ITM Web of Conferences 79, 01019 (2025) https://doi.org/10.1051/itmconf/20257901019
*KEIS-2025*

# Proposed Framework for Blockchain based Approach to Secure Healthcare Data in Cloud Computing

*Guruprasad*[1,2*], and *Nagesh.* H R[3]

[1]Visvesvaraya Technological University, Belagavi, India
[2]NMAM Institute of Technology (NMAMIT), Nitte (Deemed to be University), Nitte, Karkala, India
[3]Canara Engineering College, Bantwal Visvesvaraya Technological University, Belagavi, India

**Abstract.** The increasing reliance on cloud computing within the healthcare domain has generated considerable concerns regarding data privacy, security, and compliance with regulatory standards. Blockchain technology has emerged as a promising solution to address these challenges by enabling decentralized, tamper-proof, and transparent data management. This paper offers a detailed examination of blockchain-based methodologies for the protection of healthcare data within cloud infrastructures. It evaluates cutting-edge techniques in three fundamental dimensions: access control, encryption strategies, and performance evaluation. Through a meticulous review and categorization of extant frameworks, the research elucidates prevailing deficiencies such as the absence of interoperability, challenges related to scalability, and computational burdens. To address these limitations, an innovative blockchain-based architecture is proposed, which incorporates smart contracts and attribute-based encryption. The suggested system guarantees secure, auditable, and patient-centred sharing of healthcare data while simultaneously improving system efficiency. The proposed framework decreases reliance on centralized authorities while improving data integrity, access transparency, and patient-centric control. In addition, integrating off-chain cloud storage enhances scalability in contrast to current blockchain-only solutions. This study illustrates the transformative capacity of blockchain in revolutionizing healthcare data management by ensuring integrity, privacy, and accessibility throughout distributed systems.

## 1 Introduction

The rapid evolution of digital healthcare systems has led to unprecedented advancements in clinical efficiency, data interoperability, and personalized treatment plans. Cloud computing is one of the main technical enablers that has revolutionized the management, access, and storage of healthcare data. By providing elastic storage, scalable computational power, and ubiquitous availability, cloud computing enables healthcare providers to store vast amounts of Electronic Health Records (EHRs), support telemedicine, and improve patient engagement. Traditional security measures including encryption, authentication protocols, and access controls remain fundamental but often prove insufficient against emerging threats such as insider attacks, data manipulation, and unauthorized third-party access, especially in centralized cloud infrastructures [1] [2]. A major limitation of centralized architectures is their inherent vulnerabilities, which can compromise the availability and integrity of patient data across distributed healthcare networks. This has driven interest in decentralized solutions like blockchain, which offer a robust alternative for securing healthcare data in the cloud.

Originally developed for cryptocurrency transactions, blockchain has evolved into a powerful tool for trustless data sharing, decentralized authentication, and tamper-proof recordkeeping [3] [4]. Its application in healthcare care is driven by its ability to ensure the provenance of the data, resist tampering, and provide auditability through cryptographic techniques and consensus mechanisms [6]. Unlike traditional databases, blockchain operates on a distributed ledger system across multiple nodes, enhancing redundancy and fault tolerance. This decentralization in healthcare enables patient-centric governance by addressing important issues with data ownership, access rights, and consent management [9].

Additionally, the incorporation of smart contracts streamlines administrative and security procedures, including data-sharing agreements, compliance audits, and patient consent management [10]. These self-executing scripts enforce predefined rules without human intervention, reducing reliance on intermediaries and improving transparency. To balance security and scalability, researchers are exploring hybrid models that combine off-chain cloud storage with on-chain authentication, leveraging lightweight blockchain architectures and interoperable frameworks like IOTA and Hyperledger Fabric. Despite its promise, blockchain adoption in cloud healthcare environments faces challenges related to transaction latency, storage overhead, and interoperability with legacy systems.

* Corresponding author: pguru88@gmail.com

Scalability remains a major bottleneck, especially when dealing with high throughput healthcare applications such as imaging systems or genomic databases. Efforts are underway to address these issues through innovations like sharding, off-chain computation, and consensus optimization techniques [11].

This study offers a thorough analysis of blockchain-based methods for protecting medical records in cloud computing environments. Critically analyzes the existing frameworks, architectural paradigms, and cryptographic mechanisms that underpin these solutions. By comparing blockchain implementations across different use cases, we identify design trade-offs, performance bottlenecks, and security implications.

