PLOS ONE

RESEARCH ARTICLE

# A robust algorithm for authenticated health data access via blockchain and cloud computing

**Ali Shahzad[1], Wenyu Chen[1]*, Momina Shaheen[2], Yin Zhang[3], Faizan Ahmad[4]***

**1** School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan, China, **2** Department of Computing, University of Roehampton London, London, United Kingdom, **3** School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan, China, **4** Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, United Kingdom

* Cwy@uestc.edu.cn (WC); Fahmad@cardiffmet.ac.uk (FA)





**Citation:** Shahzad A, Chen W, Shaheen M, Zhang Y, Ahmad F (2024) A robust algorithm for authenticated health data access via blockchain and cloud computing. PLoS ONE 19(9): e0307039. https://doi.org/10.1371/journal.pone.0307039

**Editor:** Shadab Alam, Jazan University, SAUDI ARABIA

**Received:** March 9, 2024

**Accepted:** June 27, 2024

**Published:** September 23, 2024



**Data Availability Statement:** All relevant data are within the paper.

**Funding:** The author(s) received no specific funding for this work.

**Competing interests:** The authors have declared that no competing interests exist.

## Abstract

In modern healthcare, providers increasingly use cloud services to store and share electronic medical records. However, traditional cloud hosting, which depends on intermediaries, poses risks to privacy and security, including inadequate control over access, data auditing, and tracking data origins. Additionally, current schemes face significant limitations such as scalability concerns, high computational overhead, practical implementation challenges, and issues with interoperability and data standardization. Unauthorized data access by cloud providers further exacerbates these concerns. Blockchain technology, known for its secure and decentralized nature, offers a solution by enabling secure data auditing in sharing systems. This research integrates blockchain into healthcare for efficient record management. We proposed a blockchain-based method for secure EHR management and integrated Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for fine-grained access control. The proposed algorithm combines blockchain and smart contracts with a cloud-based healthcare Service Management System (SMS) to ensure secure and accessible EHRs. Smart contracts automate key management, encryption, and decryption processes, enhancing data security and integrity. The blockchain ledger authenticates data transactions, while the cloud provides scalability. The SMS manages access requests, enhancing resource allocation and response times. A dual authentication system confirms patient keys before granting data access, with failed attempts leading to access revocation and incident logging. Our analyses show that this algorithm significantly improves the security and efficiency of health data exchanges. By combining blockchain's decentralized structure with the cloud's scalability, this approach significantly improves EHR security protocols in modern healthcare setting.

## 1 Introduction

Since the early 21st century, significant advancements in digital technologies have revolutionized the global healthcare sector. This revolution is most notable in the transition from

traditional paper records to digital ones, specifically Electronic Health Records (EHRs) [1, 2]. EHRs, structured digital repositories, store various patient data like lab results, medical history, and medication records [3]. They offer several benefits over paper records, such as reduced labor, time, and space requirements [4].

The healthcare industry, with its growing reliance on various digital applications and services, generates immense amounts of data daily. This increase in data has made robust storage and management services essential, with cloud computing emerging as a key solution [5]. Cloud Service Providers (CSPs) offer cost-effective and efficient infrastructure for data storage and processing, attracting both individual and institutional users [6, 7]. Cloud-based electronic health (eHealth) systems efficiently manage EHRs, allowing for secure data sharing across healthcare networks [8, 9].

However, the use of cloud-based eHealth systems raises significant security and privacy concerns [10]. When EHRs are stored on cloud servers, issues such as data ownership, access control, and security breaches become critical challenges. These challenges can hinder the adoption and growth of cloud-based services [11, 12].

One effective way for data security within cloud computing, encryption stands as a best technology among them. Researchers often turn to encryption technologies to secure data that is outsourced to the cloud. Among these technologies, ciphertext-policy attribute-based encryption is recognized as an effective way to implement access control on less reliable cloud storage servers. Despite the existence of numerous schemes aimed at ensuring data confidentiality and user privacy, challenges persist, particularly in the effective identification, tracking, and revocation of permissions for users who misuse their access, underscoring the need for enhanced access control systems. These systems must not only provide ease of access for authorized users but must also have stringent measures for promptly revoking access when a security breach occurs. Additionally, incorporating blockchain technology can enhance security. Blockchain's transparent and immutable record-keeping is useful for secure and efficient data management, addressing concerns about data integrity [13–15].

Therefore, we propose a blockchain-enhanced security model for EMR, emphasizing traceable and direct access revocation. our research provides a scalable, efficient, and practical solution for secure healthcare data management. By combining blockchain's decentralized structure with the scalability of cloud computing, our approach significantly improves EHR security protocols, ensuring robust data security and seamless performance in modern healthcare settings.

## Our key contributions and innovations

1. **Blockchain-Empowered Security**: Our research introduces a blockchain-based method to protect privacy and secure Electronic Medical Records (EMRs). This approach leverages smart contracts to automate key management, encryption, and decryption processes, ensuring robust security and flexible access revocation.
2. **Advanced Encryption with CP-ABE**: We integrate Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to enhance data security by embedding access control policies within the ciphertext. This ensures fine-grained access control, allowing only authorized personnel to access sensitive medical data. Additionally, the dual authentication system confirms patient keys before granting data access, with failed attempts leading to access revocation and incident logging.

3. **Comprehensive Security Analysis**: We performed an in-depth security analysis demonstrating the scheme's resilience against various cyber threats and its efficiency in key management, encryption, and decryption processes.
4. **Performance Analysis and Scalability**: We conducted extensive performance evaluation, including detailed simulation experiments. Our results show that the scheme performs well in terms of communication and storage efficiency, handling large data volumes effectively. The assessment within a blockchain environment, focusing on throughput and delay, confirmed its effectiveness and practical applicability, making it highly suitable for modern healthcare systems.

The paper is organized as follows: Section 2 presents the related works, Section 4 details the system architecture, Section 7 covers the security model, Sections 9 and 10 present the security analysis and protocol design, while Section 11 presents simulation and experiments, and Section 14 summarizes our findings.

## 2 Related work

In the domain of blockchain technology for access control schemes with traceability and revocability for healthcare data management, a spectrum of research has been conducted, each contributing uniquely to the field.

T. Benil and J. Jasper's work, investigates the utilization of blockchain for managing electronic health records (EHRs), focusing on crucial aspects of data integrity and access control. However, this study brings to light concerns regarding the scalability and computational efficiency of blockchain technologies in healthcare contexts [16]. Similarly, K. Anil and Dr. Megha Kamble's "Health Block" presents a blockchain-based system adapted for healthcare data, prioritizing user-friendliness and data integrity. Aside from its innovative approach, the study falls short in thoroughly analyzing the scalability and transaction costs associated with such systems [17]. Maria Guzman Lizama and her team's systematic review of the application of blockchain for medical image sharing in the cloud environment emphasizes the security benefits of this technology. But, the review underscores the necessity for further research focusing on the scalability and efficiency of blockchain in medical contexts [18].

In Integration of Blockchain and Cloud Computing in Telemedicine and Healthcare by Asma Albassam et al. offer an insightful overview of the integration potential of blockchain and cloud computing. The paper identifies an urgent need for additional research in data manipulation and secure storage patterns within these systems [19]. Shujiang Xu and her colleagues introduce a blockchain-based scheme enhancing privacy in mobile health. Despite its advancements, the research highlights a gap in understanding its scalability and practical applicability in real-world scenarios [20].

Mercy Ehiwuogwu's investigation into the integration of blockchain technology in EHR systems is a notable contribution that discusses the enhancement of security and privacy. However, this study does not examine deeply the practical implementation challenges that such systems might face [21]. The work of Insaf Boumezbeur and Karim Zarour on hybrid encryption for healthcare data sharing in cloud environments shows promising improvements in performance. Yet, it also acknowledges the necessity for more comprehensive research into the scalability and practicality of these systems [22].

The paper "Privacy and Security of Blockchain in Healthcare" [23] offers a thorough analysis of the diverse applications of blockchain in healthcare, highlighting enhanced data integrity and patient control over their data. However, the study calls for more case studies and real-world applications to demonstrate the practicality of these blockchain solutions in healthcare

settings. [24] Upadrista addresses the potential of blockchain in remote health monitoring. It brings attention to significant challenges, including scalability, energy consumption, and the need for standardized health data formats. Anandarshan K Hebballi and his team focus on enhancing patient data privacy [25]. The study suggests a need for further exploration into the computational overhead and the practicality of implementing such systems in healthcare settings.

Xiaohong Zhang, Wenqi Du, and Ata Jahangir Moshayedi present a blockchain-based security model for data storage, introducing features like traceability and revocation. However, the study recognizes the need for more analysis of the scalability and applicability of these features in real-world scenarios [26]. Zhe Liu et al. [27] contribute to the field with a user revocation scheme in CP-ABE systems. However, his research calls for more exploration of practical implementation aspects of their scheme.

Hui Cui in "An Efficient and Expressive Ciphertext-Policy Attribute-Based Encryption Scheme" addresses the privacy challenges in ABE systems. The research indicates a gap in understanding the real-world application and system integration of these schemes [28]. Takeru Naruse and his team, in their paper "Attribute-Based Encryption with Attribute Revocation and Grant Function," introduce a proxy re-encryption-based ABE scheme. The study highlights the need for scalability research, particularly in large-scale cloud environments [29].

Humera Aqeel and Syed Taqi Ali's in [30] "Directly Revocable Attribute-Based Encryption Scheme under Ciphertext-Policy" offers an efficient user revocation method. However, the paper acknowledges the lack of in-depth exploration into scalability and computational overhead challenges.

Shangping Wang [31] in his paper proposes a traceable CP-ABE scheme for cloud storage, focusing on collusion resistance and computational efficiency. However,The main drawback is that even when a malicious user is traced, they cannot be efficiently revoked from the crypto system. The "Traceable-then-revocable ciphertext-policy attribute-based encryption scheme" paper develop a scheme with enhanced traceability and direct user revocation. However author mentioned that system can only achieve white-box traceability, which is less robust compared to black-box traceability [32].

Yong Cheng et al.'s in "Directly Revocable Attribute-Based Encryption" for CP-ABE systems in cryptographic cloud storage focuses on reducing the data owner's workload. Still, it recognizes the potential increase in data publication and retrieval costs as a drawback [33].

Zaid Ameen Abduljabbar's work emphasizes the need for secure and efficient key management protocols in healthcare settings, highlighting their proposed scheme's resilience against various security threats [34]. Samir M. Umran et al. demonstrate the integration of blockchain with their work to ensure data security and privacy in industrial settings, highlighting challenges in scalability and computational efficiency [15].

