

A Lightweight Blockchain-Assisted Framework for Privacy-Preserving Healthcare Using Hybrid AES–RSA Encryption

Shubhangi Dongre

shubhi.d95@gmail.com

Samrat Ashok Technological Institute

Sandeep Kumar Raghuwanshi

Kanak Saxena

Samrat Ashok Technological Institute

Research Article

Keywords: Blockchain Technology, Data Integrity Verification, Electronic Health Record Privacy, Healthcare Systems, Hybrid AES-RSA Encryption, Merkle Tree

Posted Date: October 20th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10783494/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Additional Declarations: No competing interests reported.

A Lightweight Blockchain-Assisted Framework for Privacy-Preserving Healthcare Using Hybrid AES–RSA Encryption

Shubhangi Dongre^{1 *}, Sandeep Kumar Raghuwanshi² and Kanak Saxena³

¹ Department of Computer Science and Engineering, Samrat Ashok Technological Institute
Vidisha, M.P.464001 India

[e-mail: shubhi.d95@gmail.com]

² Department of Innovation, Synechron Pvt. Ltd.

Bengaluru, Karnataka 560103 India

[e-mail: sraghuwanshi@gmail.com]

³ Department of Computer Science and Engineering, Samrat Ashok Technological Institute
Vidisha, M.P.464001 India

[e-mail: kanak.mcasati@gmail.com]

*Corresponding author: Shubhangi Dongre

[Received - to be completed by the Editorial Office; revised - ; accepted - ; published -]

Abstract

The rapid digitization of healthcare systems has introduced challenges related to data security, privacy, trust management, access control, auditability, and transparency. Conventional centralized healthcare architectures are vulnerable to single points of failure and exhibit limited scalability when handling large volumes of heterogeneous patient data. To address these limitations, this study proposes a blockchain-enabled privacy-preserving healthcare framework for secure and efficient medical data sharing among patients, healthcare providers, cloud servers, and research institutions. The framework integrates a hybrid AES-RSA encryption scheme, combining the efficiency of symmetric encryption with the secure key exchange of asymmetric cryptography to ensure confidentiality and controlled access. A Merkle tree-based structure is further incorporated within the blockchain to enhance data integrity and efficient verification, enabling tamper-evident record management and transparent auditing across distributed stakeholders. Experimental evaluation confirms that the proposed framework satisfies the core security objectives of confidentiality, integrity, and availability without imposing substantial computational overhead. Benchmarked against a proxy re-encryption scheme combined with zero-knowledge proofs, the proposed method reduced key-generation time from 16.30 s to 12.30 s and proof-generation time from 52 s to 43 s, while verification time decreased marginally from 0.614 s to 0.610 s. Proving key size and verification key size were also smaller, at 12.30 MB and 114.50 KB respectively, compared with 15.30 MB and 125.40 KB for the baseline scheme. These results indicate that the framework generates keys efficiently, constructs and verifies proofs within practical time bounds, and maintains compact key sizes, supporting its suitability for large-scale, distributed healthcare data management.

Keywords: Blockchain Technology, Data Integrity Verification, Electronic Health Record Privacy, Healthcare Systems, Hybrid AES-RSA Encryption, Merkle Tree.

1. Introduction

In modern healthcare ecosystems, digital medical records—namely Personal Health Records (PHRs), Electronic Health Records (EHRs), and Electronic Medical Records (EMRs)—play a pivotal role in enabling real-time telemedicine, clinical decision-making, and advanced diagnostic systems [1–3]. PHRs are typically maintained on personal devices and acquired through wearable or sensor-based health monitoring systems, whereas EMRs and EHRs are securely stored within healthcare institutions and hospital information systems [4–6]. These records provide comprehensive patient information, including medical history, diagnostic reports, and treatment outcomes, thereby significantly enhancing clinical accuracy and reducing the likelihood of misdiagnosis during treatment processes [7–9].

Blockchain is considered one of the most important innovations in recent years for the management of data in the healthcare sector. In a decentralized system, the information is not stored in a single point and therefore it is more secure. In the context of healthcare, the use of blockchain technology provides a secure way of sharing information through a distributed ledger system, which guarantees transparency, traceability and trust among the various actors of the system such as patients, healthcare professionals and research centers. In this context, healthcare systems based on blockchain technology can support numerous activities such as patient data management, supply chain management, law compliance and financial transactions. In addition, blockchain technology can ensure data confidentiality, reduce administrative workload, automate business processes, and increase regulatory compliance within healthcare institutions.

Although the above works have achieved many breakthroughs, the existing systems still have many shortcomings, such as mutual authentication, high granularity of access control, and scalability for dealing with a large amount of heterogeneous data of patients [19]. In addition, the communication cost and computational complexity are also increased [20]. Therefore, this paper proposes a Merkle tree-based blockchain-based health care system to improve the auditing efficiency, data integrity, and system simplicity.

The major contribution of this paper is to design and implement a Merkle tree-based verification mechanism in the healthcare management system to validate the integrity of the data in the database. In addition to validating the integrity of the data, it should also make it possible to quickly discover whether there has been any tampering to the data. This mechanism should be able to verify the source of specific data in the database by utilizing hierarchical hash validation.

We aim to design a new data integrity model that is highly scalable and compact, and that leverages the Merkle tree data structure to keep resource utilization such as bandwidth and storage usage low, which is especially relevant for use cases such as those in healthcare environments, where huge amounts of data are produced and accessed regularly.

In the proposed scheme, decryption and authentication are carried out in a decentralized manner, governed by the underlying consensus mechanism. System performance is assessed using several criteria, including blockchain capacity, block creation time, total execution time, and the sizes of the secret proof, verification key, and generated proof. The remainder of this paper is organized as follows. Section 2 reviews existing blockchain-based healthcare data management systems and identifies the associated research gaps. Section 3 presents the architecture of the proposed system, while Section 4 details its functional modules. Section 5 formalizes the Merkle tree-based integrity and auditing mechanism, together with the underlying algorithms. Section 6 reports the experimental results; Section 7 discusses their implications and the limitations of the study, and Section 8 concludes the paper.

2. Literature Review

In [26, 27], Tomaz et al. and Al-Aswad et al. proposed ZKP-based authentication methods to protect user privacy and to realize fine-grained authorization; however, this approach is also computation resource-intensive. In [28], Vidhya and Kalaivani integrated proxy re-encryption with lightweight cryptography and smart contracts. Although this design simplifies key management, it still faces the challenge of scalability.

To address the identified challenges, several studies have proposed the use of blockchain frameworks built on top of platforms such as Hyperledger Fabric. In this context, Kaur et al. [29]

showed the possibility of storing and querying EHRs securely using smart contracts, but at the cost of higher communication latency. Lakshmanan et al. [30] proposed a framework that uses polynomial interpolation-based cryptography and optimization algorithms for key derivation, but at the cost of higher computation latency. Other than those mentioned above, several studies have explored the use of steganography [31] to secure data and IoT-enabled blockchain systems [32–33] to secure data in various healthcare applications. In addition, several studies have proposed various IoMT security frameworks to achieve data confidentiality and traceability [34–35], but with the cost of potential interoperability issues, higher computation latency and key management challenges.

