A Blockchain-based Secure and Privacy-Preserving Healthcare Data Management Framework with SHA-256 and PoW Consensus

Geng Niu
Shaanxi Provincial Intelligent New Criminal Technology, Practical Application Research Center, Shaanxi Police College, Xi'an 710021, China
E-mail: gengniu0319@163.com

Keywords: Blockchain, healthcare data management, privacy preservation, SHA-256, Proof-of-Work (PoW), RSA, ECDSA

Received: February 25, 2025

Healthcare systems handle a vast amount of sensitive patient data, making privacy and security crucial concerns. As digital health technologies expand, ensuring accurate and secure data storage becomes increasingly important. However, the frequent exchange of medical information poses risks of unauthorized access and data breaches, complicating secure data sharing. Moreover, many blockchain-based healthcare solutions face challenges related to performance inefficiencies and insufficient privacy safeguards. To overcome these limitations, we introduce a blockchain-powered system designed to enhance privacy protection, secure data sharing, and reliable storage in healthcare environments. Our methodology integrates an access control mechanism using SHA-256 for data integrity, RSA and ECDSA for transaction signatures, and a Proof-of-Work (PoW) consensus mechanism to ensure decentralized trust and scalability. The system employs cryptographic key management with RSA-generated public-private key pairs to secure data access and prevent unauthorized modifications. Experimental results demonstrate that the proposed system achieves an average transaction latency of 15.3 ms for 10 transactions on a single node, with a data integrity success rate of 100% across all tested scenarios. Comparative evaluations against state-of-the-art frameworks show our system reduces latency by 39% while maintaining robust security. Additionally, performance analysis highlights the system's ability to maintain low computational overhead, with transaction times ranging from 25.2 ms to 157.4 ms for 1 to 15 transactions across multiple nodes, ensuring efficient processing in real-world healthcare settings.

Povzetek: V prispevku je opisano varno in razširljivo verižnoblokovno ogrodje za upravljanje zdravstvenih podatkov, ki z uporabo SHA-256, PoW, RSA in ECDSA zagotavlja zasebnost, celovitost in nizko latenco.

1 Introduction

Blockchain technology has attracted substantial attention and investment across various sectors, including digital currencies, supply chain management, the sharing economy, energy trading, financial security, copyright protection, and e-governance [1, 10]. Known for its strong security features, blockchain plays a crucial role in supporting decentralized applications and facilitating secure digital transactions [8]. The integration of blockchain with healthcare systems offers decentralized data storage, tamper-proof records, and cryptographic security mechanisms, thereby mitigating risks of unauthorized access and data breaches. In this work, we propose a blockchain-based framework that enhances healthcare data security and privacy by integrating an access control mechanism based on SHA-256 hashing for data integrity, transaction signatures using RSA and Elliptic Curve Digital Signature Algorithm (ECDSA) for authentication, and a Proof-of-Work (PoW) consensus-driven security policy to ensure decentralized trust and scalability.

To ensure a seamless user experience, transactions within these applications must exhibit high speed, low latency, strong security, and reliability. The growing incorporation of emerging technologies in healthcare is accelerating the expansion of health information processing [1], making electronic health records a crucial and widely shareable asset. Globally, the volume of medical data is rising at an unprecedented pace.

The rapid increase in health data within medical institutions is contributing to more intricate information management systems, emphasizing the need for enhanced security and privacy measures [17]. Manual paper-based health records and legacy management systems are particularly susceptible to breaches in patient privacy and data integrity. Additionally, the lack of interconnected health centers poses challenges for the long-term storage, sharing, and maintenance of medical data, hindering effective treatment and consultations. Despite the advantages of blockchain technology, existing blockchain-based healthcare frameworks often face challenges in balancing security, scalability, and efficiency. For instance, ensuring

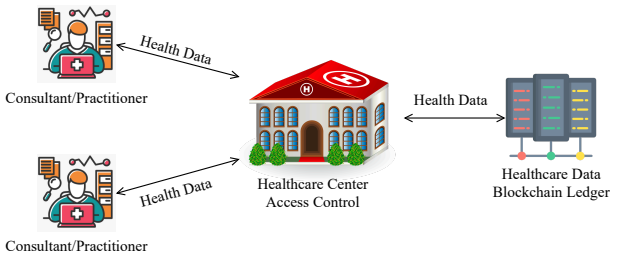

Figure 1: General overview of the functions of public healthcare center

real-time access to medical records while preserving privacy requires novel consensus mechanisms and encryption strategies [17]. Additionally, interoperability between different healthcare providers remains a concern, necessitating standardized protocols for secure data exchange [1]. Our proposed framework directly addresses these limitations by implementing a scalable blockchain architecture with low-latency transaction processing to overcome performance inefficiencies, a SHA-256 and RSA-based access control mechanism to enhance privacy safeguards, and a standardized key management protocol to ensure interoperability among healthcare providers. Furthermore, it mitigates computational and storage trade-offs by optimizing the Proof-of-Work consensus process, as detailed in section 3.

Recent studies have proposed various blockchain architectures to enhance healthcare data security. Some approaches leverage hybrid blockchain models that integrate fog computing to improve transaction speed and reduce computational overhead [8]. Others focus on homomorphic encryption techniques to enhance privacy preservation in healthcare data management [3]. However, these solutions often come with trade-offs in terms of computational complexity and storage requirements.

Blockchain technology presents offers superior security for healthcare data storage [6]. Its decentralized structure, combined with its capabilities for ensuring data integrity, security, privacy, and transparency, makes it an effective approach to healthcare data management, unlike traditional databases that rely on centralized servers vulnerable to single-point failures and unauthorized access. The adoption of blockchain-based data storage in the healthcare sector has led to the emergence of advanced digital platforms designed to replace traditional health record systems, significantly enhancing data privacy and integrity. Figure 1 illustrates the flow of health data within a blockchain-powered public health center, depicting secure transactions among authorized medical professionals, health center controllers, and the blockchain ledger. Authorized medical professionals and consultants can access these centers, retrieve patient records, and provide well-informed medical recommendations. This framework is designed to ensure the security, scalability, privacy, and integrity of health data storage and management through blockchain technology [12]. It leverages smart contracts, which function based on a consensus-driven mechanism.

This study aims to address the specific problem of inadequate privacy and efficiency in existing blockchain-based healthcare systems by developing a framework that ensures secure, scalable, and interoperable health data management. Our research objectives are: (1) to design a blockchain system with optimized access control and low-latency transactions, (2) to enhance privacy through advanced cryptographic techniques, and (3) to evaluate its performance against real-world requirements. Unlike prior solutions, this work defends against Sybil attacks through Proof-of-Work consensus, replay attacks via timestamped nonce verification, and insider threats with RSA-encrypted access control. A detailed threat model is presented in section 3.2. The key contributions of this work include:

- Development of a novel blockchain-based system for secure health data storage and sharing.
- Implementation of an optimized access control mechanism utilizing advanced cryptographic techniques, specifically SHA-256 for hashing, RSA for key generation, and ECDSA for digital signatures.
- Design of an evaluation framework to assess and demonstrate the system's performance, including a sequence diagram for the proposed model.

The remainder of this paper is structured as follows: section 2 discusses related work. section 3 describes the proposed system's design and architecture. section 4 presents the results of the experimental evaluation and section 5 discusses these findings. Finally, section 6 concludes the study.

2 Related work

Existing research on blockchain-based healthcare solutions has focused on various aspects such as access control, data confidentiality, secure storage, scalability, and information integrity. Conventional healthcare systems frequently struggle with maintaining secure data storage and facilitating safe information exchange across interconnected networks. However, state-of-the-art (SOTA) approaches often exhibit specific shortcomings in scalability, privacy, and security, necessitating a more robust solution as proposed in this work.