Following the introduction, the paper is divided into many main sections. Section 2 provides a detailed overview of relevant research on blockchain-based healthcare data security, categorizing them as access control, encryption techniques, and performance evaluation, with a summary table emphasizing key contributions in each area. Section 3 emphasizes important research gaps within these categories, highlighting concerns such as lack of interoperability, processing overhead, lack of defined benchmarks, and limited real-world implementation, which are backed by a tabular overview. Section 4 describes the proposed blockchain-based architectural framework, including its layered design of data collecting, encryption, blockchain, smart contracts, cloud storage, decryption, and end-user interaction. The results and implications of the suggested system are examined in Section 5, which also evaluates its advantages and disadvantages in terms of handling security, privacy, and performance issues. Finally, Section 6 concludes the study, summarizing its contributions and describing future research directions.

## 2 Related Works

Arunkumar et al [1]. proposes a blockchain-based decentralized cloud medical system designed to address privacy and security challenges in the management of electronic health records (EHRs). The system employs the AES 256 GCM encryption algorithm to ensure secure data exchanges, while access restrictions are implemented using Ethereum-based smart contracts written in Solidity. This framework enhances interoperability, traceability, and patient anonymity, critical for secure healthcare data management. In comparison to traditional approaches, the system performs better in encrypting and handling healthcare data by utilizing a lightweight encryption methodology. The decentralized design of the system offers effective protection of EHRs in cloud environments, reducing the danger of illegal access. Overall, the suggested methodology enhances security, efficiency, and patient-centric data management.

Azath [2] tackles privacy and security challenges in cloud-based healthcare systems by proposing the Secure and Robust Healthcare-Based Blockchain (SRHB) framework. This approach leverages blockchain technology to safeguard patient privacy by generating unique blocks for each medical record and enforcing strict data segregation. To strengthen data protection, the SRHB method uses attribute-based encryption (ABE), ensuring secure data transmission while maintaining integrity and confidentiality. The framework provides a dependable method to protect sensitive healthcare data by successfully reducing the risks related to content privacy and safe data translation. Nevertheless, the study recognizes implementation complexities, particularly concerning privacy compatibility and technical obstacles. The SRHB approach represents a significant advancement in improving data security in cloud-based healthcare systems in spite of these obstacles.

Roshan et al. [3] propose a multilayer blockchain-based framework designed to secure healthcare data in cloud environments by leveraging a decentralized peer-to-peer network, ensuring transparency and trust. This approach enables the secure and efficient management of Electronic Health Records (EHRs) by maintaining an immutable history of transactions and reducing reliance on intermediaries in healthcare data processes. The framework strengthens the security and reliability of EHR transactions, overcoming limitations of conventional healthcare systems while enhancing the accuracy of medical diagnoses and research. By adopting a decentralized architecture, the blockchain-based system ensures resilient data management, fostering transparency and trust among stakeholders. The study underscores blockchain's transformative potential for healthcare data processing, even as it acknowledges the challenges of large-scale implementation.

Kuster Bowles et al [4]. introduce the Serums Smart Health Centre System (SHCS), a blockchain-based healthcare platform made to guarantee safe and customized data exchange in cloud settings. The platform takes a patient-centric approach to data management and uses smart contracts to provide granular access control, guaranteeing adherence to GDPR and other international regulations. It facilitates secure and recorded access to medical records, allowing patients to define and manage access rules for their data. The system emphasizes structured access control, enhancing both security and privacy in healthcare data sharing. Future development plans include integrating a user-friendly interface and assessing the efficiency of its computational structures. Overall, the SHCS framework addresses critical challenges in healthcare data sharing while prioritizing transparency and patient autonomy.

Hariharan et al. [5] propose an innovative blockchain-based framework that employs a keyless signature infrastructure to strengthen data integrity, authenticity for cloud-based electronic health records (EHRs). Their approach significantly enhances security measures by ensuring both confidentiality and reliable authentication of digital signatures, while simultaneously establishing a decentralized architecture that improves accessibility to medical records and healthcare outcomes. The study demonstrates substantial performance improvements, with the proposed system achieving a 55% reduction in processing times and a 25% decrease in storage requirements compared to conventional EHR management methods. The authors critically examine the vulnerabilities inherent in centralized storage systems, particularly their susceptibility to persistent access threats and cyberattacks. By implementing blockchain technology, the solution presents a more efficient and cost-effective alternative for managing cloud-based medical records while rigorously maintaining data confidentiality and integrity. This research underscores blockchain's transformative potential in optimizing both security and operational efficiency within healthcare data management systems.