Table 1. Comprehensive Literature Survey

Ref.	Approach / Technique	Key Features	Advantages	Limitations
[21]	Blockchain-based healthcare framework	Secure data exchange, distributed storage	High trust, accuracy, low latency	Poor scalability
[22]	Blockchain + data aggregation + group authentication	Secure EHR access	Improved reliability and privacy	High block confirmation time
[23]	Permissioned Blockchain (PB-IMUA)	Identity management, authentication	Strong attack resistance, low latency	Smart contract dependency
[24]	Proxy Re-Encryption + ZKP	Privacy-preserving EHR sharing	High confidentiality and integrity	Complex key management
[25]	Blockchain + ML-based authentication	Intelligent data sharing	Reduced response time	High computational overhead
[26–27]	ZKP-based authentication	Privacy, fine-grained access control	Strong security guarantees	Computationally intensive
[28]	Proxy re-encryption + lightweight crypto	Secure and efficient encryption	Improved confidentiality	Key management complexity
[29]	Hyperledger Fabric-based system	Secure querying and storage	Efficient smart contract execution	High communication overhead
[30]	Cryptographic + optimization-based framework	Secure key generation, data sanitization	Improved security metrics	Computational complexity
[31–33]	IoT/Blockchain integrated systems	Secure IoMT data handling	Enhanced traceability, confidentiality	Interoperability issues, overhead
[34–35]	Blockchain-based IoMT security frameworks	Secure key exchange and alerts	Strong authentication, privacy	Key management challenges
[36]	Adaptive service compliance (ML + blockchain)	Improved accessibility and verification	Enhanced service compliance	Complexity in learning models
[37]	Hierarchical blockchain + ZKP + ring signature	Anonymous authentication, scalability	Strong privacy and security	High computational cost

Recently, research has been done on new encryption methods in order to improve the privacy and anonymity of blockchain networks. This includes adaptive service compliance [36] as well as hierarchical blockchain models which utilize ZKP and ring signatures in order to achieve greater anonymity and more efficient transaction processing. However, these methods are typically very heavy on resources such as computation, memory, and complex cryptography.

From the literature review we can see that, although blockchain-based health care systems have many advantages, such as security, transparency, and decentralization, there are still many problems to be solved, such as access control, mutual authentication, scalability, and high computational complexity, etc. In order to solve these problems, some literature applies simple encryption algorithms such as hash function, or complex encryption algorithms such as proxy re-encryption and ZKP, and in the process of using these encryption algorithms, there are also some problems, such as key management and system performance, etc.

The existing systems mentioned above have their own limitations and challenges. Therefore, in the proposed work, Merkle tree-based verification is incorporated into a blockchain-based health care system to tackle those challenges. The proposed modification of hash-based verification in the blockchain consensus process is the main contribution of the paper. The proposed system uses Merkle tree for verification of integrity of the data, and hence enables fast auditing, reduction in storage and bandwidth requirements, and hence proves to be a cost and bandwidth effective solution.

3. PROPOSED BLOCKCHAIN MANAGEMENT SYSTEM

The proposed framework presents a blockchain-enabled privacy-preserving healthcare management system, designed to ensure secure storage, controlled access, and efficient verification of Electronic Health Records (EHRs) across distributed healthcare entities. The architecture integrates hybrid cryptographic mechanisms (AES–RSA) with a Merkle tree-based verification model to achieve confidentiality, integrity, and auditability in a decentralized environment. The complete architecture and workflow of the proposed system are illustrated in Figure 1.

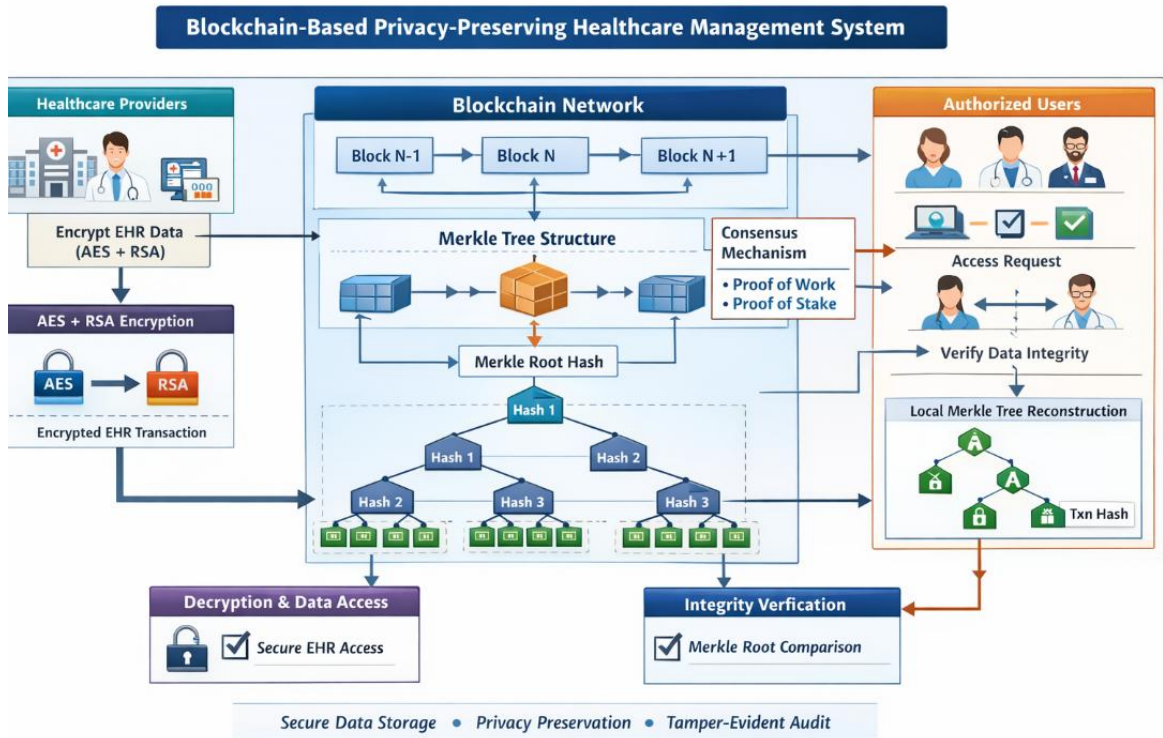


Fig. 1. Visual presentation of the proposed healthcare management system for privacy preservation

3.1 Data Generation and Transaction Formation

In the proposed system, healthcare providers (e.g., hospitals, diagnostic centers, and clinicians) generate EHRs corresponding to patient diagnoses, treatment history, laboratory reports, and clinical observations. Each EHR entry is treated as an individual transaction within the blockchain network. These transactions are digitally structured and appended to newly generated blocks, ensuring immutable and traceable storage of healthcare data.

3.2 Blockchain Structure and Hash Linking

Each block in the blockchain contains a set of validated EHR transactions along with essential metadata, including:

- Previous block hash
- Timestamp
- Transaction data (EHRs)
- Nonce (for consensus validation, if applicable)

The blocks are cryptographically linked using hash functions, where each block's hash is derived from its content and the hash of the preceding block. This chaining mechanism ensures tamper resistance and immutability, as any modification in a block propagates changes across subsequent blocks.

3.3 Merkle Tree-Based Integrity Verification

enhances verification efficiency, all transaction hashes within a block are organized into a Merkle tree structure. Pairwise hashing of transaction nodes is performed iteratively until a single Merkle Root Hash is obtained. This root hash is stored in the block header and acts as a compact representation of all transactions within that block. When an entity (e.g., patient, doctor, or research institution) requests access to a specific EHR:

1. The corresponding Merkle root hash is retrieved from the blockchain.
2. The requesting party reconstructs the Merkle path locally using the relevant transaction hash and intermediate hashes.
3. The locally computed root hash is compared with the blockchain-stored root hash to verify data integrity and authenticity.

This mechanism significantly reduces computational overhead and bandwidth requirements, as only partial hash paths are required instead of the complete dataset.

3.4 Hybrid AES–RSA Encryption for Data Security

To ensure data confidentiality and secure access control, the proposed system employs a hybrid cryptographic scheme. AES (Advanced Encryption Standard) is used for encrypting large EHR datasets due to its high computational efficiency. RSA (Rivest–Shamir–Adleman) is utilized for secure key exchange and encryption of symmetric keys. Authorized users possessing valid credentials can decrypt and access patient data, while unauthorized access is effectively prevented. This hybrid approach balances security strength and computational efficiency, making it suitable for large-scale healthcare systems.

4. SYSTEM ARCHITECTURE AND FUNCTIONAL MODULES

The proposed system will have functional phases such as authentication utility, secure data storage, record assignment, query and retrieval, integrity verification and record validation. The proposed privacy-preserving healthcare management system works in succession of these stages for management of EHRs in a secure manner.