The decentralized nature of blockchain has the potential to transform healthcare by improving clinical data monitoring, ensuring secure patient data exchange, and strengthening data storage security [7]. Al-Zubaidie and Razzaq [17] proposed a privacy-preserving framework that integrates homomorphic encryption with blockchain to secure patient data transactions. Their approach enhances data integrity but suffers from increased computational overhead, limiting scalability due to high processing demands. In another study, Alshare et al. [1] explored the role of blockchain in

Table 1: Comparative analysis of blockchain-based healthcare solutions

Approach	Security Features	Performance Metrics	Shortcomings
Al-Zubaidie and Razzaq [17]	Homomorphic encryption, blockchain	High integrity, slow processing	High computational overhead, poor scalability
Alshare et al. [1]	Smart contracts, access control	Transparent, restricted access	Weak privacy against insider threats
Mishra, Yadav, and Nath [10]	Blockchain, IPFS	Low storage cost, high availability	High retrieval latency, limited scalability
Yang and Li [15]	Immutable logs, blockchain	Prevents unauthorized access	Vulnerable to Sybil attacks
Bowman et al. [4]	PDOs, Intel SGX	Secure smart contract execution	Centralized, poor scalability
Cheng et al. [5]	TEE, smart contracts	Secure transactions	High runtime overhead, broad attack surface
Khemaissia et al. [8]	Hybrid blockchain-fog	Reduced transaction time	Infrastructure complexity, limited scalability
Boumezbeur and Zarour [3]	Blockchain, encryption	Privacy-preserving sharing	Low computational efficiency

securing healthcare data by implementing smart contract-based access control mechanisms. Their findings indicate that blockchain can significantly improve data transparency while ensuring restricted access based on predefined security policies, yet it lacks sufficient privacy safeguards against insider threats due to weak key management.

Furthermore, Mishra and Yadav [10] investigated the integration of blockchain with InterPlanetary File System (IPFS) for decentralized healthcare data management. Their approach reduces storage costs and enhances data availability but introduces challenges in retrieval latency, compromising scalability for real-time applications. Yang et al. [15] developed a blockchain-based Electronic Health Record (EHR) framework aimed at preventing unauthorized access and data manipulation by maintaining an immutable activity log within the blockchain network, but its reliance on basic cryptographic methods leaves it vulnerable to advanced attacks like Sybil attacks. In Bowman et al. [4], Private Data Objects (PDOs) are proposed, allowing multiple untrusted entities to execute smart contracts on sensitive personal data using Intel SGX. PDOs rely on an interpreter enclave to securely process smart contracts within a controlled environment, yet this centralization reduces scalability and introduces a single point of failure.

Cheng et al. [5] introduced Ekiden, a system that integrates privacy-preserving smart contracts with a blockchain-enabled Trusted Execution Environment (TEE). Ekiden employs a Proof-of-Publication protocol to facilitate secure blockchain transactions, including consensus mechanisms reliant on authorized timers. However, this method may lead to increased runtime overhead, potential security risks, and a broader attack surface, but its high runtime overhead and broader attack surface undermine efficiency and security. Khemaissia et al. [8] introduced a hybrid blockchain-fog computing model to address performance bottlenecks in healthcare applications. Their solution reduces transaction processing time but requires additional infrastructure for fog computing deployment, increasing complexity and limiting scalability across diverse healthcare settings, with trade-offs including higher deployment costs and dependency on fog node reliability. Boumezbeur and Zarour [3] proposed a blockchain-enabled electronic health record (EHR) system with a focus on privacy-preserving data sharing. However, its heavy reliance on homomorphic encryption sacrifices computational efficiency, weakening its practicality for large-scale use, as it incurs significant computational overhead and latency.

To systematically compare these SOTA approaches, table 1 summarizes their key characteristics and shortcomings. This analysis highlights that existing solutions often fail to balance scalability, privacy, and security effectively. For instance, methods like [17] and [3] prioritize privacy at the expense of scalability and efficiency, while [10] and [8] improve performance but compromise on retrieval latency or infrastructure demands. Security vulnerabilities, such as susceptibility to Sybil attacks [15] or insider threats [1], further underscore the need for a comprehensive solution. Our proposed framework overcomes these limitations by integrating SHA-256 and RSA-based access control for enhanced privacy, a PoW consensus for scalable security against Sybil attacks, and an optimized architecture that minimizes latency without additional infrastructure.

3 Proposed methodology

This section presents a blockchain based framework aimed at enhancing the secure storage of sensitive records in public health centers. The proposed solution focuses on ensur-

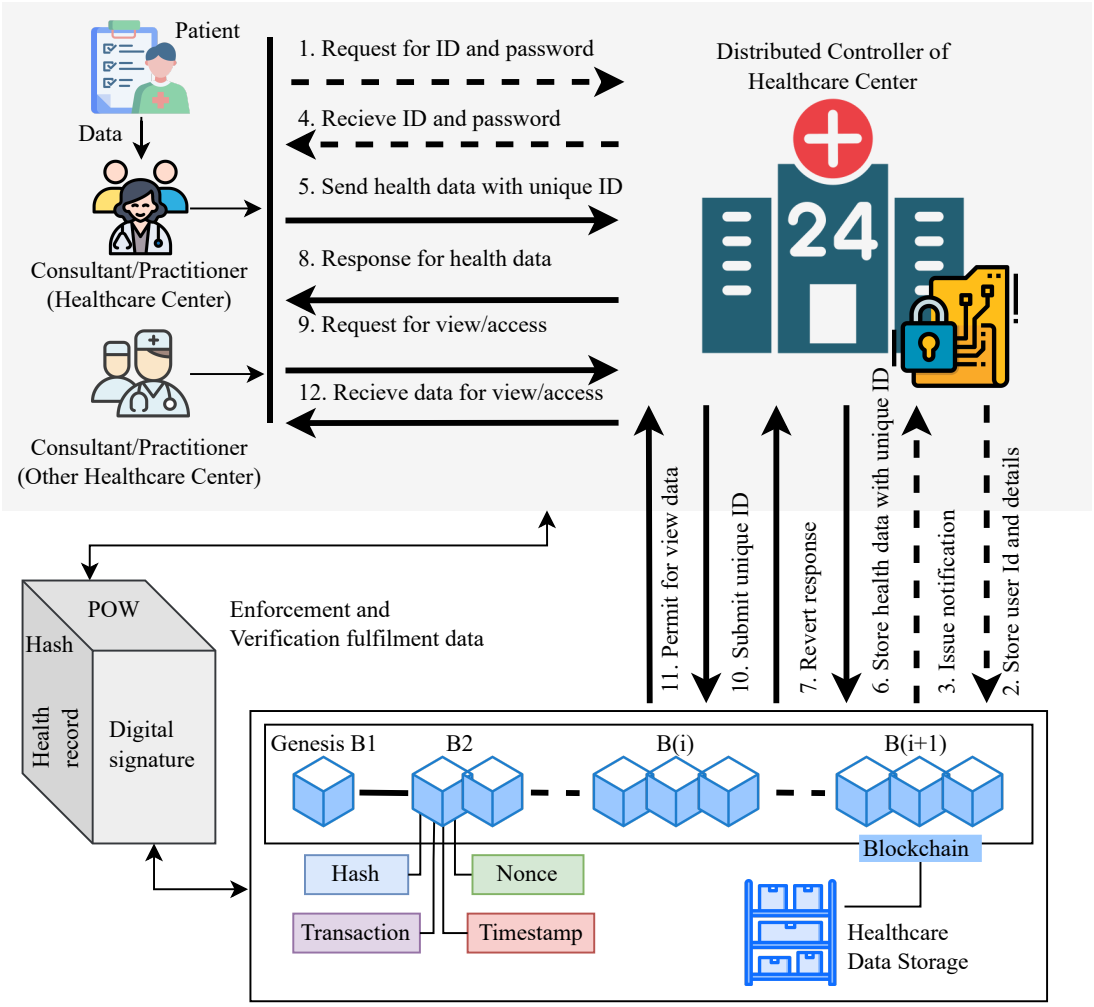

Figure 2: Framework diagram of the blockchain-based healthcare model, illustrating the sequence of interactions among users (consultants), the distributed controller, and the blockchain ledger. Step 7 ('Revert response') is conditional and occurs only if verification fails (e.g., after Step 10, if the unique ID or access request is invalid)

ing the confidentiality and integrity of healthcare processes while streamlining operations. It further describes the coordination of healthcare activities, sequence diagrams, and the workflow of block generation.