Samir and his team discusses the application of blockchain to enhance the security and reliability of their work, pointing out the need for lightweight cryptographic solutions to address resource constraints [13]. On the other hand Umran and Songfeng emphasizes in their work the importance of efficient consensus algorithms and data encryption mechanisms to secure industrial IoT data while maintaining low power consumption and high performance [14].

Similarly Vincent Omollo introduces an elliptic curve cryptography-based protocol to ensure data integrity and confidentiality in healthcare communications, addressing key concerns related to scalability and practical implementation in real-world scenarios [35]. Mustafa A. Al Sibahee focuses on enhancing security through biometric validation techniques, ensuring robust protection against unauthorized access in healthcare devices [36].

Lastly Umran presented the application of blockchain in industrial settings, emphasizing the need for scalable and efficient solutions to manage and secure data [37].

Each of these studies contributes valuable insights into the evolving field of blockchain and encryption technologies in healthcare data management, highlighting both their potential and the challenges that need to be addressed.

Despite the valuable contributions of these studies, several key limitations and gaps can be identified:

1. **Scalability Concerns**: Many existing schemes face scalability challenges when applied to large-scale healthcare systems or environments with high data volumes and numerous users. Further research is needed to ensure the practical scalability of these solutions in real-world healthcare settings.
2. **Computational Overhead**: Some of the proposed schemes introduce significant computational overhead, which may hinder their performance and efficiency, particularly in resource-constrained environments or with time-sensitive healthcare applications.
3. **Practical Implementation Challenges**: While many studies provide theoretical frameworks or simulations, there is a lack of comprehensive guidance and practical implementations to facilitate the seamless integration of these solutions into existing healthcare information systems and workflows.
4. **Interoperability and Data Standardization**: The integration of blockchain technology and secure access control mechanisms with diverse electronic health record (EHR) systems and healthcare data formats remains a challenge, highlighting the need for standardization and interoperability efforts.
5. **User Acceptance and Adoption**: The successful adoption of these solutions in healthcare settings requires addressing user acceptance factors, such as ease of use, training, and change management strategies, which have received limited attention in existing research.

Our research aims to address these gaps by proposing a scalable, efficient, and practical blockchain-based solution for secure healthcare data management, with a focus on traceability, direct access revocation, and seamless integration with existing healthcare systems and workflows.

## 3 Preliminaries

In this section, we provide an overview of the essential concepts and technologies used in our research, which are crucial for understanding the security model and proof of our proposed scheme.

### 3.1 Blockchain technology

Blockchain technology forms the backbone of our secure data management system. It is a decentralized ledger that records transactions across multiple nodes to ensure data integrity, transparency, and immutability. Each block in the blockchain contains a cryptographic hash of the previous block, a timestamp, and transaction data, creating a secure and tamper-proof chain of records [38].

### 3.2 Cloud computing

Cloud computing offers scalable and cost-effective infrastructure for storing and processing large volumes of healthcare data. Cloud Service Providers (CSPs) enable healthcare organizations to store Electronic Health Records (EHRs) in a secure, remote environment, facilitating efficient data sharing and management across healthcare networks [39].

### 3.3 Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

CP-ABE is an advanced encryption technique that enhances data security by embedding access control policies within the ciphertext. In CP-ABE, the data owner defines an access policy and encrypts the data such that only users whose attributes satisfy the policy can decrypt the information. This method ensures that only authorized personnel can access sensitive medical data [40].

### 3.4 Smart contracts

Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They run on the blockchain, enabling automated and secure transactions without intermediaries. In our system, smart contracts automate key management, encryption, and decryption processes for EHRs, ensuring that only authorized access is granted [41].

### 3.5 Notation and symbols

This section introduces the important symbols, notations, and cryptographic assumptions used throughout the paper as shown in Table 1.

### 3.6 Bilinear maps

A bilinear map $e : G_1 \times G_1 \rightarrow G_T$ has the following properties:

1. **Bilinearity**: For all $u, v \in G_1$ and $a, b \in \mathbb{Z}_p$, $e(u^a, v^b) = e(u, v)^{ab}$.
2. **Non-degeneracy**: There exists $g \in G_1$ such that $e(g, g) \neq 1$.
3. **Computability**: There is an efficient algorithm to compute $e(u, v)$ for all $u, v \in G_1$.

**Table 1. Notation and symbols.**

| Symbol | Description |
|---|---|
| G, GT | Cyclic groups of prime order p; G is the source group, and GT is the target group. |
| g | Generator of the group G. |
| e | Bilinear map $e : G \times G \rightarrow GT$. |
| H | Hash function mapping binary strings to elements of G, $H : \{0, 1\}^* \rightarrow G$. |
| $\alpha, \beta$, a, b | Randomly chosen values from the set $Z_p$. |
| PK | Public key used in the encryption scheme. |
| MK | Master key kept secret and used in the key generation process. |
| ui | User identifier within the system. |
| Lui | Attribute list for user i. |
| SKui | Secret key for a user i. |
| C | Ciphertext produced by the encryption algorithm. |
| Pi | Access policy for data Mi. |
| Ti | Access tree corresponding to Pi. |
| s | Random element from $Z_p$ used in the encryption process. |
| D | Decryption key for user ui. |
| λ | Lagrange coefficients used in polynomial interpolation. |
| f | Function to extract plaintext from decrypted messages. |
| addrID | Unique identifier for an account based on the user's password. |
| AC | Authentication Center responsible for verifying and delegating decryption. |
| SMS | Service Management System handling administrative tasks such as verifying decryption keys and tracking malicious users. |

https://doi.org/10.1371/journal.pone.0307039.t001

### 3.7 Decisional Bilinear Diffie-Hellman (DBDH) assumption

The DBDH assumption states that for any probabilistic polynomial-time adversary, the advantage in distinguishing between the tuple $(g, g^a, g^b, g^c, e(g, g)^{abc})$ and $(g, g^a, g^b, g^c, T)$ for a random $T \in G_T$ is negligible.

### 3.8 Integration of technologies

The integration of blockchain, cloud computing, CP-ABE, and smart contracts creates a synergistic framework that addresses the key challenges of data security, access control, and scalability in healthcare. Blockchain ensures data integrity and provides a transparent audit trail, while cloud computing offers scalable storage solutions. CP-ABE enhances data security with fine-grained access control, and smart contracts automate and secure the data management processes. Together, these technologies form a comprehensive solution for managing EHRs, ensuring that patient data is secure, accessible, and efficiently managed across healthcare systems.

By combining these advanced technologies, our research proposes an approach to secure healthcare data management, addressing the critical concerns of data privacy, security, and efficiency in the modern healthcare landscape.

## 4 The system architecture of data access control

Our system design introduces a secure, privacy data exchange framework, detailed in the system architecture depicted in Fig 1. This framework comprises nine key components, each outlined below.

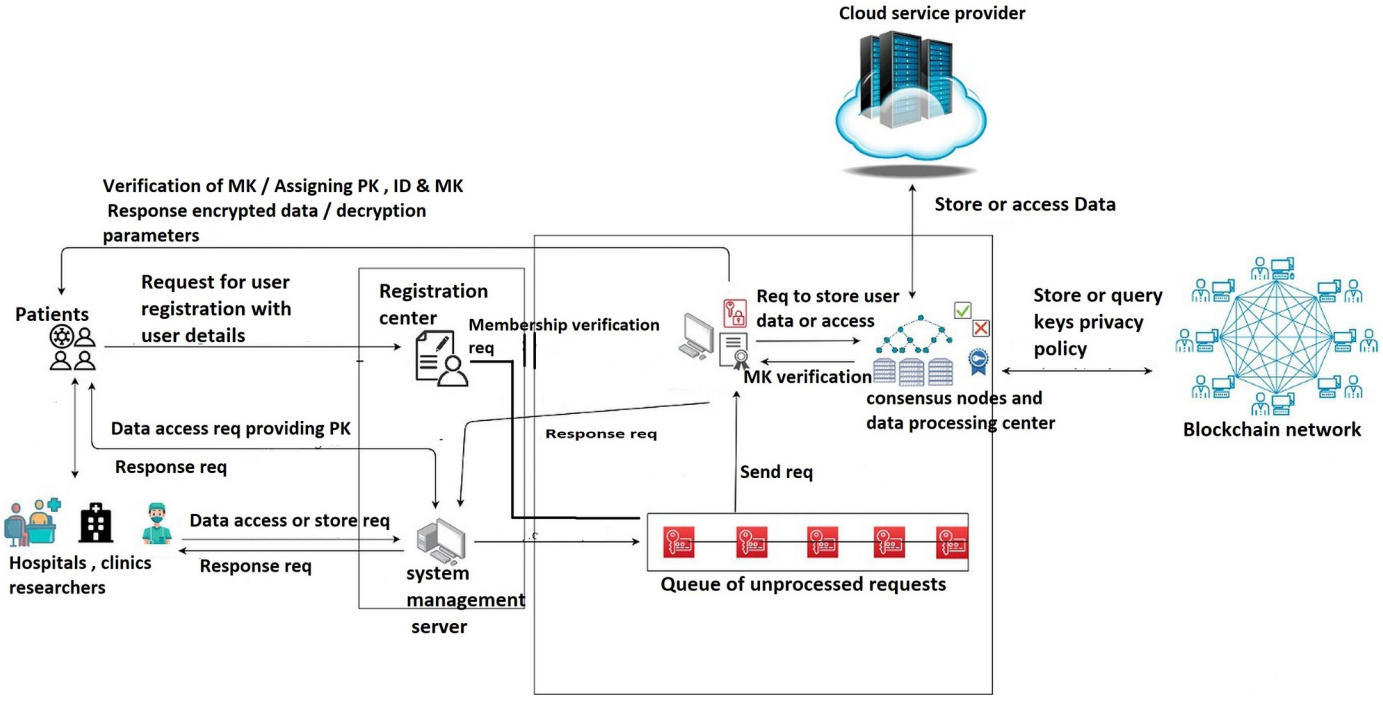


**Fig 1. System design.**

https://doi.org/10.1371/journal.pone.0307039.g001

### 4.1 Patients

In our system, patients are main participants. By enrolling in the system, they become active blockchain users, each receiving a unique identifier (ID), a public key (PK), and a master key (MK). It's crucial for patients to securely safe their MK.