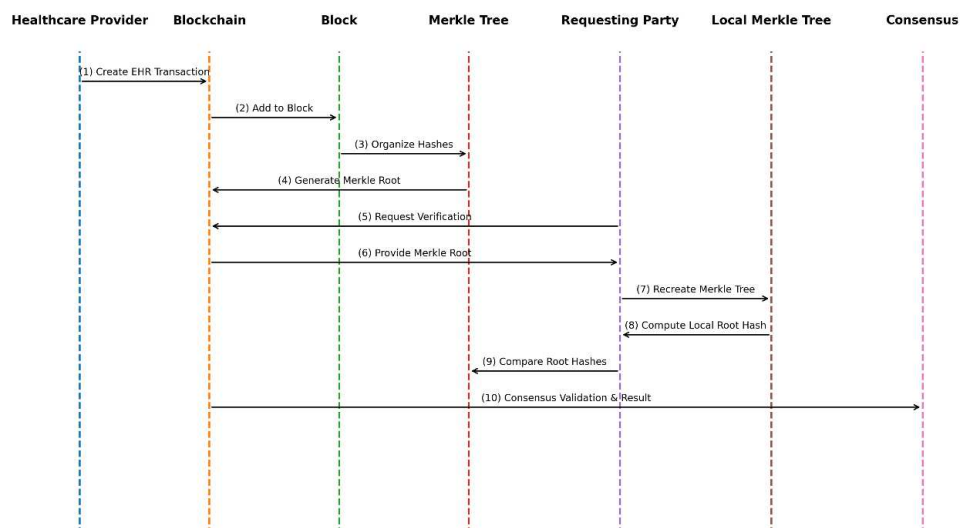


Fig. 2. Sequence diagram of EHR transaction creation, Merkle root generation, and verification between the blockchain and a requesting party

4.1 Authentication Utility - The system has an access control authentication mechanism for access management between the different entities involved such as audit authorities and patients. The system uses key data structures to manage the credentials of the users. New users' credentials are registered dynamically, while for existing users their verification has to take place before they access the system. Authentication is required at every primitive operation in the system in order to grant access to the health related information and the services of the system.

4.2 Secure Data Storage (Store Server) - The storage module is used to allow audit bodies and healthcare providers to transfer Electronic Health Records (EHRs) securely to the system. A hybrid encryption method is used for data confidentiality: • AES (Advanced Encryption Standard) is used to encrypt EHR data efficiently. • RSA (Rivest–Shamir–Adleman) is utilized for secure key generation and exchange. A unique pair of cryptographic keys are assigned to each patient record. The encrypted information is stored on the server or on the blockchain storage, providing total security and preventing any breaches.

4.3 Record Assignment and Merkle Tree Construction - Healthcare providers and regulatory agencies wish to audit EHRs efficiently and manage their integrity. We organize the EHR transactions with a Merkle tree. An authorized auditing entity forms the Merkle tree by hashing each record and putting the hashed records in a hierarchical structure and then computing the Merkle root hash of the tree. Then, a compact representation of the large set of records in EHRs can be achieved and tamper evidence is provided. Patients must authenticate themselves before accessing any assigned record in EHRs to achieve tight access control.

4.4 Querying and Retrieval of Records - The system supports the searching of the EHRs in a secure way using the proof-of-inclusion approach. After a EHR request of a patient or a third party, the corresponding Merkle proof that consists of the hashed values of the related transactions from the requested EHR to the root hash of blockchain is built. Hence, third party verifies the existence of the requested EHR in the database, not the whole database that increases the system performance and protects the privacy of the data.

4.5 Integrity and Authenticity Verification - Healthcare data integrity in blockchain systems must be validated to confirm that a patient's medical record has not been modified. For integrity verification, a comparison between the calculated Merkle root at the local hash tree using the proof path and the root hash stored in the blockchain is made. A mismatch indicates data tampering and validation ensures data integrity between the parties in the decentralized system.

4.6 Record Consistency Validation - As health care systems are dynamic and EHRs are updated frequently resulting in numerous versions of the Electronic Health Records (EHRs) of patients, it becomes essential to validate the consistency of the versions in order to ensure integrity of the data. In this paper, the proposed system will utilize a consistency validation technique that verifies the integrity of the EHRs by comparing an old version of the EHRs and a new version of the EHRs using hash-based verification. This will ensure that: • All records are maintained in the correct sequence • Newly appended data is accurately identified • Historical data remains immutable The system preserves a record of all changes and so demonstrates the integrity of data immutability, traceability and accountability.

5. Merkle Tree-Based Data Integrity and Auditing Mechanism

The audit authority constructs a Merkle hash tree from the patient audit trail stored at the audit storage point, enabling the Electronic Health Records (EHRs) to be verified quickly and at scale. This construction also improves auditing efficiency and reduces the complexity of data integrity verification. Finally, the Merkle tree maintained on the blockchain can differentiate between legitimate and illegitimate data for EHRs while keeping the underlying data private.

5.1 Merkle Tree Construction and Mathematical Formulation

In this implementation, the Leaf nodes of the tree contain hash values of individual patient data records. The intermediate nodes contain hash values of their child nodes and the Merkle root is a cryptographically compact hash of all the data in the tree. Let a node at level i and position j be denoted as $N_{i,j}$, with its corresponding hash value $H_{i,j}$. The leaf nodes (level $i = 0$) are computed as:

$$H_{0,j} = h(c_j) \quad (1)$$

where c_j denotes the patient data stored at leaf $N_{0,j}$, and $h(\cdot)$ represents a one-way cryptographic hash

function.

At higher levels, parent nodes are constructed by aggregating adjacent child nodes:

$$H_{i+1,k} = h(H_{i,j}, H_{i,j+1}, \dots, H_{i,j+t-1}) \quad (2)$$

The final Merkle root hash value, H_{root} , is used as a global hash value as a reference for each patient record's integrity. When there is a change in the underlying data, this root hash value changes and it then facilitates the tamper detection.

In the case of revocation or modification, affected leaf nodes are represented as a set:

$$\emptyset = \{c_0, c_1, \dots, c_j, \dots, c_n\} \quad (3)$$

which facilitates tracking of altered or revoked records.

5.2 Integrity Verification via Merkle Proof

Hash(m_i) is computed for each data block m_i in a specific data block segment at the leaf level of the Merkle tree. The Merkle proof contains auxiliary verification data Ω_i , which includes the hashes of the siblings nodes required to rebuild the root hash of each specific segment (i.e., x_i and y_i for the first hash):

$$\begin{aligned} H_D &\leftarrow H(h_1 \parallel h_2) \\ H_A &\leftarrow H(H_C \parallel H_D) \\ H_{root} &\leftarrow H(H_A \parallel H_B) \end{aligned}$$

This allows a fast verification of the integrity and authenticity of each data block in the segment, without reading the entire content of the segment.

5.3 Merkle Tree Operational Phases

The Merkle tree-based auditing mechanism operates in three distinct phases: (i) Set-Up Phase This phase initializes the system and prepares data for secure storage: Key Generation: This step uses a probabilistic algorithm to generate a key pair ($skey, pkey$) with the private key always kept secure and the public key published for verification purposes. Tag Generation: The metadata tags δ are generated for each data block using the input parameters ($skey_m, pkey_m$) to facilitate the verification process. Blockchain in Storage Block Signature Generation (BSG) uses a cryptographic hash function such as SHA-256 to cryptographically sign each data block before storage. (ii) Challenge-Prove Phase

This interactive phase ensures data possession and integrity: Gen-Challenge The client generates a challenge $chal$ using private parameters. Gen-Proof The server computes a proof G using public parameters, metadata, and stored data. Check-Proof: The client verifies the proof using ($pkey_m, chal_m, \delta_m, G$) and returns accept or reject. This phase guarantees that the server possesses authentic and untampered data. (iii) Update Phase To support dynamic data operations, the system incorporates update mechanisms: Perform-Update: When the server gets an update request, it updates the data and then generates the updated output ($m'^{\text{@@}}, \delta'^{\text{@@}}, G_{\text{update}}$). Verify-Update: The updated information is then verified via the public key and metadata to ensure that it has been changed correctly. This phase maintains data consistency, traceability, and immutability, even under frequent updates. The protocols of the Merkle tree is applied to implement the function of public data auditing and dynamic data maintenance. The algorithms of the blockchain class, the Merkle tree class and the proof of stake class are as follows:

Algorithm 1: Blockchain Class for Block Addition and Root Hash Computation

Input: New block b

Output: Updated blockchain and Merkle root hash H_{root}

Initialize:

1. Blocks $\leftarrow \emptyset$

2. $H_{root} \leftarrow \emptyset$

Procedure: Add_Block(b)

3. Append block b to Blocks

4. $H_{root} \leftarrow \text{Compute_Merkle_Root}(\text{Blocks})$
 5. Return H_{root}
- Function:** Compute_Merkle_Root(Blocks)
6. Extract hash values:
Hashes $\leftarrow \{b.hash \mid b \in \text{Blocks}\}$
 7. $H_{root} \leftarrow \text{MerkleTree.BuildTree}(\text{Hashes})$
 8. Return H_{root}

Algorithm 2: Merkle Tree Construction

Input: Set of data hashes $\{h_1, h_2, \dots, h_n\}$

Output: Merkle root hash H_{root}

Function: Hash(data)

1. Return SHA-256(data)

Function: BuildTree(Hashes)

2. CurrentLevel $\leftarrow$ Hashes
3. while | CurrentLevel | > 1 do
4. NextLevel $\leftarrow \emptyset$
5. for $i = 0$ to | CurrentLevel | - 1 step 2 do
6. $h_{left} \leftarrow \text{CurrentLevel}[i]$
7. $h_{right} \leftarrow \text{CurrentLevel}[i + 1]$
8. $h_{combined} \leftarrow h_{left} \parallel h_{right}$
9. Append Hash($h_{combined}$) to NextLevel
10. end for
11. CurrentLevel $\leftarrow$ NextLevel
12. end while
13. Return CurrentLevel[0] // Merkle Root

Algorithm 3: Proof-of-Stake-Based Transaction Validation

Input: Participant ID p , transaction T

Output: Validation status (Accept / Reject)

Initialize:

1. Participants $\leftarrow \{\}$

Procedure: Register_Participant(p)

2. Assign stake:
Participants[p] $\leftarrow \text{RandomInteger}(1, 100)$

Function: Validate_Transaction(p, T)

3. Stake $\leftarrow \text{Participants.get}(p, 0)$
4. MerkleKey $\leftarrow T.get("merkle_tree_key", \emptyset)$
5. if Stake > 50 and MerkleKey $\neq \emptyset$ then

6. Return Accept

7. Else

8. Return Reject

end if

It should be noted that the stake value in Algorithm 3 is assigned randomly for simulation purposes and does not represent an economic or reputation-based staking model; this simplification and its implications are discussed further in Section 7.2.

6. Result and Analysis

This privacy-preserving healthcare management framework is implemented in Python 3.11 and developed in PyCharm Community Edition. Experiments were performed on a High Performance Computing (HPC) server, with 256 GB RAM, Windows 10 operating system, 1 TB SSD storage, and NVIDIA GeForce RTX 2080 Ti Graphics Processing Unit (GPU) with 22 GB of Video Random Access Memory (VRAM).

To evaluate the performance of the proposed system, six metrics have been considered. These metrics are: blockchain memory size in MB, block generation time in seconds, total execution time in seconds, proving key size in MB, verification key size in KB, and proof size in KB. The system parameters used for the simulation are presented in Table 2. They specify details such as the blockchain configuration, the Merkle tree construction, as well as parameters that influence the length of the consensus phase.

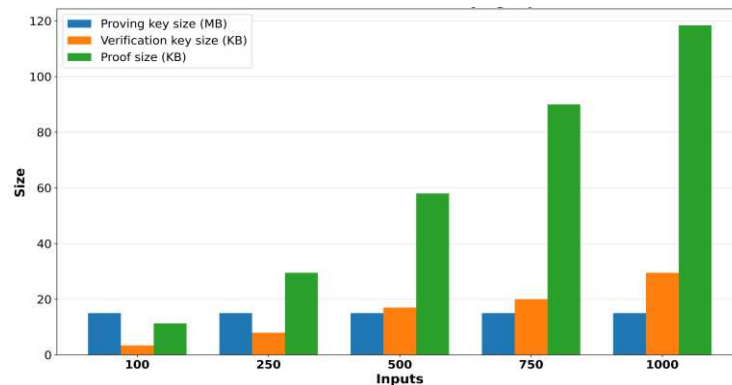


Fig. 3. Variation of cryptographic parameters (verification key size and proof size) with increasing input size in the proposed healthcare framework.

6.1 Quantitative analysis - The performance of our privacy-preserving healthcare management system is evaluated by varying input size. We report results obtained by varying the number of transactions from 100 to 1000, and present the corresponding results in Figure 3, detailing the size of the proving key, verification key and proof for each input size. Increase in the size of verification key and in the size of proof with respect to number of inputs. Even though both increase with the size of inputs, the values are within limits for being incorporated in Healthcare system.

Table 2. Parameters considered in this system

Parameter	Value
Maximum tree depth	$\log_2(\text{max transactions per block})$

Maximum transactions per block	100
Hash function	SHA-256
Maximum block size	100
Number of stakeholders	5
Transaction fee	1
Genesis timestamp	Time ()
Genesis previous hash	'0'
Genesis index	0
Block reward	10

From figure it can be observed that size of proving key does not increase even when size of inputs are increased. This means that proving time does not increase even when size of input increases. Size of verification key and size of proof both increases with increase in size of input. Size of verification key increases from 3.40 KB for 100 inputs to 29.50 KB for 1000 inputs and size of proof increases from 11.30 KB for 100 inputs to 118.40 KB for 1000 inputs. However even then the increase is within limit of normal Health care system and therefore can be easily incorporated in existing Healthcare framework. The robustness of the proposed architecture is then examined under varying patient counts presented in figure. For each patient count, key performance metrics that highlight system performance include blockchain memory size in kilobytes, block generation time in seconds and total execution time in seconds. The critical outcomes reveal that the system consistently demonstrates minor memory utilisation, accompanied by reduction in computational overhead as it processes an ever-increasing number of patient records, thereby conveying system efficiency.

Here, the overall verification mechanism becomes faster because every node needs to verify only a few parts of the Merkle tree. In this healthcare system, the Merkle tree parallelizes the verification of transactions with reduction in blockchain memory size, block generation time, and total execution time. The nodes present in the network need to quickly verify their validity while a new block is included with the blockchain. The Merkle tree performs effective verification, even without the need of the entire block. The pictorial illustration of the proposed healthcare management system by varying the patient size (1 to 15) is represented in Figure 4.

Correspondingly, figure states the results obtained from the proposed healthcare management system by varying the record size. During the transmission process, the Merkle tree ensures that the health data are not corrupted while transmitting the data between dissimilar parties. Furthermore, the use of cryptographic based hash functions improves the Merkle tree security and privacy. The use of a strong hash function makes the healthcare system more feasible and collision-resistant.

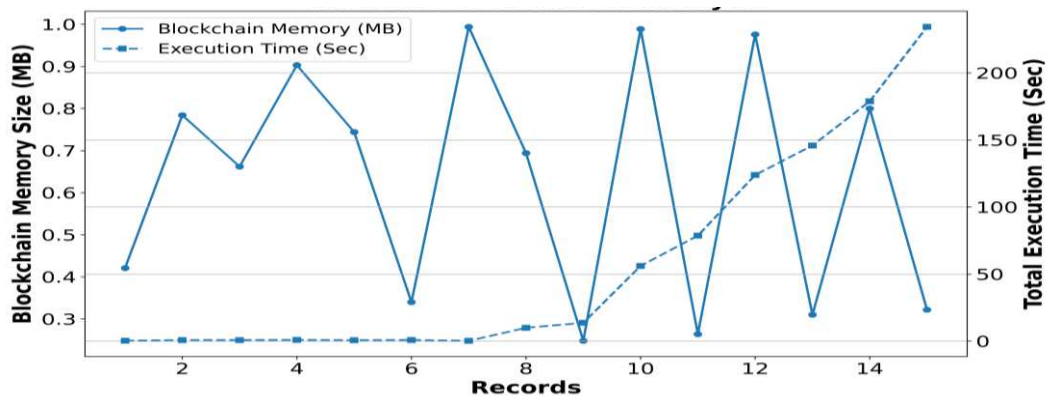


Fig. 4. Scalability analysis of the proposed system showing the relationship between record count, memory usage, and execution time.