M. Wang, H. Zhang et al [6]. provide a three-tiered blockchain-based architecture for safe healthcare data management that enhances privacy and data integrity. The system stores patient data in blocks and uses smart contracts for access control to ensure safe storage and protect privacy from both internal and external threats. The technology offers a decentralized architecture that improves data privacy by addressing issues like inadequate data reliability and unregulated data flow in telemedicine. Additionally, a machine learning method for disease prediction is integrated in the article, allowing the system to predict the future states of patients. This blockchain-based approach improves the security of telemedicine data while lowering the dangers of centralized data administration, such as single points of failure. The proposed approach effectively manages medical data and enhances disease prediction capabilities, highlighting the capabilities of blockchain within medical infrastructure.

Shamsabadi, Chehelcheshmeh, and Alipour [7] suggest a new identity-based encryption (IBE) solution that uses blockchain technology to improve access control and data integrity for safe medical data transmission in cloud-based healthcare systems. Their approach employs bilinear pairings within the IBE framework to ensure medical data confidentiality while implementing challenge-response protocols for precise user authentication. The synergistic combination of IBE and blockchain technology effectively mitigates risks associated with healthcare data confidentiality and integrity during sharing processes. The proposed solution demonstrates superior efficiency compared to existing methods, significantly reducing computational overhead for cloud-based implementations. The framework establishes a robust mechanism for secure sharing of medical records by enforcing strict access control and maintaining data privacy. This study highlights the powerful impact of combining cryptographic methods with blockchain technology to strengthen the security and confidentiality of healthcare data systems.

Thasni and Narayamparambil [8] proposed using blockchain technology to strengthen the security of medical data kept on cloud servers, guaranteeing its privacy, integrity, and protection against user traceability. The system combines decentralized storage, smart contracts, and cryptographic hashing to protect patient records from unauthorized access and modifications. It uses Base64 encoding, the AES algorithm for encryption, and SHA-256 for blockchain implementation, ensuring the confidentiality of health data. While the system improves security, it requires the server to remain live at all times and involves dividing messages into 512 input squares, which increases processing time. The proposed approach effectively integrates blockchain with encryption techniques to provide a secure solution for cloud-based healthcare data management. This framework helps safeguard patient information from potential threats while maintaining privacy and data integrity in cloud storage.

Sun et al. [9] provide a blockchain-based secure medical data storage solution that uses Attribute-Based Access Control (ABAC) and Hyperledger Fabric which provides dynamic access control and tamper-proof storage. The approach addresses the challenges of keeping massive amounts of healthcare data by lowering the storage load on the blockchain using the Inter Planetary File approach (IPFS). By optimizing access management, the suggested approach improves efficiency and security in contrast to current models, which frequently lack fine-grained access control. Medical data storage is made more flexible and private through the use of ABAC and smart contract design, which also reduces the possibility of privacy leaks. This method offers high throughput for accessing medical data while ensuring the integrity and safe archiving of medical records. The study highlights the advantages of combining blockchain technology with IPFS for healthcare data management, providing a scalable method that ensures privacy-preserving, efficient, and secure medical record storage.

Amna et al. [10] Introduce a blockchain-driven architecture aimed at strengthening the confidentiality and protection of electronic health records within cloud-based systems. Proposed system implements a multi-layered security architecture combining the Secure Hash Algorithm (SHA-256) for data integrity, Proof of Stake (PoS) consensus mechanism for network validation, and Elliptic Curve Digital Signature Algorithm (ECDSA) for robust authentication. This decentralized approach effectively mitigates vulnerabilities inherent in centralized EHR systems, particularly addressing critical concerns regarding patient privacy violations and unauthorized data access. Beyond secure cloud storage, the framework enables controlled data sharing among authorized healthcare providers while maintaining protection against potential breaches. The solution demonstrates significant advantages over conventional systems by ensuring regulatory compliance while simultaneously improving data protection measures. This research highlights blockchain's transformative potential in healthcare informatics, offering a decentralized paradigm that combines security, transparency, and efficiency for medical record management.

Md. Mainuddin et al. [11] introduce MedVault Nexus, an innovative blockchain-powered architecture designed to protect and distribute medical records securely through the Inter Planetary File System (IPFS). This hybrid architecture addresses critical security and privacy challenges in healthcare informatics by leveraging the complementary strengths of distributed ledger technology and decentralized file storage. The system implements robust cryptographic protections, utilizing both AES and RSA algorithms to ensure end-to-end data confidentiality and integrity while preventing unauthorized access or tampering with sensitive health records. Beyond its security advantages, MedVault Nexus demonstrates significant operational improvements over conventional healthcare data systems, offering enhanced efficiency and reduced administrative costs. The framework facilitates secure, permissioned data sharing among authorized medical professionals while maintaining strict privacy controls. This study highlights how combining blockchain with IPFS can revolutionize healthcare by offering a secure and scalable framework for advanced medical data management.