3.1 Healthcare center modeling using blockchain

The proposed framework is designed to improve healthcare system efficiency by reinforcing privacy, security, integrity, and verifiability of authorized health records. This section describes the system's overall architecture, as illustrated in fig. 2, which provides a comprehensive diagram of the blockchain-based healthcare data management framework for public health centers. The architecture integrates user interactions (e.g., consultants requesting ID/password and submitting health data, Steps 1, 5, 9), access control mechanisms managed by the distributed controller (Steps 1-4, 7-10), enforcement and verification processes (Step 11), and blockchain operations including secure data storage, PoW consensus, and block creation (Steps 2-3, 6). These components collectively ensure privacy, integrity, and secure access to health records. By implementing a blockchain based secure cloud storage model, this solution ensures high-performance authorization frameworks that uphold privacy and data integrity.

This blockchain based system enhances the reliability and scalability of health data, fostering greater confidence among stakeholders in data services. The core functional elements of the platform revolve around three key entities: the health data users/consultants, the health center controller, and the secure data repository. The health center controller governs the activities of data users/consultants within the blockchain based system. Each user/consultant acts as a data custodian, responsible for managing patient health records securely. Within this model, only authorized individuals can access, create, or update smart contracts related to health records on the blockchain. Consultants collect patient information and store it on the blockchain using public keys, while a unique private key is assigned to each

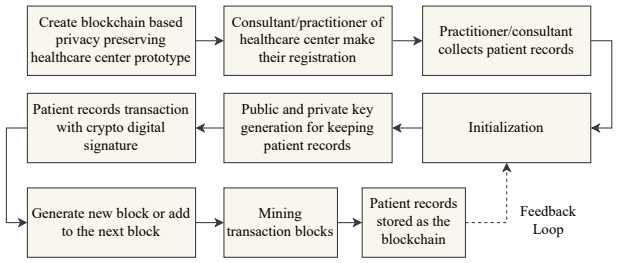

Figure 3: Workflow diagram for the proposed blockchain-based system for healthcare center, illustrating the detailed process of health data management. The ”Patient records transaction with crypto digital signature” step uses ECDSA and SHA-256 for secure signing, while ”Mining transaction blocks patient records” employs PoW consensus. A feedback loop from ”patient records stored as the blockchain” to ”Initialization” ensures error correction if verification fails.

patient's record for enhanced security.

Before gaining access, the health center controller verifies and registers each health data user/consultant, assigning a unique digital identity (ID) and password through a secure authentication framework. This registration process leverages the Bcrypt algorithm to generate encrypted digital IDs, which are then securely stored. After completing registration, authorized users can securely access the blockchain network with their digital credentials, ensuring robust authentication and strict access control.

In a system protected by blockchain, any action involving the database such as storing, modifying, or distributing data, interacts with the blockchain to maintain privacy, security, and accessibility. By utilizing a network of verified user nodes, the system guarantees the safety and accuracy of health records. Transactions are signed cryptographically and stored immutably on the blockchain, with data integrity ensured using SHA-256 hashing. The Proof-of-Work (PoW) consensus mechanism strengthens decentralization by requiring miners to expend computational effort to solve cryptographic puzzles, appending new blocks only after achieving a valid hash. This prevents unauthorized modifications in the healthcare context by making tampering economically infeasible as altering a patient record would require re-mining all subsequent blocks across the distributed network, a task computationally prohibitive due to the PoW difficulty. This ensures the immutability of medical histories critical for treatment accuracy, though it introduces energy consumption trade-offs, as analyzed in section 5. Any tampering is detected through sequential hash verification, including nonce values, timestamps, and encoded data. If an anomaly is identified, the affected block is flagged as invalid.

The operational process of data exchange in this model follows a structured approach:

1. Users/consultants authenticate themselves using their assigned IDs and passwords.
2. Upon verification, they request access to blockchain storage via the health center controller.
3. Encrypted health records are then submitted for storage and later retrieved as needed.
4. Each health record is assigned a Unique Data Identity (DID) for tracking purposes.
5. The controller manages the storage and retrieval of patient data using the assigned DID.

The DID is a composite identifier structured as a 256-bit hash, generated by concatenating the patient's unique identifier (a UUID assigned during registration), a timestamp of the record submission, and a hash of the health data itself using SHA-256. This structure ensures uniqueness and traceability: the UUID links the DID to the patient, the timestamp provides temporal context, and the health data hash ties the DID directly to the specific record. The DID is stored on the blockchain alongside the encrypted health record, enabling efficient retrieval and verification by authorized users while maintaining immutability and integrity.

The overall workflow of this blockchain-powered system is depicted in fig. 3, outlining each step involved in the development of a secure, transparent, and efficient health data management platform. Specifically, the step ”Patient records transaction with crypto digital signature” involves generating a digital signature using the ECDSA algorithm (as detailed in Algorithm 2) and hashing the transaction data with SHA-256 to ensure integrity and authenticity. The ”Mining transaction blocks patient records” step employs the Proof-of-Work (PoW) consensus mechanism, where miners solve cryptographic puzzles to validate transactions and append new blocks, as described in Algorithm 3. Additionally, a feedback loop exists: if a transaction fails verification (e.g., due to an invalid signature or hash mismatch), the system reverts to the ”Initialization” phase, prompting the practitioner to resubmit corrected data, ensuring robust error handling and data integrity.

Unlike hybrid blockchain-fog computing models [8], which rely on additional infrastructure and introduce deployment complexity, our framework avoids these trade-offs by leveraging a fully decentralized blockchain architecture with optimized PoW consensus, eliminating the need for external fog nodes while maintaining low latency. Similarly, in contrast to homomorphic encryption-based approaches [3], which incur high computational overhead, our system employs SHA-256 hashing and RSA encryption, achieving privacy and integrity with reduced processing demands.

3.2 Threat model

To ensure the robustness of the proposed blockchain-based healthcare framework, we define a threat model that identifies potential attacks and outlines corresponding mitigation strategies. This model focuses on three primary threats prevalent in healthcare data systems:

– **Sybil Attacks:** In a Sybil attack, an adversary creates multiple fake identities to gain disproportionate influence over the network. Our framework mitigates this through the PoW consensus mechanism, which requires computational effort to validate transactions and generate blocks. This makes it economically infeasible for an attacker to dominate the network with fake nodes.

– **Replay Attacks:** Replay attacks involve an adversary resubmitting valid transactions to disrupt the system or gain unauthorized access. The system defends against this by incorporating timestamped nonce values in each transaction, verified through sequential hash checks using SHA-256. Any attempt to reuse a transaction is detected and rejected, ensuring transaction uniqueness.

– **Insider Threats:** Insider threats occur when authorized users misuse their access privileges. To counter this, the framework employs RSA-encrypted access control, where each user's private key is required to sign transactions, and permissions are strictly enforced by the health center controller. Additionally, the ECDSA verifies signatures at both user and server levels, preventing unauthorized modifications, as outlined in Algorithm 2.