The pictorial illustration of the proposed healthcare management system by varying the record size (1 to 15) is depicted in Figure 4.

By inspecting the figure, the proposed healthcare management system for privacy preservation is seen to consume a minimal blockchain memory size of 0.248MB, block generation time of 0.424

The graph in Figure 5 illustrates the required encryption time versus the decryption time compared to the patient records' size. We compare the processing performance of our approach to state-of-the-art encryption methods like the Advanced Encryption Standard (AES) [30], Rivest–Shamir–Adleman (RSA) [31], Attribute-Based Encryption (ABE) [32], and Elliptic Curve Cryptography (ECC) [33]. The graphical results illustrate that the proposed method consistently obtains the shortest encryption time across all of the record sizes. The increased time of the proposed method from 3.42 ms for 0.2 MB to 70.84 ms for 24 MB is within a reasonable level. The time of conventional ABE and RSA-based schemes are higher, especially as data size increases. The proposed method can thus obtain optimal performance. Its enhanced encryption efficiency, achieved through the enhanced AES encryption and the RSA-based key management, decrease pre-transmission latency and can efficiently support real-time healthcare information sharing requirements.

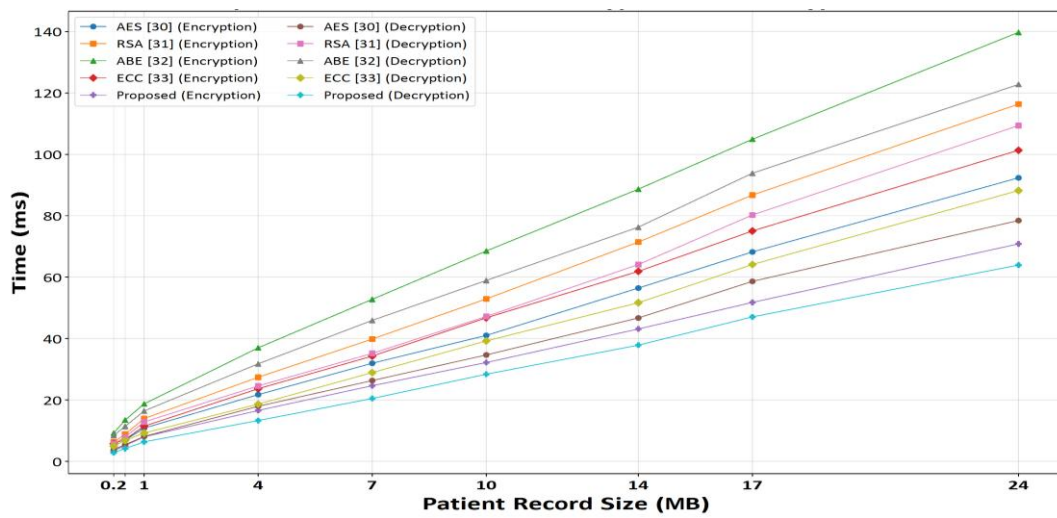


Fig. 5. Comparative analysis of encryption and decryption time with respect to patient record size for AES, RSA, ABE, ECC, and the proposed method

The same chart is shown in Figure 5 for decryption performance. The proposed method only slightly increases decryption time from 2.83 ms at 0.2 MB to 63.94 ms at 24 MB. It outperforms all of the competitors and the performance gap increases significantly as the size of data gets larger. Such an efficient decryption function is a critical requirement for various healthcare systems because faster data decryption directly affects the timing required for clinical decision-making.

Table 3 demonstrates the performance estimation of transaction time (ms) based on patient and doctor. The different number of transactions such as 10, 20, 50 and 100 are considered to estimate the transaction time between the doctor and patient. In 10th transaction, the patient and Doctor attain the transaction time 38.92ms and 47.28ms respectively. While in 100th transaction, the patient and doctor attain the transaction time of 193.78ms and 231.92ms respectively. The proportional increase demonstrates that the system maintains multi-user workloads without bottlenecks. This is important for hospital networks with simultaneous requests.

Table 3. Estimated transaction time (ms) between patient and doctor for varying numbers of transactions

Number of transactions	Patient	Doctor
10	38.92	47.28
20	76.84	93.56
50	193.78	231.92
100	382.63	468.23

Figure 6 demonstrates the quantitative analysis of the proposed method with existing methods. The proposed AES+RSA approach attains the better execution time of 59.68ms, encryption time of 32.19ms and decryption time of 28.38ms respectively. These results demonstrates that the proposed method attains significant results as compared to the existing methods like AES, RSA, ABE and ECC respectively. It helps to fast and secure data exchange among healthcare entities, improving an entire system responsiveness.

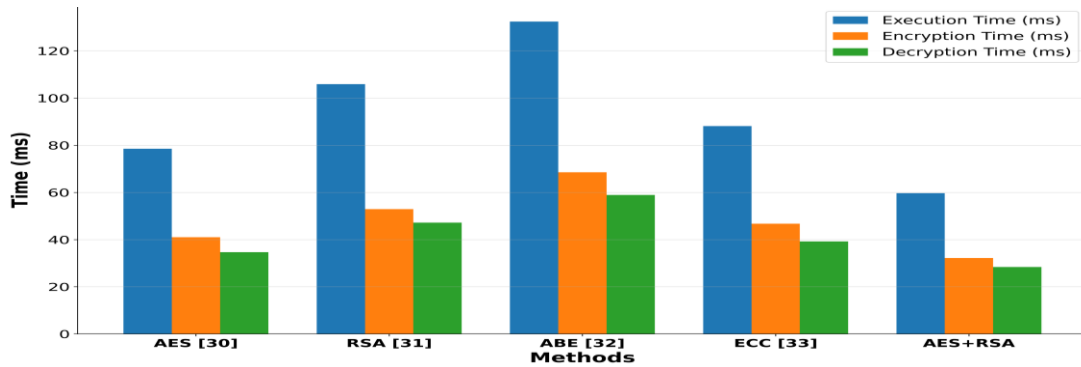


Fig. 6. Comparative performance analysis of execution time, encryption time, and decryption time for AES [30], RSA [31], ABE [32], ECC [33], and the proposed AES+RSA method.

Figure 7 illustrates the transaction cost (MB) as a function of the number of transactions. The results show that transaction cost increases only slightly as the number of transactions grows; at 100 transactions, the total cost remains well controlled compared with other blockchain-based systems. This scalability makes the system economically feasible for large hospitals, and the near-linear growth supports predictability in operational planning. The comparatively low slope reflects efficient smart contract execution, and the resulting cost efficiency supports the practical use of blockchain for health data exchange.

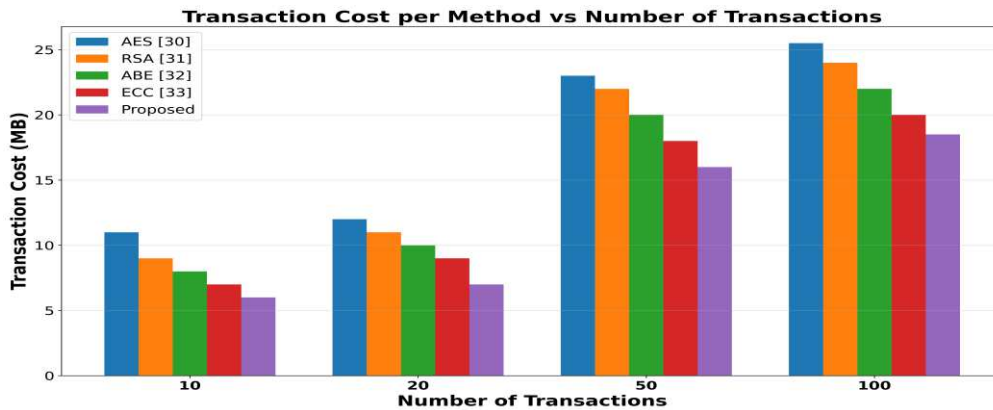


Fig. 7. Comparative analysis of transaction cost with respect to the number of transactions for AES [30], RSA [31], ABE [32], ECC [33], and the proposed method

Figure 8 shows the processing time (s) for each technique. The proposed approach has the shortest processing time, outperforming ABE and RSA by a wide margin. The hybrid AES-RSA design preserves both processing speed and cryptographic integrity; at a record size of 24 MB, its faster

processing supports scaling to high-throughput clinical environments. The proposed approach thus offers the best trade-off between speed and security among the methods compared.