Hebballi et al [17]. present a decentralized paradigm for safe medical data sharing that uses blockchain technology, RSA encryption, IPFS, and Proxy Re-encryption (PRE). This model addresses the lack of comprehensive solutions that integrate decentralization with robust privacy measures in current healthcare systems. By utilizing cryptographic methods such as RSA encryption and SHA-256 hashing, along with IPFS for distributed storage, the model enhances the accessibility, privacy, and security of medical data, removing the need for third-party intermediaries. Despite its advantages, the approach relies heavily on complex cryptographic techniques, which present challenges in scalability and integration in large scale systems. However, the use of blockchain and advanced cryptographic methods offers a robust solution to secure and decentralized medical data sharing, which benefits patients, healthcare providers and insurance companies.

Ussatova et al [12]. offer a two-step authentication technique that uses blockchain technology and cloud computing to improve healthcare data security. The technology fixes weaknesses, especially those caused by human mistake, by combining cloud encryption keys with biometric authentication to guarantee data integrity and stop unwanted access. The study emphasizes the growing necessity of healthcare information security in light of mounting cyber-attacks that risk medical data integrity and patient privacy. While blockchain offers a decentralized authentication approach, the authors note that its industrial implementation remains limited. Additionally, human factors, such as the leakage of medical personnel credentials, contribute to security risks. The proposed two-step scheme, using biometric authentication and cloud-based digital signatures, delivers a reliable approach to securing healthcare data and preserving its confidentiality

Shrabani et al. [13] propose a blockchain-based privacy preservation framework for the Internet of Medical Things (IoMT) designed to ensure secure transmission of medical data. Integrating blockchain within a fog-cloud computing framework enhances the security, integrity, and privacy of Electronic Health Records (EHRs). The system adopts a zero-trust approach for strong data protection, while utilizing Quad Merkle trees and zero-knowledge proof (ZKP) cryptography to support dependable auditing and maintain data integrity. The framework effectively mitigates critical challenges in healthcare data exchange, such as unauthorized access and tampering, through these advanced cryptographic mechanisms. In addition, it improves computational efficiency, facilitates seamless data management, and maintains high standards of data fidelity and privacy. This innovative approach demonstrates considerable promise in advancing secure and trustworthy medical data management within healthcare systems.

Varshitha [14] introduces a blockchain-driven approach for safeguarding healthcare data in cloud environments by integrating attribute-based access control (ABAC) with Amazon S3 cloud storage services. The proposed solution ensures dynamic access control, enabling authorized access while safeguarding sensitive medical information. It incorporates blockchain technology to provide immutable data storage, enhancing the reliability and security of healthcare records. The system uses ABAC to enable fine-grained access control, guaranteeing that only authorized parties can exchange or edit data. Additionally, the integration with AWS S3 enhances scalability and secure data storage capabilities. This novel solution addresses critical issues in healthcare data security, providing a strong foundation to preserve privacy and facilitate efficient data sharing. The study claims that the system has the power to completely change the management of secure healthcare data in the cloud.

Mahalingam et al [15]. propose a blockchain-based approach within a cloud framework to secure electronic medical records, focusing on enhancing data privacy, integrity, and confidentiality. The system disperses and encrypts medical records to bolster security and mitigate risks associated with data breaches. Lightweight access controls are implemented to ensure efficient and secure access for healthcare stakeholders while addressing latency issues. By leveraging blockchain technology, the framework provides a decentralized solution that strengthens network security and protects sensitive healthcare data. Additionally, it facilitates secure data transmission through portable devices, enhancing accessibility without compromising security. This innovative method provides a strong way to protect medical records while enhancing the general effectiveness and dependability of healthcare data management systems.