These mitigation strategies are integrated into the system's architecture and cryptographic operations, ensuring comprehensive protection against these threats.

3.3 Interoperability with healthcare standards

To ensure practical deployment in healthcare environments, the proposed framework is designed to comply with key standards, including Health Level Seven Fast Healthcare Interoperability Resources (HL7 FHIR), Digital Imaging and Communications in Medicine (DICOM), and Health Insurance Portability and Accountability Act (HIPAA) regulations. HL7 FHIR is supported by mapping blockchain-stored health records to FHIR resources (e.g., Patient, Observation) using standardized JSON encodings, enabling seamless data exchange with existing EHR systems. For medical imaging, DICOM compatibility is achieved by storing DICOM metadata hashes on-chain, with actual image files linked via secure off-chain storage (e.g., IPFS), balancing efficiency and integrity. Compliance with the HIPAA is ensured through RSA-encrypted access control and ECDSA signatures, safeguarding patient data confidentiality and auditability as mandated by HIPAA privacy rules. This interoperability enhances the framework's integration with diverse healthcare providers, addressing a critical limitation noted in section 2.

3.4 Smart contract security and audit methodology

The proposed framework incorporates smart contracts to manage access control and data transactions, necessitating safeguards against common vulnerabilities. To prevent reentrancy attacks, where a malicious contract repeatedly calls back into the system before state updates, we implement a non-reentrant modifier inspired by Ethereum's Solidity patterns, ensuring that state changes (e.g., access permission updates) are finalized before external calls. Integer overflows, a risk in arithmetic operations, are mitigated by using Python's arbitrary-precision integers in our Flask-based implementation, avoiding fixed-size integer limitations. For instance, nonce increments in PoW and transaction counters are immune to overflow due to this design choice.

To verify these protections, we outline a security audit methodology comprising: (1) static analysis using tools like Slither to detect reentrancy and overflow risks in smart contract logic, (2) dynamic testing with simulated attack scenarios (e.g., recursive calls) on a testnet, and (3) formal verification of critical functions (e.g., signature verification in Algorithm 2) using mathematical proofs of correctness. This multi-layered approach ensures robustness against vulnerabilities, complementing the cryptographic security detailed in section 3.2.

3.5 Coordination process

The proposed model ensures that a distributed controller in public health centers regulates access to blockchain-stored medical data. In this framework, three key participants are involved, medical practitioners/consultants (users who interact with health data), The distributed controller (responsible for registration and access management), and the blockchain ledger (which functions as a decentralized, secure database for patient health information). Blockchain serves as a highly distributed and tamper-resistant ledger, allowing only authorized entities to conduct transactions involving patient records. Participating nodes can input, retrieve, and verify data securely. The sequence diagram illustrating user activities within this model is shown in fig. 4, depicting the order of actions taken to interact with the system.

3.5.1 Registration

The framework initiates with a structured registration process designed to authenticate and onboard medical practitioners or consultants. To begin, practitioners submit a registration request to the health center controller, accompanied by relevant professional credentials. The controller then verifies the applicant's registration status; if unregistered, the applicant's details are encrypted and securely stored on the blockchain to ensure immutability and data integrity. Following successful verification, the system dynamically generates a unique user identity and password,

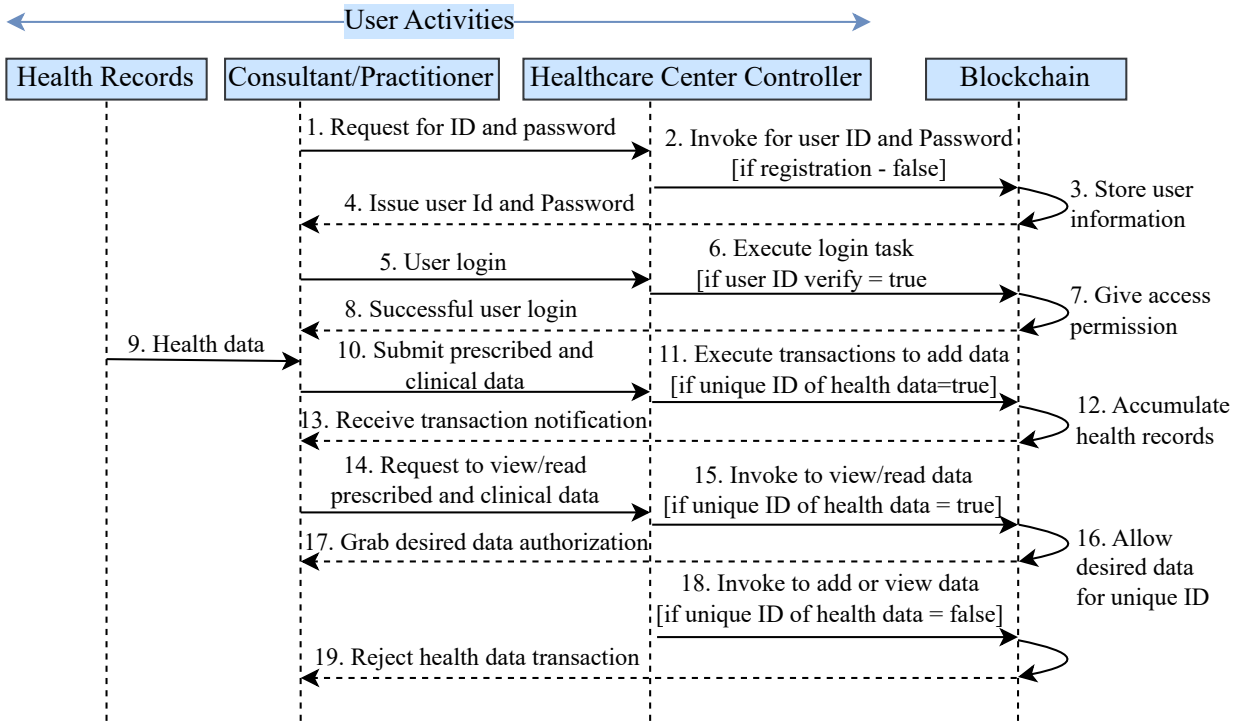

Figure 4: Diagram showing the sequence of user activities involved in blockchain based healthcare data center

which are disseminated to the practitioner via a decentralized, distributed controller. This authentication mechanism grants registered users perpetual access to the blockchain network, enabling them to log in at any time and participate in subsequent operations.

3.5.2 Data submission

Once authenticated, the framework transitions to the data submission phase. Consultants who are now part of the blockchain network, collect patient-specific clinical data such as diagnostic reports or prescribed treatments and submit these records to the health center controller. Upon receipt, the controller assigns a unique health identity to the patient, consolidating their medical history into a singular, traceable profile. To fortify security, each record is encoded with a hash based value by the blockchain, creating an indelible digital fingerprint that prevents tampering and enhances auditability. Access to upload or modify health records is rigorously restricted to authorized practitioners, with permissions governed by cryptographic keys to ensure compliance and prevent unauthorized alterations. Upon successful entry of data into the blockchain, all network participants, including relevant healthcare providers and the patients, receive instantaneous confirmation of the transaction. This real-time notification mechanism fosters transparency, accountability, and trust across the ecosystem, ensuring that stakeholders remain informed of updates to patient records while maintaining adherence to privacy and regulatory standards.

3.5.3 Data access and viewing

This section provides an in-depth explanation of the blockchain based framework for managing public health records, ensuring the confidentiality, security, and integrity of sensitive health data. The suggested system enables verified medical professionals and consultants to connect with the blockchain via the health center controller. This setup grants them access to previous health records while enforcing strict security measures to regulate access.