### 4.2 Medical practitioners

Medical practitioners are enabled to request or upload data using Service management system (SMS), leveraging the patient's PK. Data is stored on a cloud service provider (CSP) after the patient's MK is authenticated.

### 4.3 Registration center

Registration centers get requests from patients and medical practitioners to join the network. Once the registration center gets details from users after verifying them, the registration center will generate ID, PK, and MK for the user. later, the registration center requests the Authentication center to verify these keys with the users.

### 4.4 Service management system (SMS)

The SMS serves as a reliable administrative entity, facilitating hospital services to users. It maintains a database of public keys and IDs for medical professionals, processes data access or storage requests, and oversees user activities. It has the authority to withdraw data access in case of suspicious activities.

### 4.5 Authentication center (AC)

The Authentication Center (AC) plays a crucial role in validating user identities, managing data storage and access on the Cloud Service Provider (CSP), and encrypting user data. Integrated with smart contracts, the AC automates and secures key management, encryption, decryption, and access control processes. Smart contracts within the AC ensure the generation, distribution, and management of cryptographic keys; enforce access policies during encryption; verify user attributes during decryption; and log all access attempts immutably on the blockchain. This combination enhances the system's efficiency, security, and transparency, reducing the risk of human error and unauthorized access.

### 4.6 Processing and consensus nodes

These nodes manage data processing within the blockchain network. Data packages from the authentication center are encrypted and logged by processing nodes, then sent for validation. A majority consensus among these nodes is required for a block to be added to the blockchain. Failed verifications return the block to the original node.

### 4.7 Blockchain

The blockchain is providing unified identity verification. It maintains a database of user details, including IDs, PKs, MKs, and specific information for both patients and medical practitioners.

### 4.8 Queue of unprocessed requests

In this layer of the system, all the unprocessed requests will wait for their turn to be executed by the AC. From this, our system would not miss any requests.

### 4.9 Cloud service provider (CSP)

In our proposed system, the data storage layer is managed by a semi-trusted Cloud Service Provider (CSP). The CSP is responsible for storing all medical data, which has been encrypted by the Authentication Center (AC) prior to storage. This ensures that even within a semi-trusted environment, the data remains secure and inaccessible to unauthorized parties. The CSP offers scalable and reliable storage solutions, capable of efficiently handling large volumes of data. When access is requested, the AC verifies the user's identity and attributes against the blockchain data. Upon successful verification, the AC retrieves the encrypted data from the CSP and provides the decryption parameters to the authorized user. This approach leverages the scalability and availability of cloud storage while maintaining stringent security protocols through encryption and blockchain-based logging.

## 5 System flow

### 5.1 User registration

In this system, first users will request to the registration center to be a member of our system by sending their details UD, and against it, the registration center will generate user ID, PK, and data access policy accordingly and request for MK to the AC. once the AC gets a request for MK from the registration center AC will verify with the user its identity and later AC will generate MK for the user and the user must store this MK secretly. Once the user gets its MK, the AC sends a request to processing and consensus nodes to create a block and store user details, user ID, data access policy, user PK, and MK into the blockchain.

### 5.2 Case 1: Data accessing and storing

When a patient visits a hospital and hospital wants to store or access Electronic Medical Records (EMRs) below steps will be taken.

**Rules of Authentication and Data Retrieval**:

1. **Request Submission**: When hospital staff need to access a patient's Electronic Medical Records (EMRs), they initiate the process by submitting their attributes to the Service management system (SMS) with Patients data. This is the first step in ensuring secure access to sensitive medical data.
2. **Request Queue**: Submitted requests undergo initial verification by the SMS, where the medical practitioner's public key (Pk) is matched against their ID in local databases. Verified requests are then added to a queue of unprocessed requests, ensuring no request is missed.
3. **Authentication and Data Retrieval**:
   - **Forwarding to Authentication Center (AC)**: The queued requests are forwarded to the AC, where a smart contract verifies the user's details and attributes against the blockchain data.
   - **Fetching Encrypted EMRs**: Upon successful authentication, the smart contract fetches the encrypted Electronic Medical Records (EMRs) from the Cloud Service Provider (CSP), as illustrated in Fig 2.
   - **Generating and Verifying Hashes**: Before storing or retrieving the data, a cryptographic hash of the data is generated using the hash function $H : \{0, 1\}^* \rightarrow G$. This hash is stored along with the encrypted data. When the data is retrieved, the hash is recalculated and compared to the stored hash to ensure the data has not been tampered with. This process

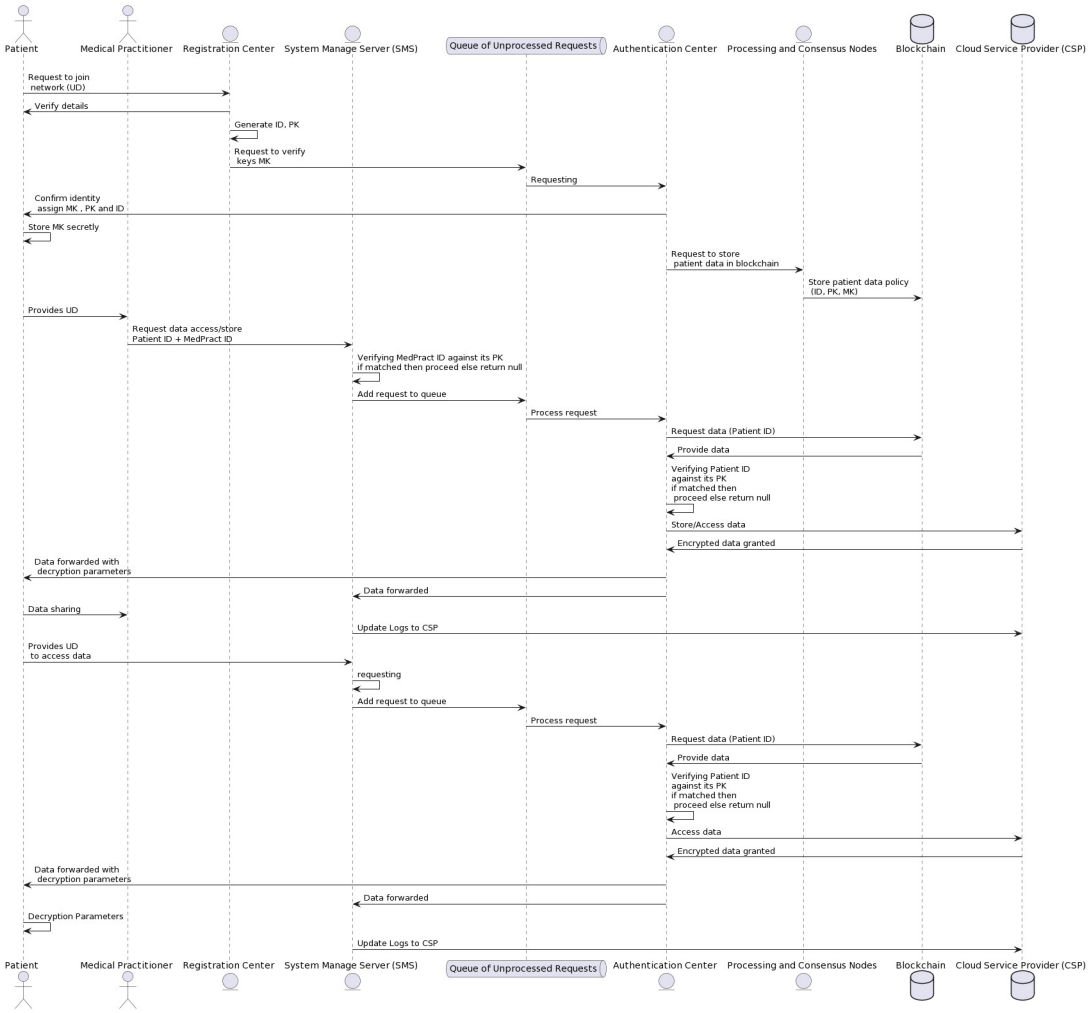


**Fig 2. UML diagram of case 1 and case 2.**

https://doi.org/10.1371/journal.pone.0307039.g002

ensures data integrity and authenticity, protecting the stored data from potential manipulation and unauthorized changes.

- **Transmitting Decryption Parameters**: The smart contract transmits the decryption parameters to the authorized user, ensuring only authenticated users can access the sensitive data.

4. **Data Decryption Request**: Simultaneously, the AC sends intermediary parameters back to the SMS to monitor and control the decryption activities, enhancing overall data access security.
5. **Data Decryption and Access**: With the received decryption parameters and their private key, users can decrypt and access the EMRs, ensuring the confidentiality of patient records during access.
6. **Access Denial and Logging**: In the event of a mismatch or unauthorized access attempt, the SMS denies access and logs the incident. These logs, stored on the CSP, are crucial for tracking potential breaches and maintaining data security.

7. **Data Storage Process**:EMRs created and stored by the hospital are encrypted using Attribute-Based Encryption (ABE) by the AC after verification with the patient's master key (MK). The encrypted records are then hashed, and both the encrypted data and its hash are securely stored on the CSP. This process ensures that any unauthorized changes to the data can be detected.

### 5.3 Case 2: Data accessing

When an individual patient sends a request to SMS for data access or storage.

**Rules of Authentication and Data Retrieval**:

1. **Request Submission**:
   - When a patient wants to access Electronic Medical Records (EMRs), the patient send a request to the Service management system (SMS) with its data
2. **Request Queue**: After a request submission, SMS transmits the request to a queue of unprocessed requests, awaiting its turn for further processing.
3. **Authentication and Data Retrieval**:
   - **Forwarding to Authentication Center (AC)**: The queued requests are forwarded to the AC, where a smart contract verifies the user's details and attributes against the blockchain data.
   - **Fetching Encrypted EMRs**: Upon successful authentication, the smart contract fetches the encrypted Electronic Medical Records (EMRs) from the Cloud Service Provider (CSP).
   - **Verifying Hashes**: When the data is retrieved, the hash is recalculated and compared to the stored hash to ensure the data has not been tampered with.
   - **Transmitting Decryption Parameters**: The smart contract transmits the decryption parameters to the authorized user, ensuring only authenticated users can access the sensitive data.
4. **Data Decryption Request**: Simultaneously, the AC sends intermediary parameters back to the SMS to monitor and control the decryption activities, enhancing overall data access security.
5. **Data Decryption and Access**: With the received decryption parameters and their private key, users can decrypt and access the EMRs, ensuring the confidentiality of patient records during access.
6. **Access Denial and Logging**: In the event of a mismatch or unauthorized access attempt, the SMS denies access and logs the incident. These logs, stored on the CSP, are crucial for tracking potential breaches and maintaining data security.

