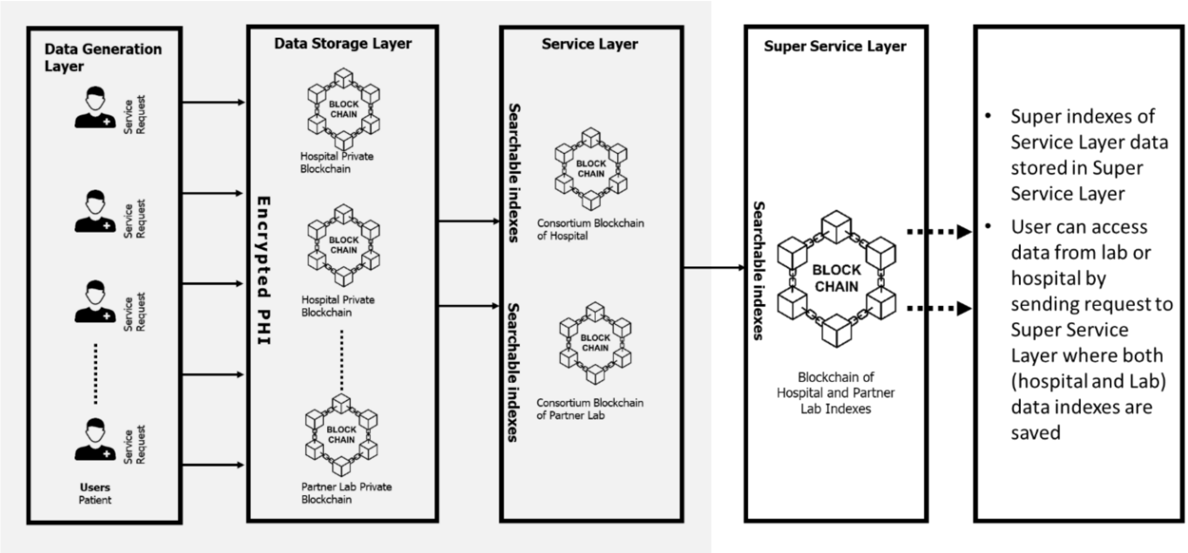

Data Generation Layer
Service Request
Service Request
Service Request
Service Request
Users
Patient
Data Storage Layer
Encrypted PHI
BLOCK CHAIN
Hospital Private Blockchain
BLOCK CHAIN
Hospital Private Blockchain
BLOCK CHAIN
Partner Lab Private Blockchain
Service Layer
Searchable indexes
Searchable indexes
BLOCK CHAIN
Consortium Blockchain of Hospital
BLOCK CHAIN
Consortium Blockchain of Partner Lab
Super Service Layer
Searchable indexes
BLOCK CHAIN
Blockchain of Hospital and Partner Lab Indexes
• Super indexes of Service Layer data stored in Super Service Layer
• User can access data from lab or hospital by sending request to Super Service Layer where both (hospital and Lab) data indexes are saved

Figure 7. Super service layer

The Super Service Layer functions as a unified aggregator of services and searchable indexes across various healthcare institutions, implemented through a Super Consortium Blockchain. Within this framework, users (patients or authorized healthcare entities) submit service requests that initiate privacy-preserving queries. These queries employ trapdoors, which are cryptographic search mechanisms that allow the retrieval of encrypted and relevant data without exposing sensitive content to intermediaries.

Algorithm

```
Begin:
  Input userAddress, username, userNID
  if caller == admin then
    Declare structure User
      String username
      String userNID
    EndStruct
    Declare mapping userRegister(address → User)
    Create a new variable newUser of type User
    Set newUser.username ← username
    Set newUser. userNID ← userNID
    Set userRegister[userAddress] ← newUser
  else
    Reject the function call with error "Unauthorized access"
  end if
End
```

Once processed, the system returns verified and trustworthy results from multiple distributed healthcare providers. This architecture ensures that, regardless of a user's physical location or the origin of care, their complete medical history remains accessible and secure. Moreover, the distributed nature of the blockchain guarantees data integrity and patient privacy while enabling seamless, real-time access through mobile or cloud-based platforms, thereby supporting the vision of truly global, interoperable healthcare.

b. System Workflow

This section presents a stepwise framework for a blockchain-integrated EHR system that addresses data sharing, management, and storage. The workflow start with user creation as described in Algorithm.