To retrieve patient health data, medical practitioners must first authenticate themselves using their unique digital identity and password, which is verified through the distributed controller. They must also provide the unique patient identifier corresponding to the specific individual's health record. Once the request is submitted, the health center controller verifies the identifier's validity and grants access to the requested clinical data if the credentials match the stored records. This process ensures that only authorized personnel can view and analyze previous prescriptions and medical history. If the verification process identifies an invalid patient identifier, the blockchain system automatically rejects the access request. The ability to securely retrieve prior medical records enables healthcare professionals to monitor patient health progress, formulate new prescriptions, and update the system accordingly.

The interactions among different entities within this system facilitate the seamless integration of blockchain technology into public healthcare data management. The sequence diagram in fig. 5 illustrates the blockchain trans-

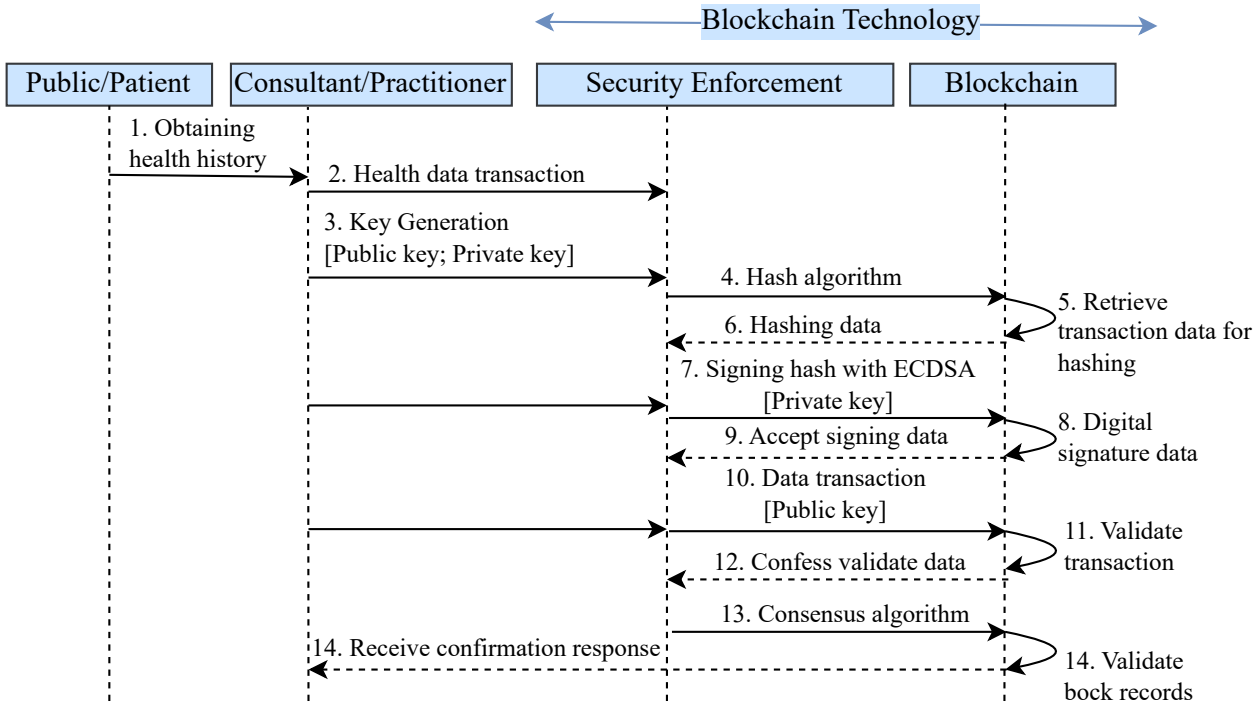

Figure 5: Diagram showing the sequence of processes in a blockchain transaction.

action process, which involves medical consultants, security mechanisms, and the underlying blockchain operations. When consultants collect health records from patients, they interact with the blockchain to execute transactions, ensuring that all health data is securely stored and processed. The system employs a key generation algorithm to create distinct public and private key pairs for secure data access. These keys, generated randomly, enhance the security of transactions within the platform by allowing encrypted communication between users and the blockchain ledger.

To reinforce data security, the blockchain framework incorporates cryptographic hashing and digital signing mechanisms. When a consultant shares a patient's health record with another authorized entity, no physical data transfer occurs. Rather than transferring data directly, the transaction is carried out by adjusting access permissions within the blockchain network. Every request to reallocate access must be authenticated by a digital signature, created using the sender's private key and validated against their public key to confirm legitimacy. The SHA-256 hash function is central to these operations, generating a unique cryptographic hash for each transaction and allowing data retrieval through hashed URLs within the web based platform. Additionally, participating nodes digitally sign transactions to confirm their authenticity, ensuring that data integrity remains uncompromised.

A crucial aspect of this blockchain based system is the PoW consensus mechanism, which governs block generation and verification. Nodes participating in the network validate health transactions, and miners are selected to generate the next block. This process ensures that all stored health data remains tamper-proof and synchronized across the distributed ledger. The RSA cryptographic algorithm and SHA-256 hashing play a fundamental role in securing the data, encrypting transactions, and maintaining the confidentiality of patient records. The blockchain storage mechanism ensures that all medical data remains accessible while being protected against unauthorized modifications.

Algorithm 1 Generate Transaction Key-pair

```
procedure transactionKeyGenerate
    if user U_h submits a health data transaction request to the health center controller then
        Procedure set(transactionKeyGenerate)
        randomValue ← generate_random(
                          cryptographic_value)
        privateKey ← generate_RSA(
                        1024, randomValue,
                        padding=OAEP, mode=encryption)
        publicKey ← privateKey · Kpb(i)
        decode_in_PEM_ascii(privateKey, publicKey)
        get privateKey, publicKey
    else
        do nothing
    end if
end procedure
```

The system's structural integrity relies on the SHA-256 cryptographic hash, which maintains the hierarchical organization of blockchain data blocks. Each new block added to the chain contains essential components such as the block number, timestamp, nonce, blockchain address, and hash of the previous block. The block header links all blocks to-

Algorithm 2 Digital Signature Generation for Data Transaction

```
procedure GenerateSignature(transaction)
    if user U_h requests transaction T over Blockchain then
        T ← make T exclude sender's privateKey
        privateKey ← GenerateRSAKey(
                        sender's privateKey)
        transactionSigner ← CreateDigitalSignature(
                                privateKey)
        hashValue ← ComputeHash(standard_input_value)
        signedTransaction ← SignTransaction(
                                transactionSigner,
                                hashValue)
        return EncodeASCII(signedTransaction)
    else
        don't create signature for T
    end if
end procedure
```

Algorithm 3 Creation and Addition of New Block for Hash based Health Data Transactions

```
procedure createNewBlock(healthData)
    Initialize healthTransactions ← ∅
    Set block ← (blockNumber, healthTransactions, nonce,
                 timestamp, previousBlockHash)
    if blockNumber = length(chain) + 1 then
        Append block to chain
        Reset running transaction status
        Add block to chain
    end if
    if EncodeJSON(block, standard_value) as a file then
        hash256Value ← CreateSHA256Hash()
        Update hash256Value.blocks
        return HexEncode(hash256Value)
    else
        Do nothing
    end if
end procedure
```

Algorithm 4 Append Node to Health Blockchain Network

```
procedure registrationRequest(node)
    if health data user requests a node then
        Create registrationNode
    end if
    Initialize parameters: (healthTransaction, chain,
                            nodes, genesisBlock)
    urlNodeInfo ← ParseURL(urlNode)
    if sets urlNodeInfo.Netloc and urlNodeInfo.path then
        Add urlNodeInfo.Netloc and urlNodeInfo.pathto
            nodes
    else
        Append a new node to nodes
    end if
    Do not append
end procedure
```

Algorithm 5 Secure Health Data Management on Blockchain

```
procedure AccumulateAndPublish
    Initialize transaction parameters for healthcare data
    Create a new transaction block
    Authenticate digital transaction signature
    publicKey ← GetRSAPublicKey()
    signatureVerifier ← CreatePKCS1Verifier(
                            publicKey)
    dataHash ← GenerateSHAHash(health_transaction)
    dataHash ← GenerateSHAHash(
                    health_transaction)
    VerifySignature(dataHash,
                    hexTransactionSignature)
    Execute PoW mechanism
    Fulfull mining conditions for valid proof
    Synchronize blockchain nodes
    Confirm blockchain transaction validity
    Append data to the transaction chain
    if transaction signature is verified then
        Transfer or share data between nodes
        Grant access to health records
    end if
end procedure
```

gether, ensuring seamless verification and establishing an immutable record of all transactions.