## 6 Protocol illustration

We employ a robust and secure encryption algorithm, Ciphertext-Policy Attribute-Based Encryption (CP-ABE), integrated with blockchain technology, to ensure the confidentiality, integrity, and traceability of Electronic Health Records (EHRs). The Security Algorithm Framework consists of cryptographic operations for secure and traceable EHR management in cloud systems (as shown in Table 2). Our implementation includes the following key components:

**Table 2. Security algorithm framework.**

| |
|---|
| 1: **procedure** SystemSetup(λ) |
| 2: Select distinct groups $G$ and $G_T$ with a prime order $p$, and choose an element $g$ from $G$. |
| 3: Select a bilinear map function $e$ that maps elements from $G * G$ to $G_T$. |
| 4: Randomly choose values $\alpha$ and $\beta$ from the set $\mathbb{Z}_p$. Subsequently, calculate $g^{\alpha}$, $g^{\beta}$, and $e(g, g)^{\alpha\beta}$. |
| 5: Define a hash function $H$ that converts binary strings $H : \{0, 1\}^* \rightarrow G$ |
| 6: **return** $(g, g^{\alpha}, g^{\beta}, e(g, g)^{\alpha\beta}, H)$ |
| 7: **end procedure** |
| 8: **procedure** KeyGeneration$(g, g^{\alpha}, g^{\beta})$ |
| 9: For user $i$ with attributes $A_i$, pick random $r_i \in \mathbb{Z}_p$ |
| 10: Compute secret keys $SK_i$ for each attribute $a \in A_i$ |
| 11: $SK_i[a] \leftarrow g^{(r_i + H(a))\beta}$ |
| 12: **return** $SK_i$ |
| 13: **end procedure** |
| 14: **procedure** Encryption$(M, g, g^{\beta}, H, \mathcal{T})$ |
| 15: Choose a random element $s$ from $\mathbb{Z}_p$ and compute $C_0$ as the product of $M$ and $e(g, g)^{\alpha s}$. |
| 16: For each $a_j \in \mathcal{T}$, compute $C_j = g^s \cdot H(a_j)^s$ |
| 17: **return** $(C_0, \{C_j\}_{j \in \mathcal{T}})$ |
| 18: **end procedure** |
| 19: **procedure** Decryption$(C_0, \{C_j\}, SK_i, \mathcal{T}, H)$ |
| 20: Validate that $SK_i$ satisfies $\mathcal{T}$ |
| 21: Compute $e(g^{\beta}, C_j)/e(SK_i[a_j], g)$ for each $a_j \in \mathcal{T}$ |
| 22: Recover $M$ from $C_0$ using the computed values |
| 23: **return** $M$ |
| 24: **end procedure** |
| 25: **procedure** Challenge$(g, g^{\alpha}, g^{\beta}, H, \mathcal{T}, \mathcal{A})$ |
| 26: Choose random messages $M_0$, $M_1$, compute C* = Encryption($M_b$, . . .) for a random bit $b$ |
| 27: Adversary $\mathcal{A}$ attempts to guess $b$ given C* and access to a decryption database. |
| 28: **return** success if $\mathcal{A}$ guesses $b$, otherwise failure |
| 29: **end procedure** |

https://doi.org/10.1371/journal.pone.0307039.t002

## 6.1 System setup initialization

The initial step involves invoking the `setup` function to generate the Primary key (PK) and Master key (MK). This involves choosing two bilinear groups, denoted as $G_T$ and $G$ each associated with a prime number $p$. We establish a bilinear map $e : G \times G \rightarrow G_T$ based on two generators $g$ and $v$. We define $U = \{\text{addrID}_{ui} \mid 1 \leq i \leq n\}$ as the user set and attr = $\{a_j \mid 1 \leq i \leq m\}$ as the global attribute set. A query list $v$ initiates with the state, comprising a random parameter and an addrID. We select a hash function $H : \{0, 1\}^* \rightarrow G$ and choose random elements $a, b \in \mathbb{Z}_p$. The system ultimately outputs the Primary key PK and Master key MK, which are defined as follows:

$$PK = \{g, v, h = v^b, \hat{h} = g^b, y = e(g, v)^a, H\}.$$
$$MK = \{a, b\}$$

## 6.2 Generate keys

To generate user-specific keys, `KeyGen`(MK, $L_{ui}$, addrID$_{ui}$) outputs ($DK_{ui}$, $SK_{ui}$). For each user *ui*, based on their attribute set $L_{ui}$ and identification addrID$_{ui}$, A random element $t$ from the set of $\mathbb{Z}_p$ is chosen, and the following calculations are performed:

$$\begin{aligned} D_{ui}^{(1)} &= g^{(a+t)/(b+bt)}, \\ D_{ui}^{(2)} &= \{g^t H(a_j)\}_{a_j \in L_{ui}}, \\ D_{ui}^{(3)} &= g^{\text{addrID}_{ui} bt}, \\ D_{ui}^{(4)} &= h^t. \end{aligned}$$

These parameters, along with $t$, are recorded in $W$. The Secure Key $SK_{ui} = (D_{ui}^{(3)}, D_{ui}^{(4)})$ and the Decryption Key $DK_{ui} = (t, D_{ui}^{(1)}, D_{ui}^{(2)})$ are securely transmitted to user *ui*.

## 6.3 Data encryption

When medical practitioners create medical records, they invoke `Encrypt(PK, Pi, Mi, R)` to encrypt the data $M_i$ for patient $u_i$ under an access policy $P_i$ and a revocation list $R$. The encryption process involves the following steps:

1. **Develop Access Tree Structure**: Develop an access structure $T_i$ that corresponds to the stipulated policy $P_i$. This structure can be defined using logical operators (AND, OR) and threshold gates to represent the necessary conditions for access.
2. **Random Element Selection**: Choose a random element $g$ from the field $\mathbb{Z}_p$ and perform the following calculations:

$$\begin{aligned} C_p^{(1)} &= M_i \cdot e(g, v)^{ag} \\ C_p^{(2)} &= h^g \end{aligned}$$

3. **Secret Sharing**: Assign secret shares to the tree nodes using threshold secret sharing:
   - For an AND gate, distribute $g$ among child nodes as per the $(t, n)$-threshold scheme.
   - For an OR gate and threshold gates, similarly distribute $g$ using polynomials defined for the $(t, n)$-threshold.
4. **Leaf Node Calculation**: For every leaf $a_j$ in $T$, compute

$$C_{aj,k}^{(3)} = v^{g^k} H(a_j)^{-1},$$

   with $k$ denoting the node index.
5. **Ciphertext Generation**: For each user in the revocation list R, generate a unique random number and compute the corresponding components of the ciphertext. The resulting ciphertext $C_{pi}$ is defined as:

$$C_{pi} = (C_p^{(1)}, C_p^{(2)}, \{C_{aj,k}^{(3)}\}_{a_j \in T_i}, \{C_{uj}^{(4)}\}_{u_j \in R}, \{C_{uj}^{(5)}\}_{u_j \in R}).$$

Smart contracts play a crucial role in this process by verifying the access policy Pi and ensuring that the encryption parameters are correctly calculated and securely stored. The smart contract automates the enforcement of access policies during the encryption process, ensuring that only authorized users can later decrypt the data.

## 6.4 Decryption delegation

The delegation function is defined as `Delegate`(PK, $L_{ui}$, $DK_{ui}$, $C_p^{(2)}$, $C_{j,i}^{(3)}$) which returns $(K_{ui}, C_i')$. When a user requests access to their medical data, they send their attribute list $L_{ui}$ and Decryption Key $DK_{ui}$ to the AC. The Authentication center(AC) carries out the delegation process by identifying the minimal subset $L_0'$ that fulfills the conditions of the access tree $T_i$. For every attribute $a_j$ within $L_0'$, the AC then calculates the corresponding partial decryption factor:

$$K_{ui} = \prod_{a_j \in L_0'} e(D_{ui}^{(1)}, C_p^{(2)}) \cdot e(D_i^{(2)}, C_{a_j,i}^{(3)})^{\lambda_i^{(0)}} \tag{1}$$

where $\lambda_i^{(0)}$ are the Lagrange coefficients for the minimal set $L_0'$. The AC then sends the transformed ciphertext $C_i'$ along with $K_{ui}$ to the user.

## 6.5 Data decryption

The decryption function `Decrypt`($C_{pi}'$, $K_{ui}$, $SK_{ui}$) outputs $M_i'$. Upon receiving $(K_{ui}, C_i')$, the user can proceed with decryption if $\text{addrID}_{ui} \notin R$ and $\text{addrID}_{ui} \in S$. The system calculates the decryption key for each attribute $a_j \in L_0'$ as follows:

$$K' = \prod_{j=1}^{r} \left( \frac{e(D_{uj}^{(3)}, C_{uj}^{(4)})}{e(C_{uj}^{(5)}, D_{uj}^{(4)})} \right)^{\frac{1}{\text{addrID}_{ui} - \text{addrID}_j}} \tag{2}$$

where $r$ is the number of attributes $a_j$ where $\text{addrID}_{uj} \in R$. The final decryption key $K$ and the original message $M_i'$ are obtained by:

$$K = \frac{K_{ui}}{K'} \tag{3}$$

$$M_i' = f\left( \frac{C_p^{(1)}}{K} \right) = f(M_i) \tag{4}$$

where $f$ is a function that extracts the plaintext from the decrypted message. Only the intended user $ui$ with $\text{addrID}_{ui} \in S$ can recover the plaintext by applying the decryption function to the received $(K_{ui}, C_i')$ using their secret key $SK_{ui}$.

## 6.6 Monitoring of malicious users

The tracking function `Trace`(PK, $L_{ui}$, $DK_{ui}$) outputs either the user's address identifier $\text{addrID}_i$ or invalid. The Service management system (SMS) verifies $DK_{ui}$ by checking if addrID can be located in list $W$, using parameter $t$ to monitor decryption activities and provide referential data for tracking potentially malicious users. The process is bifurcated into two parts:

**Verify phase:** Given $L_{ui}$, PK, and $DK_{ui}$, the SMS computes:

$$Rs_1 = e(D^{(1)}, h), \quad Rs_2 = y^{\delta} \cdot \prod_{a_i \in L_{ui}} e(D^{(2)}, h_2) \cdot v^{H(a_i)^{-1}} \tag{5}$$

If $Rs_1 = Rs_2$, the user passes verification as a legitimate user.