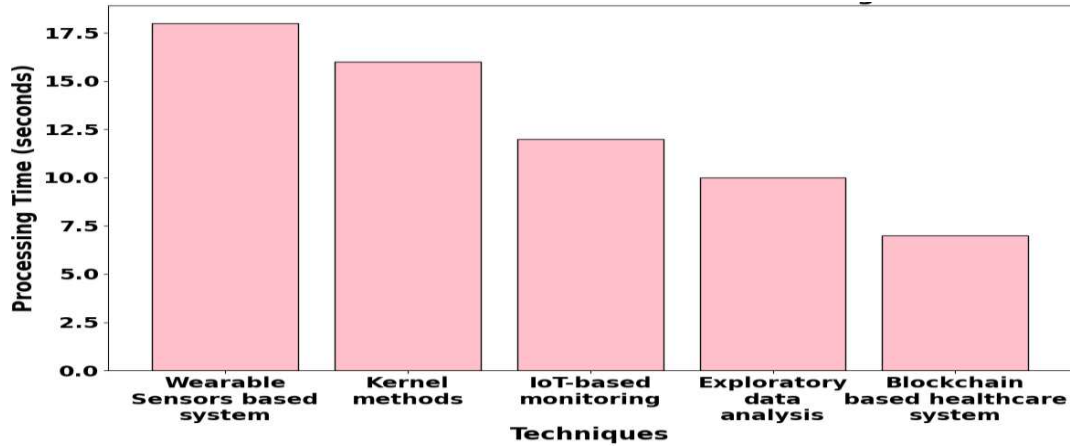


Fig. 8. Graphical representation of processing time (s) based on different techniques

Figure 9 shows transaction delay (%) as a function of the number of transactions, reflecting effective queue handling and transaction validation. The minimal delay observed supports continuous workflows in clinical settings, and transaction speed remains stable under load, indicating better dependability. Efficient delay management supports real-time diagnostic data routing, which in turn improves the timeliness of care delivery in networked hospital settings.

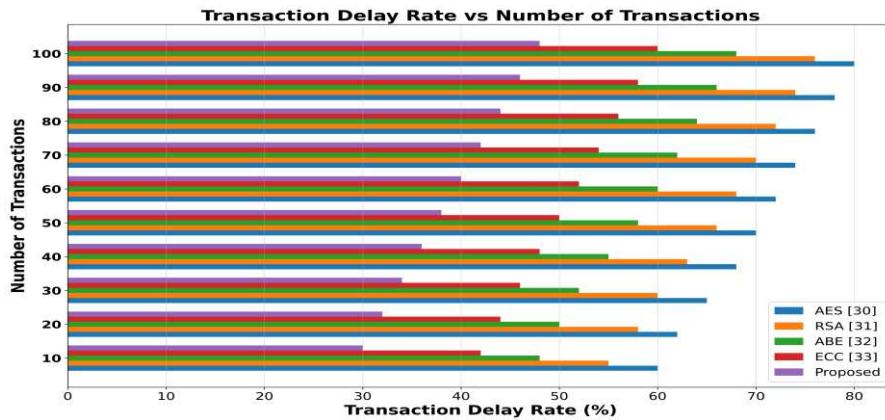


Fig. 9. Comparative analysis of transaction delay rate with respect to the number of transactions for AES [30], RSA [31], ABE [32], ECC [33], and the proposed method

Table 4 demonstrates the statistical analysis of the proposed method based on F-test. The proposed AES+RSA approach attains the better F-test of 0.037 as compared to other existing approaches. These results demonstrate hybrid approach attains significant performance as compared to the individual approaches.

Table 4. Statistical analysis of the proposed method based on F-test

Methods	F-test
AES	0.049
RSA	0.051
ABE	0.054
ECC	0.042
AES+RSA	0.037

Comparison of proposed healthcare management framework with state of the art approach is shown in Table 5. There is considerable research work going on to improve healthcare management. Huang et al. in [24] had proposed blockchain based healthcare system for secure sharing of Electronic Health Records (EHRs) amongst patients, research groups and cloud servers. In the proposed system, Zero-Knowledge Proof (ZKP) with proxy re-encryption is utilised to achieve data privacy, security and availability. Simulation results demonstrated desired security features.

Table 5. Comparative analysis between the proposed and existing healthcare management system

Parameters	Proxy re-encryption algorithm with ZKP [24]	Merkle tree based Proposed approach
Key-Gen	16.30 sec	12.30 sec
Prove	52 sec	43 sec
Verify	0.614 sec	0.610 sec
Proving key size	15.30 MB	12.30 MB
Verification key size	125.40 KB	114.50 KB

The Merkle tree-based approach achieves better performance in most indicators. The time spent in key generation is 12.30 s, proof generation is 43 s, verification is 0.610 s, the size of the proving key is 12.30 MB, and the size of the verification key is 114.50 KB. Compared with these results, the proxy re-encryption with ZKP approach has greater overhead in terms of computation and storage, at 16.30 s for key generation, 52 s for proof generation, 0.614 s for verification, 15.30 MB for the proving key, and 125.40 KB for the verification key.

The experimental results demonstrate that the proposed method substantially reduces both the computation time and memory usage while maintaining comparable verification accuracy. This is because the method relies on a lightweight hierarchical hashing structure, i.e., Merkle tree, which does not involve time-consuming ZKP-based cryptographic computations, compared to prior methods. Hence, the proposed method provides an efficient and scalable solution for privacy-preserving healthcare data management.

7. Discussion

Based on experimental results, it has been demonstrated that incorporation of the Merkle tree structure into the blockchain further increases auditing efficiency, reducing complexity of calculations. The environment for healthcare management systems includes a vast number of different types of pieces of information—sensitive, dispersed across multiple levels of the management system (such as treatment histories, diagnostic reports, and medical documents of in-patient beds), which requires effective and organized management.

We present in this paper a framework, based on Merkle trees, to efficiently verify integrity of large datasets. A Merkle tree transforms a set of data records into a hierarchy of hash values, where a single value, the root hash, serves as a compact summary of the entire set of records. By storing, in addition to the root hash, a subset of the internal hash values, one can efficiently verify entire datasets without having to transfer all the data.

In addition, when coupled with a distributed or decentralized ledger, the Merkle tree provides an enhancement to overall system security by enabling tamper-evident storage of data and verifiable audit trails. The hierarchical hashing provided by the Merkle tree facilitates fast and lightweight verification. Verification using the Merkle tree is highly scalable, meaning that performance is not adversely affected as the size of the dataset grows.

7.1 Security Considerations and Threat Model - The proposed framework assumes a semi-honest adversary model, in which participating nodes and cloud servers follow the protocol correctly but may attempt to infer sensitive information from stored or transmitted data. Under this assumption, the hybrid AES-RSA scheme preserves data confidentiality, since RSA-based key exchange prevents an eavesdropper from recovering the AES session key without access to the corresponding private key. The Merkle tree further provides tamper evidence; an unauthorized modification of a stored record changes its leaf hash and, consequently, the root hash maintained on the blockchain, so alteration can be detected without re-verifying the entire dataset. The current design, however, does not address a fully malicious adversary capable of colluding with multiple nodes or compromising the audit authority, and it has not been evaluated against replay attacks, denial-of-service attempts, or side-channel leakage during key generation. It should be noted that RSA-based key exchange is not resistant to a sufficiently powerful quantum adversary; migrating to a post-quantum key-encapsulation mechanism is left as future work, along with a formal treatment of key rotation and revocation following device compromise.