The Elliptic Curve Digital Signature Algorithm (ECDSA) further strengthens data security by verifying digital signatures at both the user and server levels. If any discrepancy is detected such as tampering or altered data values, the transaction is immediately discarded, preventing unauthorized modifications to stored health records. This two-tier verification approach ensures that only authenticated users can access and manage data, mitigating risks associated with data forgery.

Within the blockchain framework, each health transaction generates a public-private key pair to facilitate secure encryption and decryption. Algorithm 1 illustrates the RSA based key pair generation process, which assigns unique keys to all participants for secure interactions. The PEM method maps these cryptographic keys with ASCII encoding for seamless transaction decoding. Algorithm 2 details the process of generating digital signatures for health data transactions, ensuring encrypted authentication during network interactions.

To maintain data integrity, algorithm 3 outlines the steps involved in creating and adding new health data blocks to the blockchain. Each transaction block consists of essential attributes such as the block number, health data transaction, nonce, timestamp, and hash value. These components collectively ensure that public health records remain secure, transparent, and immutable. Algorithm 4 describes the procedure for integrating new nodes into the blockchain based public health center network, allowing for distributed and decentralized transaction processing. Algorithm 5 defines how public health data is accumulated, accessed, and managed within the blockchain.

The PoW consensus mechanism plays a vital role in the blockchain based public health network by validating transactions before they are shared or accessed across different nodes. This method dynamically adjusts the number of participating nodes, ensuring optimal network scalability and accelerating the health data transaction process. Once the transactions are validated, the system publishes the data blocks within the blockchain ledger, preserving the security and integrity of all recorded public health center transactions.

3.6 Complexity analysis of proposed algorithms

To evaluate the computational efficiency of the proposed framework, we analyze the time complexity of key algorithms, focusing on transaction signing (Algorithm 2) and block validation (Algorithm 3).

For Algorithm 2 (Digital Signature Generation), the primary operations are RSA key generation, SHA-256 hashing, and ECDSA signing. RSA key generation has a complexity of $O(k^3)$, where k is the key size (1024 bits in our implementation). SHA-256 hashing operates in $O(n)$, where n is the input data size, typically small for transaction metadata. ECDSA signing has a complexity of $O(k^2)$ due to elliptic curve operations. Since these steps are sequential, the overall complexity is dominated by RSA key generation, yielding $O(k^3)$.

For Algorithm 3 (Block Creation and Addition), the complexity hinges on SHA-256 hashing and the PoW mechanism. Hashing the block data is $O(n)$, where n is the block size. However, PoW requires solving a cryptographic puzzle by iterating nonce values until a valid hash is found, with an expected complexity of $O(2^d)$, where d is the difficulty level (configurable but typically fixed for consistent performance). Thus, block validation complexity is dominated by PoW, resulting in $O(2^d)$.

These complexities indicate that transaction signing is computationally intensive due to RSA, while block validation's efficiency depends on the PoW difficulty, a trade-off for security against Sybil attacks.

4 Results

This section provides an in-depth evaluation of the proposed blockchain based secure storage management system for public health centers, focusing on user nodes and assessing its ability to meet data security and privacy requirements. Experimental assessments and qualitative analyses were conducted to validate the system's effectiveness in ensuring confidentiality, integrity, and availability of health records. The results presented here focus on raw performance metrics, with comparisons and interpretations deferred to the subsequent Discussions section.

4.1 Evaluation environment

The experimental setup was conducted in a controlled environment using a Windows 11 system equipped with an Intel(R) Core i7-12700H processor (2.3GHz, 14 cores, x64 based architecture) and 16 GB RAM. The implementation leveraged Python 3.11 (64-bit) with Flask 2.2.5 as the web server gateway interface, ensuring seamless interactions between user nodes and the blockchain. The evaluation approach integrated multiple user nodes and a blockchain node to assess the performance and scalability of the health data management framework under real-world operational conditions. To enhance the robustness of the evaluation, additional tests were conducted on a cloud-based environment (AWS EC2 t2.medium instance with 2 vCPUs and 4 GB RAM) and a resource-constrained device (Raspberry Pi 4 with 1.5 GHz quad-core processor and 4 GB RAM) to simulate diverse deployment scenarios.

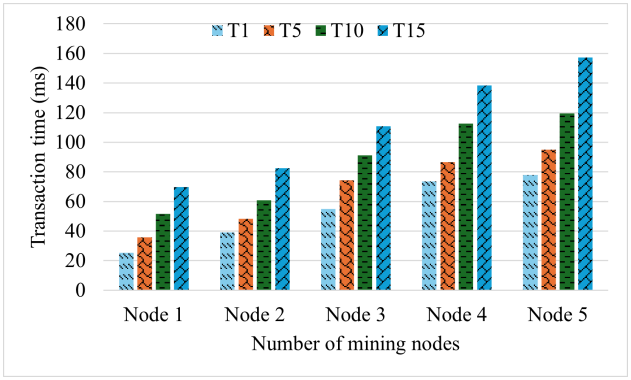

Figure 6: Average transaction time for different user nodes.

4.2 Performance evaluation

To measure performance, multiple user nodes were configured to interact with the blockchain server, enabling the evaluation of key parameters such as transaction time and latency. The system was evaluated by having user nodes conduct transactions in batches of 1, 5, 10, and 15 (T1, T5, T10, and T15) within the blockchain network. As each transaction block was mined and distributed across the blockchain-powered health center, the test provided valuable insights into the system's ability to manage growing transaction volumes efficiently.

4.3 Transaction time

Transaction time was recorded to assess how quickly the system processed data across different user nodes. The results, as illustrated in fig. 6, indicate that for node 1, transaction time ranged from 25.2ms for T1 to 69.8ms for T15. For node 5, transaction time started at 77.9ms for T1, reaching a peak of 157.4ms for T15, reflecting the system's performance under increasing transaction loads.

4.4 Latency

Another key performance metric analyzed was latency, which represents the delay experienced in transmitting and receiving data blocks within the blockchain network. As shown in fig. 7, latency for node 1 was 10.42ms for T1 and increased to 20.32ms for T15. For node 5, latency began at 25.18ms for T1 and reached a peak of 37.5ms for T15, demonstrating a consistent increase with higher transaction volumes.