**Query phase.** If verification succeeds and $DK_{ui}$ is valid, addrID is retrievable from list $W$ using $t$, and the corresponding addrID is output. If verification fails, the output is false or invalid.

### 6.7 Data re-encryption

The encryption function `Encrypt`(PK, Π, $M_i$, $R_0$) yields $C'_{pi}$. When the revocation list $R$ changes to $R_0$, only elements $\{C^{(4)}_{uj}\}$ for $uj \in R_0$ and $\{C^{(5)}_{uj}\}$ for $uj \in R_0$ in $C_{pi}$ need updating. For instance, upon adding a malevolent user's addrID$_e$ to $R$, the new components $C^{(4)}_e = h^{\text{te}}$ and $C^{(5)}_e = h^{\text{addrID}_e \cdot t^{-1}}$ are included in the updated sets. The revised ciphertext $C''_{pi}$ is defined as:

$$C''_{pi} = (C^{(1)}_p, C^{(2)}_p, \{C^{(3)}_{a_j,k}\}_{a_j \in T_i}, \{C^{(4)}_{uj}\}_{uj \in R_0}, \{C^{(5)}_{uj}\}_{uj \in R_0}) \tag{6}$$

## 7 Security model

In this section, we outline the IND-CPA (Indistinguishability under Chosen Plaintext Attack) cryptographic security model. The model involves a protocol between an adversary, denoted as $\mathcal{A}$, and a challenger, denoted as $\mathcal{B}$. The steps of the protocol are as follows:

1. **Initial Step:** The opponent $\mathcal{A}$ selects a specific access structure $T^*$ and compiles a group of revoked users $R^*$. This data is then passed to the challenger $\mathcal{B}$.
2. **Setup Phase:** The challenger $\mathcal{B}$ generates a $MK$ and a $PK$. The PK is shared with $\mathcal{A}$, while the MK is kept secret.
3. **Phase 1:** $\mathcal{A}$ requests multiple secret keys $SK_u$ that correspond to a predefined list $L^*$. $\mathcal{B}$ produces these keys using a designated key generation algorithm.
4. **Challenge Step:** $\mathcal{A}$ presents two messages of equal size, $M_1$ and $M_2$, to $\mathcal{B}$. $\mathcal{B}$ chooses a random bit $u$ from {0, 1} and encrypts one of the messages using $T^*$ and $R^*$. The ciphertext $C_p$ is then given to $\mathcal{A}$.
5. **Phase 2:** This phase is similar to the First Phase, with $\mathcal{A}$ continuing to request secret keys.
6. **Prediction Step:** $\mathcal{A}$ predicts the value of $u$ as $u'$. The adversary's success is defined if $u' = u$, with the probability given by $\Pr[u' = u] - \frac{1}{2}$.

The security of our model is considered robust if adversaries constrained to polynomial time have but a negligible success probability in the aforementioned game, thereby affirming the system's resilience against plain text disclosure attacks.

## 8 Security proof

Consider a scenario where an adversary, denoted as $\mathcal{R}$, successfully compromises the robustness of an encryption protocol within the IND-CPA security. In response, we formulate an algorithm, $\mathcal{A}$, that utilizes $\mathcal{R}$ to solve the DBDH problem. This is achieved by verifying whether $e(g, g)^z$ is identical to $e(g, g)^{abc}$.

The process is structured as follows:

1. **Initial Step:** Adversary $\mathcal{R}$ picks a specific access structure, $\mathcal{T}'$, and a group of revoked users, $\mathcal{R}'$. These selections are forwarded to the challenger, $\mathcal{A}$.
2. **Preparation Phase:** $\mathcal{A}$ begins by executing the initial setup algorithm. It chooses a random element $x$ from $\mathbb{Z}_p$ and calculates $a$ as $ab+x$, which leads to $y = e(g, g)^a$. Subsequently, $\mathcal{A}$ generates a series of random elements $\{b_i\}_{i=1}^r$, ensuring their collective sum is $b$, and computes $h = \prod_{i=1}^r g^{b_i}$. This results in the creation of both the public key PK and the master key MK, with PK being revealed to $\mathcal{R}$.
3. **Phase 1:** Here, $\mathcal{R}$ requests private keys for users who are neither part of $\mathcal{T}'$ nor among the revoked. In response, $\mathcal{A}$ generates and provides the necessary keys to $\mathcal{R}$.
4. **Challenge Stage:** $\mathcal{R}$ proposes two messages of equal length, $M_1$ and $M_2$. $\mathcal{A}$ randomly chooses $u$ from {0, 1} and encrypts $M_u$ considering both $\mathcal{T}'$ and $\mathcal{R}'$, using a random $s$. The resultant ciphertext, $C'_p$, is then handed over to $\mathcal{R}$.
5. **Phase 2:** Similar like First Phase, $\mathcal{R}$ continues to make further private key requests, to which $\mathcal{A}$ responds as required.
6. **Concluding Guess:** $\mathcal{R}$ then attempts to deduce $u$ and presents its guess as $u'$. If $u'$ matches $u$, $\mathcal{A}$ concludes that $e(g, g)^z$ and $e(g, g)^{abc}$ are equivalent. Otherwise, $\mathcal{A}$ infers that $e(g, g)^z$ is a random value.

## 9 Security analysis of the proposed method

The security of electronic health records (EHRs) in cloud environments is of paramount importance. Our proposed algorithm integrates blockchain and smart contracts with cloud-based healthcare Service Management Systems (SMS) to ensure robust security measures. This section presents a detailed security analysis, demonstrating the resilience of our scheme against various cyber threats.

### 9.1 Data confidentiality

Data confidentiality ensures that sensitive information is accessible only to authorized users. In our system, we achieve confidentiality through the use of Ciphertext-Policy Attribute-Based Encryption (CP-ABE). CP-ABE embeds access control policies within the ciphertext, ensuring that only users whose attributes satisfy the policy can decrypt the data. This method is particularly effective in preventing unauthorized access to EHRs.

### 9.2 Data integrity

Data integrity involves maintaining the accuracy and consistency of data over its lifecycle. Blockchain technology inherently provides immutability and transparency, ensuring that once data is recorded, it cannot be altered or tampered with. Each transaction involving EHRs is hashed and stored on the blockchain, and any attempt to alter the data can be easily detected. This guarantees that the data remains intact and unaltered.

### 9.3 Authentication and authorization

Our system employs a dual authentication mechanism to enhance security. Patients and medical practitioners are required to authenticate their identity using a combination of public keys

(PK) and master keys (MK). The authentication center (AC) validates user identities before granting access to EHRs. This two-factor authentication mechanism ensures that only legitimate users can access the data.

### 9.4 Access control and revocation

The integration of CP-ABE with blockchain allows for fine-grained access control. Access policies are dynamically embedded within the encrypted data, allowing only users with matching attributes to decrypt it. Furthermore, our system supports direct access revocation, where the SMS can revoke data access in case of suspicious activities. The blockchain ledger maintains a log of all access attempts, making it easier to track and revoke permissions for malicious users.

### 9.5 Data auditing and traceability

Blockchain's decentralized ledger provides a transparent and immutable audit trail for all data transactions. This audit trail is crucial for tracking data access and modifications. Smart contracts within the system automate the logging of all access attempts, ensuring that any unauthorized access is promptly detected and logged. This feature enhances the traceability of data and simplifies auditing processes.

### 9.6 Resistance to cyber attacks

Our system effectively handles several critical security threats through its robust design. The dual authentication mechanism and CP-ABE encryption ensure strong defenses against impersonation and dictionary attacks by requiring both public and master keys for access. The decentralized nature of blockchain, coupled with consensus mechanisms, mitigates the risks of Sybil and 51% attacks, while multiple peer connections protect against Eclipse attacks. Time-stamped transactions and nonce values prevent replay attacks by ensuring the uniqueness of each transaction. Additionally, the transparent audit trail provided by the blockchain helps detect and prevent insider threats, ensuring comprehensive security for electronic health records (EHRs).

## 10 Protocol design

### 10.1 Scheme overview

We introduce a suite of cryptographic operations aimed at enabling the traceable and secure management of CEMRs within cloud storage systems. These operations include:

- **IDGen**(***password***): This method generates a distinct account identifier, named **addrID**, based on the user's password. When the AC confirms the policy through the **Delegate()** function, this method yields the decryption elements along with the encrypted data. The user can then apply the **Decrypt()** function for data decryption.
- **Setup**(***security_param***): This function takes a designated security parameter and establishes the system's *PK* and the *MK*.
- **KeyGen**(***MK, attributes, addrID_ui***): Generates a user-specific decryption key *DK_ui* and secret key *SK_ui*, utilizing the master key *MK*, user's attributes, and account identifier.
- **Encrypt**(***PK, policy, M, R***): Encrypts a message *M* using the public key *PK*, an access policy *policy*, and a revocation directive *R*, producing an encrypted output *Cp_i*.
- **Delegate**(***PK, attributes, DK_ui, Cp_i***): Converts the ciphertext *Cp_i* into a form suitable for decryption $Cp'\_i$, using the decryption key *DK_ui*, public key, and user attributes.

- **Decrypt**(***C'pi, K_ui, SK_ui***): Deciphers the transformed ciphertext $C'pi$ back into the original message $M$ using the secret key $SK\_ui$ and decryption parameter $K\_ui$.
- **Trace**(***PK, attributes, DK_ui***): Identifies a user's account $addrID\_ui$ or yields a placeholder based on the public key, user attributes, and decryption key.
- **ReEncrypt**(***PK, policy, M, R'***): Re-encrypts a message in accordance with an updated policy or revocation list, generating a fresh ciphertext $Cp'\_i$.
- **TransactionSave**(***privateKey, addrID, content, timestamp***): Logs transactions on the blockchain using the sender's identifier *addrID*, transaction content *content*, and the timestamp *timestamp*, with the private key *privateKey* serving for authentication. It confirms whether the transaction was successful.

The system's operational process is as follows:

1. Users create a blockchain account, which in turn generates an address $addrID_{ui}$.
2. The SMS implements the Initialization Procedure to set up the system's PK and MK, ensuring they conform to the defined attribute standards of the system.
3. Medical practitioners draft access policies in consideration of patient privacy and encrypt relevant data using **Encrypt()** before dispatching it to the CSP.
4. Users request access to medical data from the CSP by submitting their $DK_{ui}$ and attribute set.