1. *Step 1- Clinical Data Generation:* The foundational data originates from patient interactions with healthcare professionals, including general physicians and specialists. This data encompasses medical histories, symptoms, diagnostic notes, and physiological metrics.
2. *Step 2- EHR Creation:* The primary data collected is structured into a comprehensive Electronic Health Record (EHR). In addition to physician-entered information, this EHR may also include *i)* Medical imaging data, *ii)* Prescription and medication histories, *iii)* Treatment and procedural records and *iv)* Laboratory results. This aggregated health profile becomes the basis for data sharing and personalized care.
3. *Step 3- Patient-Centric Ownership and Access Control:* In a blockchain-enabled environment, patients retain ownership of their EHRs. Through smart contracts or access control protocols, they can grant or restrict access to third parties. When healthcare providers or researchers request access, patients have full authority to approve, deny, or conditionally permit data use.
4. *Step 4- Secure Storage via Blockchain and Cloud Integration:* At the heart of the framework lies a distributed storage infrastructure, combining the Cloud-based storage for scalability and Blockchain networks for security and auditability. Blockchain does not store the data itself but logs transactions and access control permissions immutably. This ensures data privacy, integrity, and resilience against tampering or unauthorized use.
5. *Step 5- Decentralized, Global Access to Healthcare Services:* Blockchain enables borderless access to health records. Patients can receive treatment anywhere in the world—from clinics, group care centers, or hospitals—with their data accessible via mobile devices authenticated through distributed ledgers.

Health professionals can provide care based on verified, real-time patient information, promoting continuity of care across regions and systems.

5. Results and Discussion

a. Experimental Setup and Performance Evaluation

The proposed blockchain-based healthcare system was developed and tested within a controlled local Ethereum test network environment. The simulation was executed on a workstation configured with an Intel(R) Core i5-5300 CPU @ 2.30 GHz, 16 GB RAM, and running Windows 10. To simulate blockchain transactions through a web interface, the MetaMask browser extension was employed, providing an interactive and realistic testing experience for user interactions and smart contract executions.

The experimental setup incorporated both Proof-of-Work (PoW) and Proof-of-Authority (PoA) consensus algorithms to comparatively evaluate system performance. Key evaluation metrics included transaction throughput, gas consumption, and scalability, allowing for a comprehensive assessment of each consensus model's effectiveness in a healthcare context. Ethereum, as a decentralized platform powered by a global network of Ethereum Virtual Machines (EVMs), facilitated the deployment and execution of smart contracts. Transactions within this network are executed using Ether (ETH), which serves as computational fuel or “gas.” The cost of executing a transaction is determined by the formula:

$$\textit{Transaction Cost} = \textit{Gas Limit} \times \textit{Gas Price} \tag{1}$$

where the Gas Limit defines the upper bound of computational effort allowed, and the Gas Price denotes the fee per unit of gas. This plays a critical role in optimizing performance and cost-efficiency in blockchain operations. By analyzing system behavior under both PoW and PoA models, the experiment provided valuable insights into the optimal configuration for secure, efficient, and scalable healthcare data management.

b. Consensus Mechanism Comparison

To assess the performance of the proposed blockchain-based healthcare system under varying operational conditions, two Ethereum test networks were utilized: the Rinkeby test network, which operates under a PoA consensus mechanism, and a local Ethereum test network employing PoW. This dual-network setup enabled a comparative analysis of throughput and scalability across differing consensus models.