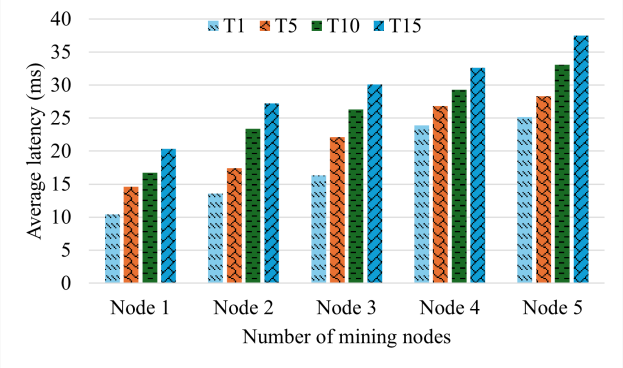

Figure 7: Average latency (ms) for different number of user nodes

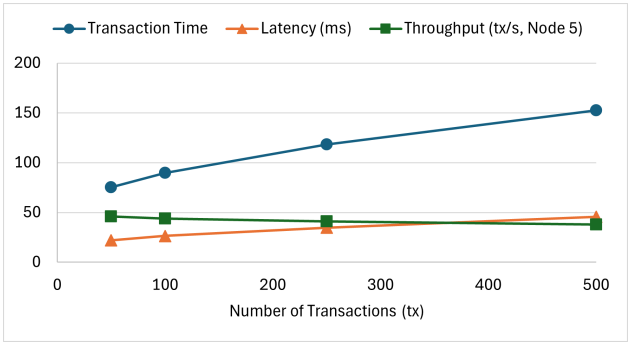

Figure 8: Performance Metrics with Increasing Blockchain Storage (Node 1 unless specified)

4.5 Functionality comparison

A detailed analysis was performed to evaluate the functional capabilities of the proposed system in comparison to other blockchain-based healthcare data storage solutions. Table 2 provides a comparative overview, highlighting the presence or absence of key security features, including availability (A), confidentiality (C), integrity (I), server-side verifiability (SSV), and user-side verifiability (USV), with a simple Yes or No indication. The findings reveal that many existing schemes lack essential security features necessary for comprehensive health data protection. In contrast, the proposed model ensures robust verifiability, data confidentiality, and system integrity, making it a more reliable and effective solution for secure healthcare data storage and management.

Table 2: Functionalities comparison

Ref.	A	C	I	SSV	USV
[16]	No	Yes	Yes	No	No
[14]	Yes	Yes	Yes	No	No
[9]	Yes	No	Yes	No	No
[11]	No	No	Yes	No	No
[2]	No	No	Yes	No	No
[13]	No	Yes	Yes	No	No
Our work	Yes	Yes	Yes	Yes	Yes

4.6 Impact of blockchain storage growth

To evaluate the system's performance as blockchain storage grows, we simulated an increasing number of healthcare transactions in batches of 50, 100, 250, and 500. Transaction time, latency, and throughput were measured for these batches. Results, summarized in fig. 8, indicate that for node 1, transaction time increased from 75.3ms for 50 transactions to 152.6ms for 500 transactions, and latency rose from 22.1ms to 45.8ms. For node 5, throughput, defined as transactions per second, ranged from 46 tx/s for 50 transactions to 38 tx/s for 500 transactions, reflecting performance under growing storage loads.

4.7 Storage overhead analysis

To assess the system's scalability for long-term medical record storage, we analyzed the storage overhead as blockchain data accumulates. Each transaction block, containing a header (block number, timestamp, nonce, previous hash) and health data (e.g., patient ID, hashed record), averages 1 KB, based on SHA-256 hash outputs (32 bytes) and metadata. For 500 transactions (fig. 8), the blockchain size is approximately 0.5 MB per node. Extrapolating to a healthcare center processing 10,000 transactions annually, the storage grows to 10 MB per year per node. Over a decade, this reaches 100 MB, manageable for modern hardware but potentially burdensome in a multi-node network with hundreds of centers.

To handle long-term storage efficiently, we propose an off-chain approach using the IPFS. Full medical records (e.g., text, images) are stored on IPFS, with only their cryptographic hashes and access metadata recorded on-chain. This reduces on-chain growth to ĩ00 bytes per transaction (hash + metadata), shrinking annual storage to 1 MB and decadal storage to 10 MB per node, a 90% reduction. IPFS ensures data availability and integrity via content-addressing, while blockchain enforces access control, balancing scalability and security for lifelong patient records.

4.8 Ablation study on cryptographic elements

An ablation study was conducted to assess the individual contributions of cryptographic components (SHA-256 hashing, RSA encryption, and ECDSA signatures) to performance. We evaluated four configurations for T10 on node 1: (1) full system (SHA-256 + RSA + ECDSA), (2) without ECDSA, (3) without RSA, and (4) without SHA-256. Results, detailed in table 3, show that the full system recorded a transaction time of 48.5ms and latency of 15.3ms. Removing ECDSA reduced transaction time to 42.1ms and latency to 13.8ms, excluding RSA lowered

Table 3: Ablation study results for T10 on node 1

Configuration	Transaction Time (ms)	Latency (ms)	Security Impact
Full System (SHA-256 + RSA + ECDSA)	48.5	15.3	None
Without ECDSA	42.1	13.8	Vulnerable to signature forgery
Without RSA	39.8	12.9	Weakened access control
Without SHA-256	36.4	11.5	Reduced data integrity

them to 39.8ms and 12.9ms, and omitting SHA-256 resulted in 36.4ms and 11.5ms, reflecting the performance impact of each component.

5 Discussions

This section compares the results of the proposed system with state-of-the-art (SOTA) solutions, providing numerical performance comparisons, analyzing trade-offs, and addressing the implications of design choices such as the use of PoW and SHA-256.

5.1 Comparison with state-of-the-art solutions

The proposed system's performance was benchmarked against a centralized SQL-based system and a SOTA blockchain-based framework [17], as shown in fig. 9. For T10 on Node 1, our system achieved a latency of 15.3 ms, compared to 8.1 ms for the SQL baseline and 25.2 ms for [17]. On Node 8, latency increased to 37.6 ms, higher than the SQL baseline's 12.4 ms but less than [17]'s 52.6 ms. Compared to other SOTA approaches in table 1, such as [10] (high retrieval latency) and [8] (reduced transaction time but complex infrastructure), our system offers a balanced performance, avoiding excessive computational overhead or external dependencies.

5.2 Performance trade-offs

The proposed system exhibits higher latency and transaction times than the SQL baseline due to the decentralized nature of blockchain and the computational overhead of PoW and cryptographic operations. However, this trade-off enhances security: the SQL system lacks tamper-proofing and decentralized trust, making it vulnerable to single-point failures and unauthorized access. Compared to [17], our lower latency (15.3 ms vs. 25.2 ms on Node 1) stem from an optimized PoW implementation and efficient SHA-256

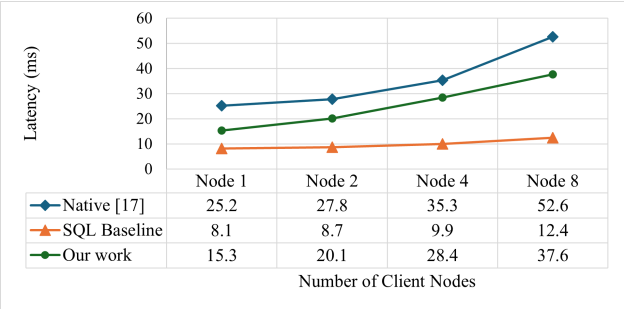

Figure 9: Comparison of latency vs number of client nodes for publishing a transaction

hashing, despite similar security goals. The ablation study (table 3) confirms that removing cryptographic elements reduces latency (e.g., 11.5 ms without SHA-256) but compromises security, justifying the performance cost for robust protection in healthcare settings.