## 11 Simulation experiment

This part of the document evaluates the performance of the suggested framework. Performance metrics were gathered by conducting 700 iterations of linear pairing and exponentiation calculations on a system equipped with an Intel Core i7 processor clocked at 2.7 GHz, running a 64-bit version of Windows 10, and 32 GB of RAM. The selection of Ethereum (Ganache) and Truffle Node for the data environment and for implementation was motivated by its simplified verification process.

In evaluating the performance of networked systems, particularly those based on blockchain technology, throughput and delay serve as crucial metrics. Throughput is the measure of how many transactions a system can handle per second, while delay denotes the time taken for data to be transmitted between nodes, often described as latency. We assessed the system's read and write performance by varying the transaction load from 100 to 700 transactions per second as shown in Table 3.

**Table 3. Selected transaction data.**

| Active Transactions | Transaction Time (ms) | Throughput (Tx/s) |
|---|---|---|
| 100 | 2167 | 46.1 |
| 200 | 3202 | 62.4 |
| 300 | 4305 | 69.6 |
| 400 | 6462 | 61.9 |
| 500 | 6895 | 72.5 |
| 600 | 8426 | 71.2 |
| 700 | 10158 | 68.9 |

https://doi.org/10.1371/journal.pone.0307039.t003

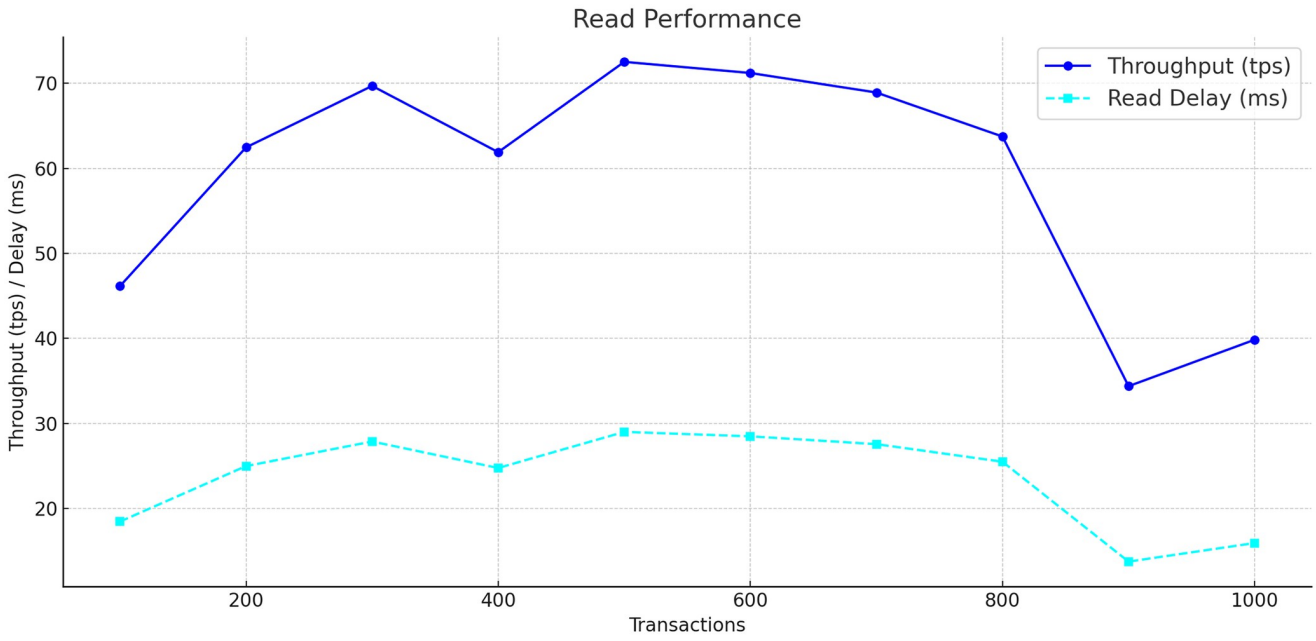


**Fig 3. Read performance and throughput.**

https://doi.org/10.1371/journal.pone.0307039.g003

The resulting graphs Figs 3 and 4 show the read and write performances. In the read performance graph, throughput is represented by the blue line, which shows an increase with the number of transactions. The cyan dashed line indicates the read delay, showing a trend that suggests an increase in latency as transaction volume rises. For write performance, represented

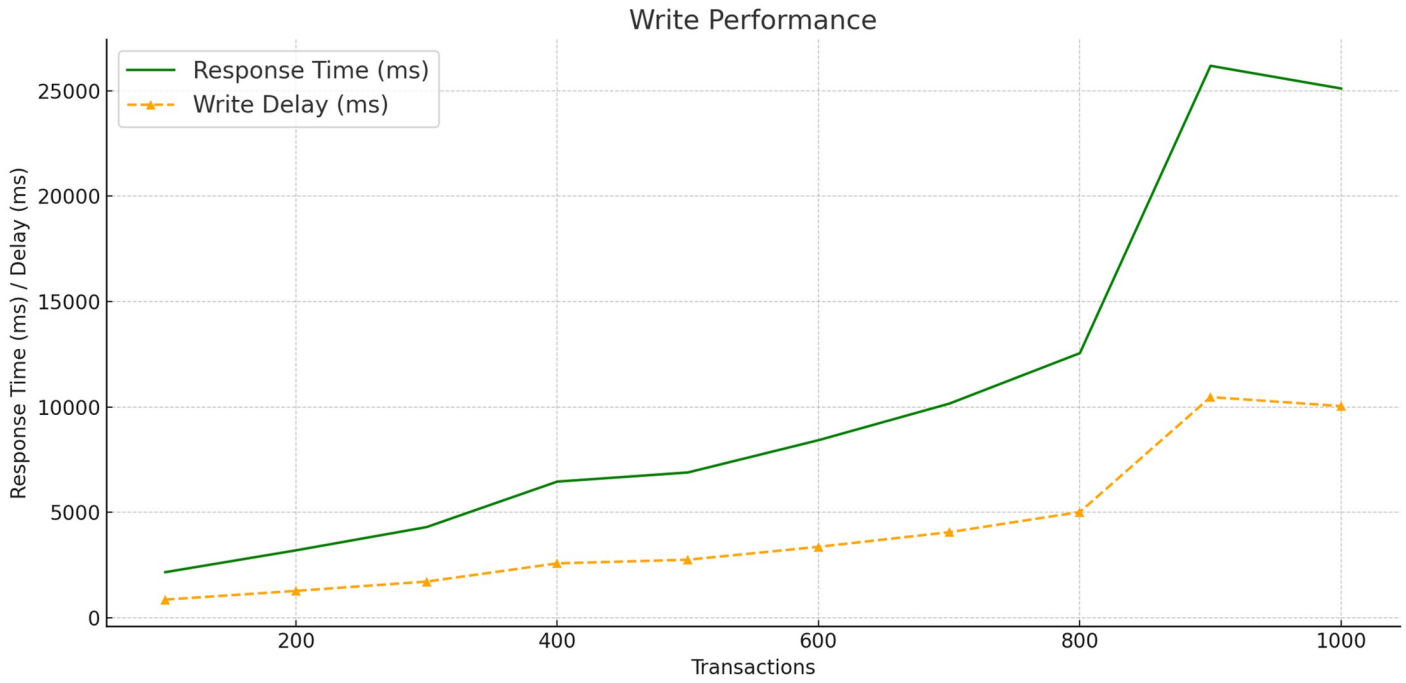


**Fig 4. Write performance and throughput.**

https://doi.org/10.1371/journal.pone.0307039.g004

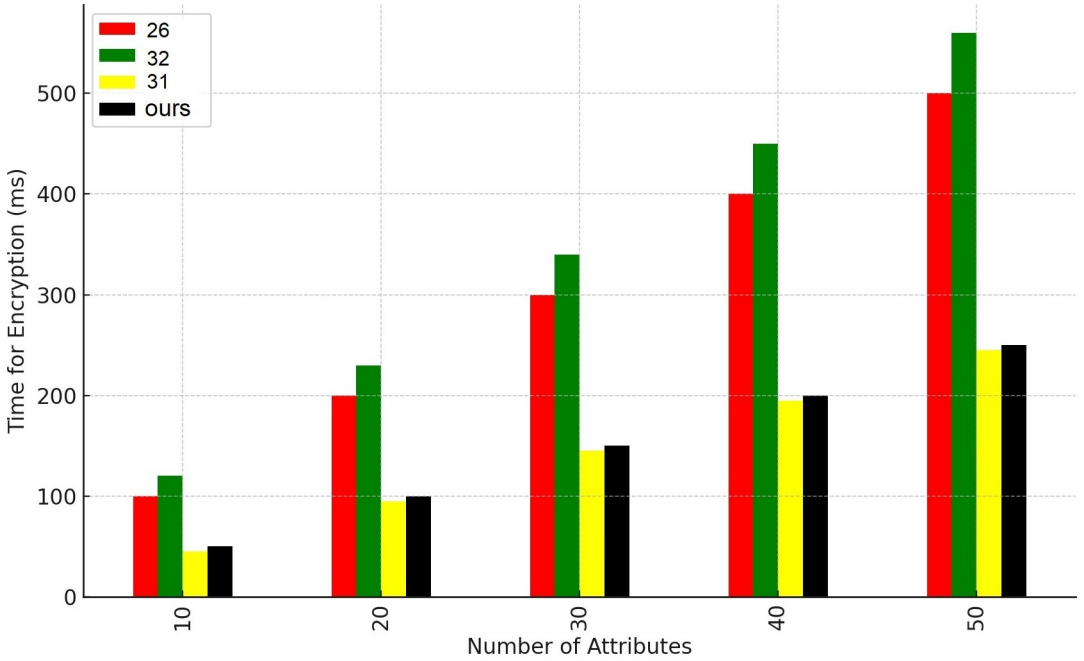


**Fig 5. Encryption performance.**

https://doi.org/10.1371/journal.pone.0307039.g005

by the green line, throughput initially increases with the number of transactions, peaks, and then slightly decreases. The orange dashed line reflects write delay, illustrating a rise in latency with increased transaction volume.

On the other hand The comparison results for time overhead between our proposal and other works [26, 31, 32] are shown in Figs 5 and 6 which shows the system performance in terms of encryption and decryption times. Notably, both the encryption and decryption times exhibit an upward trend as the number of transactions increases but still our system performance is better then other compared systems. Fig 7 shows our smart contract cost in wei which we have implemented by using solidity truffle environment and ganache Ethereum simulator.