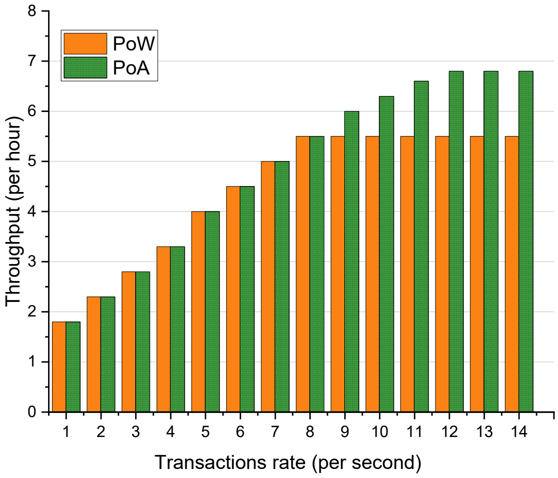


Figure 8. Comparison between PoW and PoA throughput for consensus

The results revealed a clear performance distinction. The PoW-based local network achieved a maximum throughput of approximately 55,000 transactions per hour, equivalent to around 8 transactions per second (TPS). In contrast, the PoA-based Rinkeby network demonstrated superior performance, processing nearly 68,000 transactions per hour or roughly 14 TPS. Consequently, the higher transaction rate of PoA reflects reduced latency by avoiding the computationally intensive mining puzzles of PoW. While the block confirmation occurs faster, this results in shorter waiting times for individual transactions. These findings underscore the efficiency and scalability advantages of PoA over PoW, particularly in contexts that demand high transaction throughput, such as healthcare information systems., Overall, the experimental data confirm that PoA is more suitable for enterprise-level healthcare applications, where rapid data processing, reduced latency, and reliable access control are essential. The improved throughput offered by PoA enhances the responsiveness and scalability of blockchain implementations in healthcare, without compromising security in a permissioned environment.

c. Smart Contract deployment cost

Figure 10 illustrates multiple deployment instances (different smart contracts), with PoW and PoA transaction costs plotted for each instance. For most deployments, both PoA and PoW show comparable gas costs, indicating that smart contract complexity (not consensus model) primarily influences the gas consumed. Also in most cases, PoA has yielded slightly lower gas costs compared to PoW. This is expected since PoA's block finality is faster and less resource-intensive, which can lead to reduced execution latency and miner overhead.

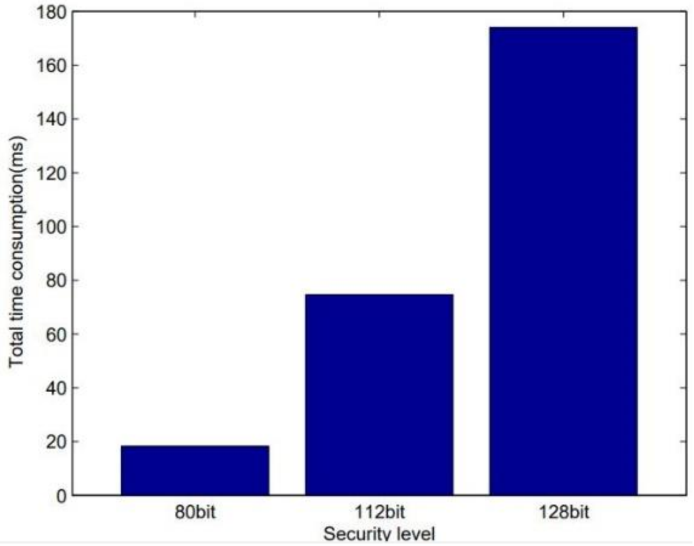


Figure 9. Computational cost of experiments of the proposed scheme with different security levels

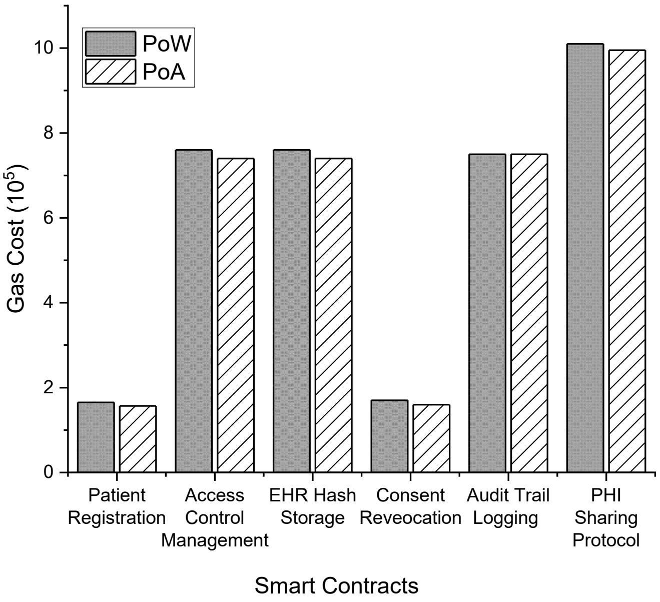


Figure 10. Smart contract deployment cost

Overall, smart contract deployment costs under PoA were significantly lower than PoW due to optimized execution and fewer computational overheads. This efficiency makes PoA more suitable for high-volume, enterprise-grade healthcare systems, where numerous smart contract operations occur daily. Whereas PoW, while secure, is costlier and slower due to energy-intensive mining and block finality delays.

d. Communication and Computational Overhead

Figure 11 compares communication cost with varying keyword set sizes. The proposed system demonstrates consistent communication efficiency across a range of keywords. Figure 9 shows computational overhead under different security levels, indicating that the system maintains a balance between performance and security.