7.2 Limitations of the Study - Several limitations of this study should be acknowledged. First, the experiments were conducted on synthetic transaction data generated to resemble typical EHR workloads rather than on data drawn from an operational hospital information system, and results on real, heterogeneous clinical datasets, which often include unstructured content such as imaging reports and clinical notes, may differ from those reported here. Second, the proof-of-stake mechanism used for transaction validation (Algorithm 3) is a simplified simulation in which stake is assigned as a random integer rather than derived from an economic or reputation-based model; a production deployment would require a more rigorous consensus design together with an analysis of its resistance to stake-grinding and collusion. Third, performance was evaluated on a single high-performance workstation rather than across a geographically distributed network of nodes, so the reported block generation and transaction times do not capture network latency, node heterogeneity, or the effects of concurrent write contention that a multi-institutional deployment would introduce. Fourth, the comparative evaluation in Table 5 benchmarks the proposed method against a single prior scheme based on zero-knowledge proofs and proxy re-encryption, and a broader comparison against more recent Hyperledger Fabric-based and attribute-based encryption frameworks would strengthen the generalizability of the performance claims. Finally, the framework has not been assessed for compliance with specific regulatory frameworks such as HIPAA or the GDPR, and a formal mapping between the proposed access-control and audit mechanisms and these regulatory requirements remains to be established.

8. Conclusion

The rapid development of network and information technology has recently been accelerating the switch from paper-based patient records to electronic health records (EHRs) and the efficient sharing of such data among medical care systems through data transmission. However, even with such improvements in data transmission, the safety and privacy of patient information are being threatened by various types of attacks and information leaks. Thus, there is a strong need for development of appropriate, highly trusted safety and privacy protection technology. Blockchain has the potential to be implemented in a variety of settings within healthcare due to the inherent blockchain features like decentralization, immutability, transparency and tamper resistance. However, there are challenges associated to the implementation of blockchain-based healthcare systems such as scalability, interoperability, complexity and immaturity of existing blockchain infrastructure.

To handle the above challenges, a Merkle tree-integrated blockchain-based healthcare management framework is proposed. Based on the proposed framework, an improved auditing-efficient mechanism is designed and its efficiency is evaluated by several key performance indicators, such as blockchain memory size, block generation time, total execution time, proving key size, verification key size and proof size. The experimental results show that the proposed solution outperforms its Merkle-tree-free counterpart based on proxy re-encryption and zero-knowledge proofs (ZKP). The overhead of the proposed solution is lower across every measured indicator: the verification key size and the proving key size are 114.50 KB and 12.30 MB respectively, compared with 125.40 KB and 15.30 MB for the ZKP-based baseline. The time for verification is 0.610 s, the time for generating the proof is 43 s, and the time for generating a new key pair is 12.30 s, each of which improves on the corresponding baseline value. These results indicate that the proposed scheme is efficient enough to handle large volumes of health data while keeping key and proof sizes within practical limits. Future work can extend the

proposed architecture toward additional healthcare applications, including telemedicine, remote health monitoring, and virtual clinical consultations, and toward the security and consensus refinements identified in Section 7, so as to establish real-time, secure, and intelligent healthcare environments.

Data Availability Statement

The synthetic transaction data and simulation code used to evaluate the proposed framework are available from the corresponding author upon reasonable request. No real patient records were used in this study, and no ethical approval was required.

Funding Declaration

This work has not received any funding.

Ethics Approval and Ethical Considerations

This study does not involve human participants, human tissue, animal experimentation, or personally identifiable information. Therefore, ethical approval was not required for this research. All research activities were conducted in accordance with applicable ethical standards and principles of responsible research.

Consent to Participate

Not applicable. This study does not involve human participants.

Consent to Publish

Not applicable. This manuscript does not contain any individual person's data, images, or other personally identifiable information requiring consent for publication.

References

- [1] Shah, D., Rani, S., Shoukat, K., Kalsoom, H., Shoukat, M.U., Almujiabah, H. and Liao, S., 2024. Blockchain factors in the design of smart-media for e-healthcare management. *Sensors*, 24(21), p.6835.
- [2] Ali, A., Al-Rimy, B.A.S., Alsubaei, F.S., Almazroi, A.A. and Almazroi, A.A., 2023. Healthlock: Blockchain-based privacy preservation using homomorphic encryption in internet of things healthcare applications. *Sensors*, 23(15), p.6762.
- [3] Tiwari, S., Dhanda, N. and Dev, H., 2023. A real time secured medical management system based on blockchain and internet of things. *Measurement: Sensors*, 25, p.100630.
- [4] Andrew, J., Isravel, D.P., Sagayam, K.M., Bhushan, B., Sei, Y. and Eunice, J., 2023. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. *Journal of Network and Computer Applications*, 215, p.103633.
- [5] Xu, G., Qi, C., Dong, W., Gong, L., Liu, S., Chen, S., Liu, J. and Zheng, X., 2023. A privacy-preserving medical data sharing scheme based on blockchain. *IEEE Journal of Biomedical and Health Informatics*, 27(2), 698-709. doi: 10.1109/JBHI.2022.3203577
- [6] Sharma, V., Kumar, A. and Sharma, K., 2025. Digital twin: securing IoT networks using integrated ECC with blockchain for healthcare ecosystem. *Knowledge and Information Systems*, 67(3), pp.2395-2426.

- [7] Chandini, A.G. and Basarkod, P.I., 2023. Patient centric pre-transaction signature verification assisted smart contract based blockchain for electronic healthcare records. *Journal of Ambient Intelligence and Humanized Computing*, 14(4), 4221-4235. Article (CrossRef Link)
- [8] Zakzouk, A., El-Sayed, A. and Hemdan, E.E.D., 2023. A blockchain-based electronic medical records management framework in smart healthcare infrastructure. *Multimedia Tools and Applications*, 82(23), 35419-35437. Article (CrossRef Link)
- [9] Almalki, J., 2024. State-of-the-art research in blockchain of things for healthcare. *Arabian Journal for Science and Engineering*, 49(3), pp.3163-3191.
- [10] Haddad, A., Habaebi, M.H., Suliman, F.E.M., Elsheikh, E.A., Islam, M.R. and Zabidi, S.A., 2023. Generic patient-centered blockchain-based EHR management system. *Applied Sciences*, 13(3), p.1761.
- [11] Hegde, P. and Maddikunta, P.K.R., 2023. Amalgamation of Blockchain with resource-constrained IoT devices for Healthcare applications—State of Art, Challenges and Future Directions. *International Journal of Cognitive Computing in Engineering*, 4, pp.220-239.
- [12] Sun, Z., Han, D., Li, D., Weng, T.H., Li, K.C. and Mei, X., 2023. MedRSS: A blockchain-based scheme for secure storage and sharing of medical records. *Computers & Industrial Engineering*, 183, 109521. Article (CrossRef Link)
- [13] Kumar, M., Raj, H., Chaurasia, N. and Gill, S.S., 2023. Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. *Internet of Things and Cyber-Physical Systems*, 3, pp.309-322. Article (CrossRef Link)
- [14] Elkhodr, M., Gide, E., Darwish, O. and Al-Eidi, S., 2023. BioChainReward: A Secure and Incentivised Blockchain Framework for Biomedical Data Sharing. *International Journal of Environmental Research and Public Health*, 20, 6825. Article (CrossRef Link)
- [15] Babu, E.S., Yadav, B.V.R.N., Nikhath, A.K., Nayak, S.R. and Alnumay, W., 2023. MediBlocks: secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns. *Cluster Computing*, 26(4), 2217-2244. Article (CrossRef Link)
- [16] Yang, X., Li, W. and Fan, K., 2023. A revocable attribute-based encryption EHR sharing scheme with multiple authorities in blockchain. *Peer-to-peer Networking and Applications*, 16(1), 107-125. Article (CrossRef Link)
- [17] Abdelgalil, L. and Mejri, M., 2023. HealthBlock: A Framework for a Collaborative Sharing of Electronic Health Records Based on Blockchain. *Future Internet*, 15, 87. Article (CrossRef Link)
- [18] Sonkamble, R.G., Bongale, A.M., Phansalkar, S., Sharma, A. and Rajput, S., 2023. Secure Data Transmission of Electronic Health Records Using Blockchain Technology. *Electronics*, 12, 1015. Article (CrossRef Link)
- [19] Kaur, J., Rani, R. and Kalra, N., 2024. Attribute-based access control scheme for secure storage and sharing of EHRs using blockchain and IPFS. *Cluster Computing*, 27(1), 1047-1061. Article (CrossRef Link)
- [20] Chamola, V., Goyal, A., Sharma, P., Hassija, V., Binh, H.T.T. and Saxena, V., 2023. Artificial intelligence-assisted blockchain-based framework for smart and secure EMR management. *Neural Computing and Applications*, 35(31), 22959-22969. Article (CrossRef Link)
- [21] Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S. and Almansour, F.M., 2024. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Personal and Ubiquitous Computing*, 28(1), 59-72. Article (CrossRef Link)
- [22] Li, C.T., Shih, D.H., Wang, C.C., Chen, C.L. and Lee, C.C., 2020. A blockchain based data aggregation and group authentication scheme for electronic medical system. *IEEE Access*, 8, 173904-173917. doi: 10.1109/ACCESS.2020.3025898
- [23] Xiang, X., Wang, M. and Fan, W., 2020. A permissioned blockchain-based identity management and user authentication scheme for e-health systems. *IEEE access*, 8, 171771-171783. doi: 10.1109/ACCESS.2020.3022429
- [24] Huang, H., Zhu, P., Xiao, F., Sun, X. and Huang, Q., 2020. A blockchain-based scheme for privacy-preserving and secure sharing of medical data. *Computers & Security*, 99, 102010. Article (CrossRef Link)
- [25] Liu, H., Crespo, R.G., Martínez, O.S. Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts. *Healthcare* 2020, 8, 243. Article (CrossRef Link)