These graphs show that our blockchain system offers higher throughput and lower latency during read operations compared to write operations. The read operations are handled efficiently by the system, while the write operations introduce more latency, likely due to the complexities of data validation and recording on the blockchain and CSP. The overall results point to a blockchain solution that is effective in managing high throughput and maintaining low latency, which aligns with the operational requirements of hospital data management systems.

## 12 Comparison

Our work introduce an integrated security framework that significantly enhances the protection and accessibility of Electronic Health Records (EHRs) through the synergy of blockchain, smart contract and cloud computing technologies. This work transcends previous research by delivering a more scalable, efficient, and practical solution for healthcare data management, incorporating advanced traceability and direct access revocation mechanisms. The proposed model not only addresses current challenges in data security and privacy but also demonstrates

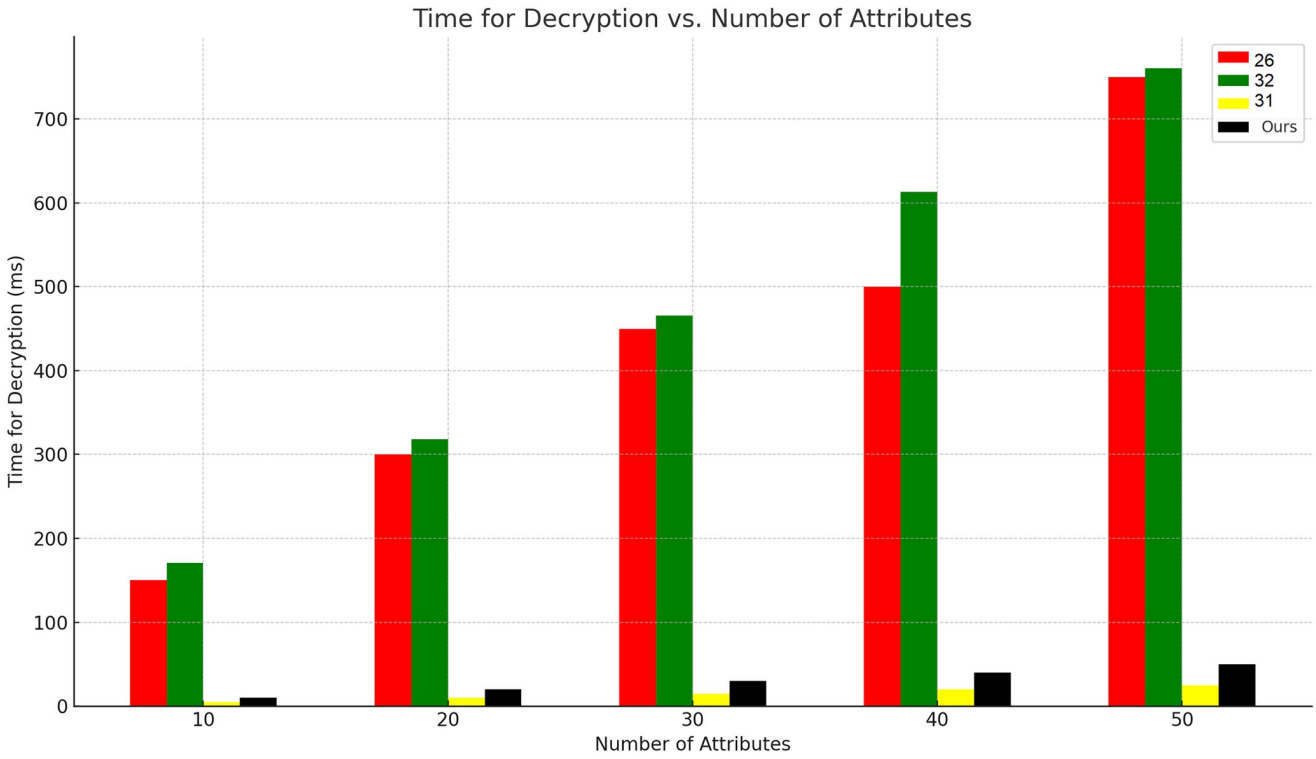


**Fig 6. Decryption performance.**

https://doi.org/10.1371/journal.pone.0307039.g006

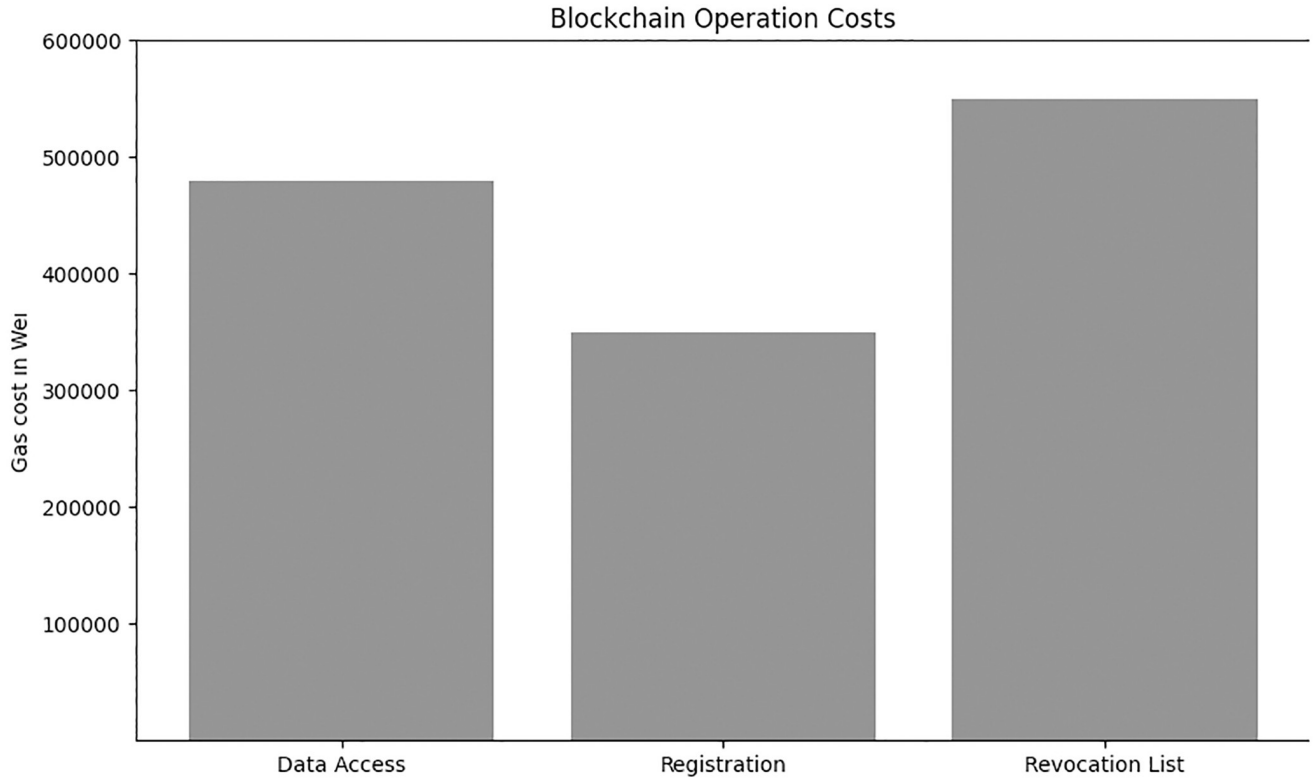


**Fig 7. Smart contract cost in wei.**

https://doi.org/10.1371/journal.pone.0307039.g007

**Table 4. Comparison of our system with others.**

| Functionalities | Our work | [31] | [32] | [26] |
|---|---|---|---|---|
| Scalability | Yes | Yes | No | Yes |
| Blockchain Utilization | Yes | No | Yes | No |
| Data Traceability | Yes | Yes | Yes | No |
| Data Auditing and Provenance | Yes | No | Yes | No |
| Identity Management | Yes | Yes | Yes | Yes |
| Immutability | Yes | No | Yes | No |
| User Authentication | Yes | Yes | Yes | Yes |

https://doi.org/10.1371/journal.pone.0307039.t004

a clear, implementable pathway towards improving healthcare information systems, marking a pivotal advancement in secure digital health records management, as shown in Table 4.

## 13 Future works

In future work, we aim to explore the integration of advanced machine learning algorithms with our blockchain-cloud-based framework to enhance the predictive analysis and personalization of healthcare services. This will involve developing AI-driven models for real-time health data analysis, leading to more accurate and timely disease diagnosis and treatment recommendations. Additionally, we plan to expand the scope of our platform to include interoperability with a wider range of electronic health record systems and medical devices, ensuring seamless data exchange across different healthcare providers and platforms. Another key area of focus will be enhancing the security features of our system by incorporating newer cryptographic techniques and exploring quantum-resistant algorithms to safeguard against evolving cyber threats. Furthermore, we intend to conduct extensive field trials to validate the efficacy of our proposed system in diverse healthcare settings, ranging from urban hospitals to remote healthcare units, thus broadening its applicability and impact.

## 14 Conclusion

It is a huge challenge to take secure storage and sharing of Medical data among different cloud-based hospital systems. We proposed a robust algorithm that integrates blockchain technology and smart contracts with cloud computing to ensure secure and authenticated access to health data. The proposed solution addresses critical concerns in the healthcare sector, including data privacy, security, and integrity, by leveraging the decentralized nature of blockchain and the scalability of cloud computing. The results demonstrate that this integrated approach not only enhances the security of sensitive health data but also ensures seamless and efficient data access for authorized users. This algorithm sets a new standard in healthcare data management, offering a promising path forward for healthcare providers and patients alike in the age of digital health information.