5.3 Energy consumption analysis of PoW

The use of PoW introduces significant computational cost and energy consumption, as miners must solve complex cryptographic puzzles to validate transactions and generate blocks. For 500 transactions (fig. 8), transaction time reached 152.6 ms, reflecting this overhead. In large-scale healthcare deployments, this could lead to high energy usage, raising environmental concerns and operational costs. While PoW ensures strong resistance to Sybil attacks, its scalability is limited compared to Proof-of-Stake (PoS), as throughput stabilized at 38 tx/s for 5 nodes. In contrast, PoS eliminates mining by selecting validators based on staked assets, reducing energy consumption to near-negligible levels. PoS offers comparable security in permissioned settings but may compromise decentralization in trustless healthcare environments, where untrusted nodes require robust Sybil resistance, as PoS could favor wealthier nodes, potentially skewing fairness among healthcare providers. While PoW's energy inefficiency is a limitation, its decentralized trust aligns with the framework's goals. Future work could explore hybrid consensus (e.g., PoW-PoS) to balance security and sustainability, tailoring the system for energy-constrained healthcare settings.

5.4 Choice of SHA-256 and PoW

SHA-256 was selected for its proven collision resistance and widespread adoption in blockchain systems like Bitcoin, ensuring data integrity with a fixed 256-bit output that is computationally efficient for healthcare data hashing. PoW was chosen over Proof-of-Stake (PoS) or Byzantine Fault Tolerance (BFT) due to its robustness in trustless environments, critical for public healthcare where nodes may not be fully trusted. BFT, effective in permissioned settings, lacks the decentralization needed for broad interoperability among healthcare providers. PoW's computa-

tional barrier, though costly, aligns with our goal of maximizing security against Sybil and insider threats, as detailed in section 3.2, making it suitable despite energy drawbacks. RSA was chosen for key generation and encryption due to its maturity, widespread support in cryptographic libraries, and compatibility with existing healthcare standards like HIPAA, which often require established asymmetric encryption methods for secure access control. While alternatives like ECC offer smaller key sizes and faster computation, RSA's larger key sizes (e.g., 1024 bits) provide a higher security margin against brute-force attacks, critical for protecting sensitive health data over long-term storage.

5.5 Scaling challenges in real-world healthcare environments

While the proposed framework demonstrates scalability for up to 500 transactions, real-world healthcare environments present additional challenges. A large-scale healthcare network, such as a national health system, may involve hundreds or thousands of nodes (e.g., hospitals, clinics, and labs), significantly increasing network complexity. Our evaluation with 5 nodes showed a throughput of 38 tx/s for 500 transactions, but as node count scales to hundreds, network latency could rise due to increased consensus overhead in PoW, potentially exceeding 100 ms per transaction based on linear extrapolation. This could impact real-time access to critical patient records during emergencies, necessitating optimizations like sharding or hybrid consensus mechanisms (e.g., combining PoW with PoS).

Integration with legacy healthcare systems also poses a challenge. While our framework complies with standards like HL7 FHIR and DICOM, many healthcare providers rely on outdated systems lacking API support for blockchain integration. For instance, a hospital using a 1990s-era EHR system may require custom middleware to map data to FHIR resources, introducing deployment complexity and potential security risks during data migration. Additionally, the computational requirements of PoW and RSA encryption (e.g., $O(k^3)$ complexity for RSA key generation, may strain resource-constrained environments, such as rural clinics with limited hardware. Future work could explore lightweight cryptographic alternatives (e.g., ECC instead of RSA) and off-chain computation to mitigate these challenges, ensuring broader adoption across diverse healthcare settings.

6 Conclusion

This study tackles the increasing need for digital transformation in healthcare by introducing a secure storage system built on a privacy-focused and high-performance blockchain. A standout feature of this system is its reliable access control mechanism, which facilitates the safe and efficient exchange of health records among authorized users. By structuring functional units and implementing a systematic blockchain-enabled process, the model facilitates decentralized data storage while maintaining data confidentiality, availability, integrity, and scalability.

The proposed framework significantly enhances security compared to conventional healthcare data management schemes, allowing consultants or users to store and access medical records securely. Performance evaluation metrics, including publishing transaction time cost and latency, demonstrate the system's ability to efficiently process health data transactions across multiple user nodes. Compared to traditional storage methods, this blockchain based approach offers a robust and reliable solution for managing health records in public health centers.

Despite its advantages, the system's reliance on blockchain technology presents a potential limitation in terms of energy consumption during data transactions and storage. This raises environmental concerns, particularly as blockchain networks grow in scale. Future research will focus on optimizing energy efficiency and extending the framework to include metadata auditing for cloud storage, further enhancing security and data management capabilities in healthcare environments.

Funding

Independent fund project of Shaanxi Provincial Intelligent New Criminal Technology Practical Application Research Center (SXZHXJ202202)

References

[1] M. Alshare et al. "Assessing Blockchain's Role in Healthcare Security: A Comprehensive Review". In: *Informatica* (2024). url: https://www.informatica.si/index.php/informatica/article/view/6155.

[2] N. Al Asad et al. "Permission-Based Blockchain with Proof of Authority for Secured Healthcare Data Sharing". In: *2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT)*. IEEE, 2020, pp. 35–40.

[3] I. Boumezbeur and K. Zarour. "Privacy-Preserving and Access Control for Sharing Electronic Health Record Using Blockchain Technology". In: *Acta Informatica Pragensia* (2022). url: https://www.ceeol.com/search/article-detail?id=1061177.

[4] M. Bowman et al. "Private Data Objects: an Overview". In: *arXiv preprint* arXiv:1807.05686 (2018).

[5] Raymond Cheng et al. "Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts". In: *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. 2019, pp. 185–200. doi: 10.1109/EuroSP.2019.00023.

[6] M.S. Islam et al. “Healthcare-Chain: Blockchain-Enabled Decentralized Trustworthy System in Healthcare Management Industry 4.0 with Cyber Safeguard”. In: *Computers, MDPI* 12.2 (2023), p. 46.

[7] A. Khatoon. “A blockchain-based smart contract system for healthcare management”. In: *Electron.* 9.1 (2020).

[8] R. Khemaissia et al. “Prschain: A Blockchain-Based Privacy Preserving Approach for Data Service Composition”. In: *Informatica* (2023). url: https://www.informatica.si/index.php/informatica/article/view/5081.

[9] A. R. Lee, M. G. Kim, and I. K. Kim. “SHAREChain: Healthcare data sharing framework using Blockchain-registry and FHIR”. in: *Proc. - 2019 IEEE Int. Conf. Bioinforma. Biomed. BIBM 2019*. 2019, pp. 1087–1090.

[10] R.K. Mishra, R.K. Yadav, and P. Nath. “Integration of Blockchain and IPFS: Healthcare Data Management & Sharing for IoT Environment”. In: *Multimedia Tools and Applications* (2024).

[11] C. D. Parameswari and V. Mandadi. “Healthcare data protection based on blockchain using solidity”. In: *Fourth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*. IEEE, 2020, pp. 577–580.

[12] M.A. Rahman et al. “EduChain: CIA-compliant blockchain for intelligent cyber defense of microservices in education industry 4.0”. In: *IEEE Transactions on Industrial Informatics* 18.3 (2021), pp. 1930–1938.

[13] V. Ramani et al. “Secure and Efficient Data Accessibility in Blockchain Based Healthcare Systems”. In: *2018 IEEE Glob. Commun. Conf. GLOBECOM 2018 - Proc.* 2018.

[14] H. Wang and Y. Song. “Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain”. In: *Journal of Medical Systems* 42.8 (2018), p. 152.

[15] G. Yang and C. Li. “A design of blockchain-based architecture for the security of electronic health record (EHR) systems”. In: *Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom*. Vol. 2018-December. 2018, pp. 261–265.

[16] Z. Ying et al. “A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud”. In: *IEEE Access* 6 (2018), pp. 53698–53708.

[17] M.H. Al-Zubaidie and R.H. Razzaq. “Maintaining Security of Patient Data by Employing Private Blockchain and Fog Computing Technologies Based on Internet of Medical Things”. In: *Informatica* (2024). url: https://www.informatica.si/index.php/informatica/article/view/6047.