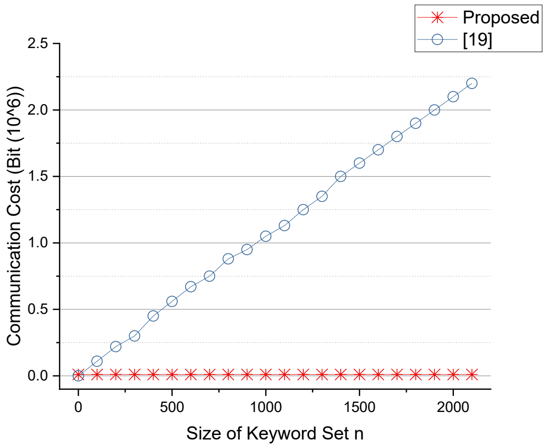


Figure 11. Communication cost comparison vs size of keyword set

e. Comparative Analysis

The proposed system was benchmarked against existing medical data sharing schemes ([28-30]). Table 2 compares six design factors as discussed in Table 1, highlighting the improved security, reduced complexity, and better scalability of the proposed scheme.

Table 2. Comparison of current solutions

Design Factors	[28]	[29]	[30]	Proposed Scheme
Decentralized	×	✓	✓	✓
Tamper-resistant	×	✓	✓	✓
Privacy protection	×	✓	✓	✓
Consensus	PoW	DPOS	dBFT	iDPOS
Pressure of main chain	Big	Small	Big	Small
Difficulty of implementation	×	×	×	✓

Legend: ✓= Supported, ×= Not Supported, **PoW** = Proof-of-Work, **DPOS**= Delegated Proof-of-Stake, **dBFT**= Delegated Byzantine Fault Tolerance, **iDPoS=** Improved Delegated Proof of Stake

f. Security Properties Comparison

The protocol ensures confidentiality and integrity through public-key encryption and digital signatures. PHI stored on the private blockchain is encrypted, and only authenticated users with valid permissions can access the data. The system supports time-controlled revocation, ensuring doctors cannot access future records without reauthorization. Additionally, the use of pseudonyms protects patient identities.

6. Conclusion

This research explored the integration of blockchain into e-health data sharing, highlighting its advantages in security, decentralization, and transparency. It analyzed the technical architecture and consensus mechanisms and proposed a hybrid system leveraging private and consortium blockchains. The proposed protocol incorporates public-key encryption, searchable encryption, and smart contracts to support secure data access, controlled revocation, and identity protection. Experimental results show PoA achieves higher throughput and lower costs than PoW. Comparative analysis validates the superiority of the proposed protocol across critical security and performance metrics. In summary, the proposed blockchain framework presents a robust, scalable solution for managing sensitive healthcare data in decentralized environments. For future work, we intend to optimize the proposed protocol through the integration of lightweight smart contracts, thereby reducing computational overhead while preserving functionality. In addition, we plan to design and implement a dynamic auditor election algorithm that can automatically select trusted validators based on predefined criteria, further strengthening system trust, transparency, and automation within the healthcare blockchain ecosystem.