## Author Contributions

**Conceptualization:** Ali Shahzad.

**Data curation:** Ali Shahzad.

**Formal analysis:** Yin Zhang.

**Investigation:** Ali Shahzad.

**Methodology:** Ali Shahzad.

**Project administration:** Wenyu Chen.

**Software:** Ali Shahzad, Faizan Ahmad.

**Supervision:** Wenyu Chen.

**Validation:** Yin Zhang, Faizan Ahmad.

**Visualization:** Momina Shaheen, Faizan Ahmad.

**Writing – original draft:** Ali Shahzad.

**Writing – review & editing:** Ali Shahzad.

## References

1. Sivan R, Zukarnain ZA. Security and Privacy in Cloud-Based E-Health System. In: Symmetry. vol. 13. MDPI AG; 2021. p. 742. Available from: https://doi.org/10.3390/sym13050742.
2. Butpheng C, Yeh KH, Xiong H. Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. Symmetry. 2020; 12. https://doi.org/10.3390/sym12071191
3. Karhade AV, Schwab JH, Fiol GD, Kawamoto K. SMART on FHIR in spine: integrating clinical prediction models into electronic health records for precision medicine at the point of care. The Spine Journal. 2021; 21:1649–1651. https://doi.org/10.1016/j.spinee.2020.06.014 PMID: 32599144
4. Hossain A, Quaresma R, Rahman H. Investigating factors influencing the physicians—adoption of electronic health record (EHR) in healthcare system of Bangladesh: An empirical study. International Journal of Information Management. 2019; 44:76–87. https://doi.org/10.1016/j.ijinfomgt.2018.09.016
5. Alouffi B, Hasnain M, Alharbi A, Alosaimi W, Alyami H, Ayaz M. A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. IEEE Access. 2021; 9:57792–57807. https://doi.org/10.1109/ACCESS.2021.3073203
6. Ansari MD, Gunjan VK, Rashid E. On Security and Data Integrity Framework for Cloud Computing Using Tamper-Proofing. In: Advances in Intelligent Systems and Computing. vol. 1076. Springer; 2020. p. 1294–1305. Available from: https://doi.org/10.1007/978-981-15-7961-5_129.
7. Sailunaz K, Alhussein M, Shahiduzzaman M, Anowar F, Al Mamun KA. CMED: Cloud based Medical System Framework for Rural Health Monitoring in Developing Countries. Computers and Electrical Engineering. 2016; p. 469–481. https://doi.org/10.1016/j.compeleceng.2016.02.005
8. Cao S, Zhang G, Liu P, Zhang X, Neri F. Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Information Sciences. 2019; 485:427–440. https://doi.org/10.1016/j.ins.2019.02.038
9. Majhi M, Pal AK, Pradhan J, Miah SJ, Khan MK. Computational Intelligence Based Secure Three-Party CBIR Scheme for Medical Data for Cloud-Assisted Healthcare Applications. Multimedia Tools and Applications. 2021; 81:41545–41577. https://doi.org/10.1007/S11042-020-10483-7
10. Kanwal T, Anjum A, Malik SUR, Khan A, Khan MA. Privacy preservation of electronic health records with adversarial attacks identification in hybrid cloud. Computer Standards and Interfaces. 2021; 78:103522. https://doi.org/10.1016/j.csi.2021.103522
11. Liang Y. Identity Verification and Management of Electronic Health Records with Blockchain Technology. In: 2019 IEEE International Conference on Healthcare Informatics, ICHI 2019. IEEE; 2019. Available from: https://doi.org/10.1109/ICHI.2019.8904712.
12. Sharma P, Dutta Borah M, Namasudra S. Improving security of medical big data by using Blockchain technology. Computers and Electrical Engineering. 2021; 93:107529. https://doi.org/10.1016/j.compeleceng.2021.107529
13. Umran SM, Lu S, Abduljabbar ZA, Tang X. A Blockchain-Based Architecture for Securing Industrial IoTs Data in Electric Smart Grid. Computers, Materials and Continua. 2023; 74(3):5389–5416. https://doi.org/10.32604/cmc.2023.034331
14. Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain Blockchain Based Secure Data-sharing Framework for Industrial IoTs Smart Devices in Petroleum Industry. Internet of Things. 2023; 14:100456. https://doi.org/10.1016/j.iot.2023.100456
15. Umran SM, Lu S, Abduljabbar ZA, Tang X. Secure and Privacy-preserving Data-sharing Framework based on Blockchain Technology for Al-Najaf/Iraq Oil Refinery. In: 2022 IEEE Smartworld, Ubiquitous Intelligence and Computing, Scalable Computing and Communications, Digital Twin, Privacy Computing,

Metaverse, Autonomous and Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Metaverse); 2022. p. 2284–2292. Available from: https://ieeexplore.ieee.org/document/9876544.

16. Benil T, Jasper J. Blockchain based secure medical data outsourcing with data deduplication in cloud environment. Computer Communications. 2023; 209:1–13. https://doi.org/10.1016/J.COMCOM.2023.06.013
17. Anil K, Kamble M. Health Block: A Blockchain Based Secure Healthcare Data Storage and Retrieval System for Cloud Computing. International Journal on Recent and Innovation Trends in Computing and Communication. 2023; 11(9):96–104. https://doi.org/10.17762/IJRITCC.V11I9.8324
18. Lizama MG, Huesa J, Claudio BM. Use of Blockchain technology for the exchange and secure transmission of medical images in the cloud: Systematic Review with Bibliometric Analysis. ASEAN Journal of Science and Engineering. 2024; 4(1):71–92. https://doi.org/10.17509/AJSE.V4I1.65039
19. Albassam A, Almutairi F, Majoun N, Althukair R, Alturaiki Z, Rahman A, et al. Integration of Blockchain and Cloud Computing in Telemedicine and Healthcare. IJCSNS International Journal of Computer Science and Network Security. 2023; 23(6). https://doi.org/10.22937/IJCSNS.2023.23.6.3
20. Xu S, Zhong J, Wang L, Zhang DHS, Shao W. A privacy-preserving and efficient data sharing scheme with trust authentication based on blockchain for mHealth. CONNECTION SCIENCE. 2023. https://doi.org/10.1080/09540091.2023.2186316
21. (PDF) MITIGATING SECURITY, AND PRIVACY ISSUES IN AN ELECTRONIC HEALTH RECORD SYSTEM, USING BLOCKCHAIN;. Available from: www.researchgate.net/publication/376520222_MITIGATING_SECURITY_AND_PRIVACY_ISSUES_IN_AN_ELECTRONIC_HEALTH_RECORD_SYSTEM_USING_BLOCKCHAIN.
22. Insaf BoumezbeurKarim ZZ. Improving Privacy-preserving Healthcare Data Sharing in a Cloud Environment Using Hybrid Encryption. Acta Informatica Pragensia. 2022. https://doi.org/10.18267/j.aip.182
23. Taherdoost H. Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives. Sci. 2023; 5(4). https://doi.org/10.3390/SCI5040041
24. Upadrista V, Nazir S, Tianfield H. Secure data sharing with blockchain for remote health monitoring applications: a review. Journal of Reliable Intelligent Environments. 2023; 9(3):349–368. https://doi.org/10.1007/S40860-023-00204-W/FIGURES/5 PMID: 37359293
25. Hebballi AK, Bharath J, Agarwal A, Challa M. Securing Medical Data Records using Blockchain in a Cloud Computing Environment. 2023 3rd International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies, ICAECT 2023. 2023.
26. Zhang X, Du W, Moshayedi AJ. A traceable and revocable multi-authority attribute-based access control scheme for mineral industry data secure storage in blockchain. Journal of Supercomputing. 2023; 79(13):14743–14779. https://doi.org/10.1007/S11227-023-05222-2/TABLES/8
27. Liu Z, Wang F, Chen K, Tang F. A New User Revocable Ciphertext-Policy Attribute-Based Encryption with Ciphertext Update. Security and Communication Networks. 2020; 2020. https://doi.org/10.1155/2020/8856592
28. Cui H, Deng RH, Lai J, Yi X, Nepal S. An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited. Computer Networks. 2018; 133:157–165. https://doi.org/10.1016/J.COMNET.2018.01.034
29. Naruse T, Mohri M, Shiraishi Y. Attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating. Lecture Notes in Electrical Engineering. 2014; 276 LNEE:119–125. https://doi.org/10.1007/978-3-642-40861-8_18/COVER
30. Aqeel H, Ali ST. Directly revocable Attribute Based Encryption scheme under Ciphertext-policy. 2017 International Conference on Computer, Communications and Electronics, COMPTELIX 2017. 2017; p. 383–387.
31. Wang S, Guo K, Zhang Y. Traceable ciphertext-policy attribute-based encryption scheme with attribute level user revocation for cloud storage. PLOS ONE. 2018; 13(9):e0203225. https://doi.org/10.1371/JOURNAL.PONE.0203225 PMID: 30212473
32. Liu Z, Duan S, Zhou P, Wang B. Traceable-then-revocable ciphertext-policy attribute-based encryption scheme. Future Generation Computer Systems. 2019; 93:903–913. https://doi.org/10.1016/J.FUTURE.2017.09.045
33. Cheng Y, Wang ZY, Ma J, Wu JJ, Mei SZ, Ren JC. Efficient revocation in ciphertext-policy attribute-based encryption based cryptographic cloud storage. Journal of Zhejiang University: Science C. 2013; 14(2):85–97. https://doi.org/10.1631/JZUS.C1200240/METRICS
34. Nyangaresi VO, Abduljabbar ZA, Sibahee MAA, Ibrahim A, Hussain MA, Hussien ZA, et al. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. In: 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET); 2021. p. 1–6. Available from: https://ieeexplore.ieee.org/document/9698744.

35. Nyangaresi VO, Ma J, Abduljabbar ZA, Sibahee MAA. Verifiable Security and Privacy Provisioning Protocol for High Reliability in Smart Healthcare Communication Environment. In: 2022 4th Global Power, Energy and Communication Conference (GPECOM); 2022. p. 1–6. Available from: https://ieeexplore.ieee.org/document/9815685.

36. Nyangaresi VO, Sibahee MAA, Abduljabbar ZA, Ma J, Khalefa MS. Biometric-Based Packet Validation Scheme for Body Area Network Smart Healthcare Devices. 2022; p. 726–731. https://doi.org/10.1109/MELECON53508.2022.9842900

37. Umran SM, Lu S, Abduljabbar ZA, Zhu J, Wu J. Secure Data of Industrial Internet of Things in a Cement Factory Based on a Blockchain Technology. Applied Sciences. 2021; 11(14):6376. https://doi.org/10.3390/app11146376

38. Amazon Web Services. What is Blockchain?—Blockchaining Explained; 2023. Available from: https://aws.amazon.com/what-is/blockchain/.

39. Amazon Web Services. What is Cloud Computing?; 2023. Available from: https://aws.amazon.com/what-is-cloud-computing/.

40. Bethencourt J, Sahai A, Waters B. Ciphertext-Policy Attribute-Based Encryption with Anonymous Access Policy. IEEE Symposium on Security and Privacy. 2007; p. 321–334.

41. Taherdoost H. Smart Contracts in Blockchain Technology: A Critical Review. Information. 2023; 14 (2):117. https://doi.org/10.3390/info14020117