- [26] Tomaz, A.E.B., Do Nascimento, J.C., Hafid, A.S. and De Souza, J.N., 2020. Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. IEEE access, 8, 204441-204458. doi: 10.1109/ACCESS.2020.3036811
- [27] Al-Aswad, H., El-Medany, W.M., Balakrishna, C., Ababneh, N. and Curran, K., 2021. BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation. Arab Journal of Basic and Applied Sciences, 28(1), 154-171. Article (CrossRef Link)
- [28] Vidhya, S. and Kalaivani, V., 2023. A blockchain based secure and privacy aware medical data sharing using smart contract and encryption scheme. Peer-to-Peer Networking and Applications, 16(2), 900-913. Article (CrossRef Link)
- [29] Kaur, J., Rani, R. and Kalra, N., 2021. Blockchain-based framework for secured storage, sharing, and querying of electronic healthcare records. Concurrency and Computation: Practice and Experience, 33(20), e6369. Article (CrossRef Link)
- [30] Lakshmanan, M., Mala, G.S.A. and Anandkumar, K.M., 2024. Highly secured EHR management system based on blockchain technology with digitally signed authentication using data sanitization and polynomial interpolation. Biomedical Signal Processing and Control, 87B, 105412. Article (CrossRef Link)
- [31] Nath, S.S., Sadagopan, S., Babu, D.V., Kumar, R.D., Jonnala, P. and Murthy, M.Y.B., 2023. Block chain-based security and privacy framework for point of care health care IoT devices. Soft Computing, pp.1-13.
- [32] Sharma, P., Namasudra, S., Crespo, R.G., Parra-Fuente, J. and Trivedi, M.C., 2023. EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. Information Sciences, 629, pp.703-718.
- [33] Taloba, A.I., Elhadad, A., Rayan, A., Abd El-Aziz, R.M., Salem, M., Alzahrani, A.A., Alharithi, F.S. and Park, C., 2023. A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. Alexandria Engineering Journal, 65, pp.263-274.
- [34] Tomar, A., Gupta, N., Rani, D. and Tripathi, S., 2023. Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system. Internet of Things, 23, p.100849.
- [35] Lodha, L., Baghela, V.S., Bhuvana, J. and Bhatt, R., 2023. A blockchain-based secured system using the Internet of Medical Things (IOMT) network for e-healthcare monitoring. Measurement: sensors, 30, p.100904.
- [36] Arul, R., Alroobaea, R., Tariq, U., Almulihi, A.H., Alharithi, F.S. and Shoaib, U., 2024. IoT-enabled healthcare systems using block chain-dependent adaptable services. Personal and Ubiquitous Computing, 28(1), pp.43-57.
- [37] Nasr Esfahani, M., Shahgholi Ghahfarokhi, B. and Etemadi Borujeni, S., 2021. End-to-end privacy preserving scheme for IoT-based healthcare systems. Wireless Networks, 27(6), pp.4009-4037.
- [38] Lakshmanan, M., Mala, G.S.A. and Anandkumar, K.M., 2024. Highly secured EHR management system based on blockchain technology with digitally signed authentication using data sanitization and polynomial interpolation. Biomedical Signal Processing and Control, 87B, 105412. Article (CrossRef Link)
- [39] Islam, M.S., Ameendeen, M.A.B., Rahman, M.A., Ajra, H. and Ismail, Z.B., 2023. Healthcare-chain: blockchain-enabled decentralized trustworthy system in healthcare management industry 4.0 with cyber safeguard. Computers, 12(2), p.46.
- [40] Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M. and Abid, M., 2021. HealthBlock: A secure blockchain-based healthcare data management system. Computer Networks, 200, 108500. Article (CrossRef Link)
- [41] Nanda, S.K., Panda, S.K. and Dash, M., 2023. Medical supply chain integrated with blockchain and IoT to track the logistics of medical products. Multimedia Tools and Applications, 82(21), pp.32917-32939.
- [42] Taherdoost, H., 2023. Blockchain and healthcare: A critical analysis of progress and challenges in the last five years. Blockchains, 1(2), pp.73-89.
- [43] Idrissi, H. and Palmieri, P., 2024. Agent-based blockchain model for robust authentication and authorization in IoT-based healthcare systems. The Journal of Supercomputing, 80(5), pp.6622-6660.
- [44] Preetha, A.D. and Kumar, T.P., 2023. Securing IoT-based healthcare systems from counterfeit medicine penetration using Blockchain. Applied Nanoscience, 13(2), pp.1263-1275.

- [45] Lakshmanan, M. and Mala, G.S.A., 2024. Merkle tree-blockchain-assisted privacy preservation of electronic medical records on offering medical data protection through hybrid heuristic algorithm. *Knowledge and Information Systems*, 66(1), 481-509. Article (CrossRef Link)
- [46] Liu, Z., Ren, L., Feng, Y., Wang, S. and Wei, J., 2023. Data integrity audit scheme based on quad merkle tree and blockchain. *IEEE Access*, 11, 59263-59273. doi: 10.1109/ACCESS.2023.3240066

Author Profile



Shubhangi Dongre

Shubhangi Dongre received her M.Tech from the Maulana Azad National Institute of Technology (MANIT), Bhopal, and currently works as an Assistant Programmer in the State GST Department. Her research interests include blockchain technology, data security, and healthcare information systems.



Sandeep Kumar Raghuwanshi

Sandeep Kumar Raghuwanshi has over 20 years of experience in machine learning, artificial intelligence, and computer science, and has taught and mentored more than 10,000 students and industry professionals. He holds a PhD in Accelerated Singular Value Decomposition (ASVD) using momentum-based gradient descent optimization and currently works in the Department of Innovation at Synechron Pvt. Ltd. His research interests include data science leadership, applied machine learning, and the mathematical foundations of deep learning.



Kanak Saxena

Kanak Saxena has 34 years of experience in academia and research, working in data science, software architecture, and machine learning, with a particular focus on healthcare applications. She has authored more than 100 papers in journals and conferences and has supervised 17 PhD candidates. She serves on the editorial boards of several journals, regularly reviews research papers, and has contributed to the organization of international conferences as a panellist and session chair.