References

1. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Satoshi Nakamoto, 2008.
2. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE international congress on big data (BigData congress), 2017, pp. 557-564.
3. J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," PloS one, vol. 11, p. e0163477, 2016.
4. G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1-32, 2014.
5. G. Zyskind and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in 2015 IEEE security and privacy workshops, 2015, pp. 180-184.
6. G. B. Prasad and M. V. Rao, "Cloud-Based Secure Blockchain Framework Utilizing Smart Contracts for Regulating Access to Confidential Electronic Medical Health Records," International Journal of Communication Networks and Information Security, vol. 16, pp. 117-128, 2024.
7. K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE access, vol. 4, pp. 2292-2303, 2016.
8. F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telematics and informatics, vol. 36, pp. 55-81, 2019.
9. C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: a systematic review," in Healthcare, 2019, p. 56.
10. K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," Journal of medical systems, vol. 42, pp. 1-7, 2018.
11. A. Roehrs, C. A. Da Costa, R. da Rosa Righi, and K. S. F. De Oliveira, "Personal health records: a systematic literature review," Journal of medical Internet research, vol. 19, p. e5876, 2017.
12. D. C. Nguyen, M. Ding, P. N. Pathirana, and A. Seneviratne, "Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: A survey," Ieee Access, vol. 9, pp. 95730-95753, 2021.
13. D. Zilong, M. M. Alobaedy, M. N. Hafiz, B. Ibrahim, and X. Huang, "A Blockchain Technology Framework to Enhance Security and Interoperability of Electronic Healthcare Records," 2024.
14. N. U. A. Tahir, U. Rashid, H. J. Hadi, N. Ahmad, Y. Cao, M. A. Alshara, et al., "Blockchain-Based Healthcare Records Management Framework: Enhancing Security, Privacy, and Interoperability," Technologies, vol. 12, p. 168, 2024.
15. P. Thantharate and A. Thantharate, "ZeroTrustBlock: Enhancing security, privacy, and interoperability of sensitive data through ZeroTrust permissioned blockchain," Big Data and Cognitive Computing, vol. 7, p. 165, 2023.
16. F. A. Reegu, H. Abas, Y. Gulzar, Q. Xin, A. A. Alwan, A. Jabbari, et al., "Blockchain-based framework for interoperable electronic health records for an improved healthcare system," Sustainability, vol. 15, p. 6337, 2023.
17. M. M. Rashid, S.-H. Lee, P. Choi, and K.-R. Kwon, "A blockchain-based approach in healthcare supply chain using smart contracts and decentralized storage systems," in Proceedings of the 2022 ACM Conference on Information Technology for Social Good, 2022, pp. 300-307.
18. A. Khan and A. Anjum, "Blockchain-based distributed platform for accountable medical data sharing," in Proceedings of the 14th IEEE/ACM International Conference on Utility and Cloud Computing Companion, 2021, pp. 1-8.
19. J. Durfee and M. J. Lee, "How Censorship Resistant Are Decentralized Systems?," Federal Reserve Bank of New York2025.
20. L. K. Oh and H. T. Sukmana, "A Comprehensive Study on Public and Private Blockchain Performance," Journal of Current Research in Blockchain, vol. 2, pp. 13-27, 2025.

21. S. R. Mallick, P. K. Sahu, U. Bagarti, and R. K. Lenka, "Blockchain: Tools, Challenges and Benefits," in 2024 IEEE International Conference on Communication, Computing and Signal Processing (IICCCS), 2024, pp. 1-6.
22. A. Sharma, R. K. Kaushal, and N. Kumar, "A Comprehensive Study on Blockchain and its Frameworks," in 2024 IEEE 11th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2024, pp. 1-6.
23. M. D. Hossain, Q. Mamun, and R. Islam, "A Comparative Study on Permissioned Based Blockchain Implementation on Healthcare Data: From Security and Privacy Perspective," in 2024 IEEE International Conference on Future Machine Learning and Data Science (FMLDS), 2024, pp. 222-227.
24. A. Pal, C. K. Tiwari, and A. Behl, "Blockchain technology in financial services: a comprehensive review of the literature," Journal of Global Operations and Strategic Sourcing, vol. 14, pp. 61-80, 2021.
25. S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," Peer-to-peer Networking and Applications, vol. 14, pp. 2901-2925, 2021.
26. O. Kuznetsov, A. Rusnak, A. Yezhov, K. Kuznetsova, D. Kanonik, and O. Domin, "Merkle trees in blockchain: A study of collision probability and security implications," Internet of Things, p. 101193, 2024.
27. N. Szabo, "Formalizing and securing relationships on public networks," First monday, 1997.
28. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in 2016 2nd international conference on open and big data (OBD), 2016, pp. 25-30.
29. A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," Journal of medical systems, vol. 42, p. 140, 2018.
30. T.-F. Xue, Q.-C. Fu, C. Wang, and X. Wang, "A medical data sharing model via blockchain," Acta Automatica Sinica, vol. 43, pp. 1555-1562, 2017.