Shahzad, Ali, et al. [16] suggest a blockchain-enabled architecture that utilizes smart contracts to streamline access control and manage cryptographic keys, thereby improving the security and performance of cloud-hosted healthcare data systems. The system leverages blockchain's decentralized architecture to ensure secure auditing, maintain data integrity, and streamline electronic health record (EHR) management. A key innovation is the implementation of Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Implements fine-grained access control mechanisms to effectively mitigate critical privacy and security concerns inherent in healthcare-oriented cloud computing environments. While demonstrating significant improvements in securing health data exchange through the synergistic combination of blockchain's decentralization and cloud scalability, the study also addresses implementation challenges including data standardization, interoperability issues, computational overhead, and scalability constraints. This study proposes an effective framework for managing electronic health records securely and efficiently within modern healthcare infrastructures, ensuring an optimal balance between data confidentiality and operational performance.

Murugeswari et al. [18] explore how blockchain technology can improve healthcare data security by distributing patient records among a dispersed network of nodes in a decentralized manner. This innovative approach significantly enhances data confidentiality and accuracy while safeguarding sensitive medical records through blockchain's immutable ledger properties, which prevent unauthorized access and tampering. The research demonstrates how blockchain technology enables transformative improvements in the management and sharing of secure patient data, leading to more efficient healthcare operations. The decentralized framework not only strengthens the security of medical records, but also fosters greater trust in data management systems. By addressing critical challenges in healthcare data protection, this solution provides a robust mechanism for maintaining data integrity, reliability, and security while handling sensitive patient information.

Table 1 provides a summary of the related work in blockchain based health care systems.

**Table 1.** Categorization of related work in blockchain-based healthcare systems.

| Category | Authors | Summary of Contributions |
|---|---|---|
| Access Control | Arunkumar et al. [1]<br>Kuster Bowles et al. [4]<br>Wang et al. [6]<br>Sun et al. [9]<br>Shahzad et al. [16]<br>Varshitha [14]<br>Shamsabadi et al. [7] | Ethereum-based access control via Solidity smart contracts.<br>GDPR-compliant, patient-centric access using smart contracts.<br>Tiered smart contract access for enhanced EHR privacy.<br>ABAC and IPFS for dynamic, fine-grained access control.<br>CP-ABE and smart contracts for automated access control.<br>ABAC combined with AWS S3 for dynamic control and scalability.<br>Identity-Based Encryption for access verification and user-specific permissions.<br>Two-step biometric and key-based access control scheme. |
| Encryption Mechanisms | Arunkumar et al. [1]<br>Azath [2]<br>Thasni et al. [8]<br>Amna et al. [10]<br>Mainuddin et al. [11]<br>Hebballi et al. [17]<br>Shrabani et al. [12] | Utilizes AES-256 GCM for secure EHR data exchange.<br>Attribute-Based Encryption ensures confidentiality in cloud transmission.<br>Blockchain with encryption to ensure data sensitivity and trust.<br>Integrates AES and SHA-256 with blockchain for secure cloud storage.<br>ECDSA, SHA-256, and PoS for data integrity and authentication.<br>AES and RSA encryption combined with IPFS for secure sharing.<br>Proxy Re-Encryption (PRE), RSA, and SHA-256 for robust security<br>. |
| Performance Evaluation | Roshan et al. [3]<br><br>Hariharan et al. [5]<br><br>Sun et al. [9]<br><br>Shahzad, Ali, et al. [16]<br>Murugeswari et al. [18]<br><br>Mahalingam et al. [15] | Analyzes trust, immutability, and performance in multilayer EHR architecture.<br>Proposes tools and metrics for evaluating system efficiency and reliability.<br>Achieves 55% reduction in processing time and 25% reduction in storage cost.<br>Demonstrates high throughput and optimized data access using ABAC and IPFS.<br>System performance and interoperability evaluation in cloud-based EHR.<br>Evaluates scalability, accuracy, and privacy in decentralized EHR data sharing.<br>Reduces latency and enables secure, real-time EHR access.<br>Assesses transparency and auditability in cloud-based blockchain storage. |

## 3 Research Gaps

Despite extensive research on blockchain-based healthcare data management, a detailed analysis of existing literature reveals significant gaps in three major areas: access control, encryption mechanisms, and performance evaluation.

In the area of access control, interoperability issues arise from the heterogeneity of models like Identity-Based Encryption (IBE), Ciphertext-Policy Attribute-Based Encryption (CPABE), and Attribute-Based Access Control (ABAC). Most approaches lack standardization, hindering seamless integration with legacy healthcare systems. Furthermore, limited focus is given to the scalability and usability of access control mechanisms, especially in dynamic and emergency healthcare scenarios. Real-time revocation of access rights is insufficiently addressed, and although some solutions aim to comply with regulations such as GDPR and HIPAA, they often lack enforceable, auditable compliance frameworks.

For encryption mechanisms, the adoption of computationally intensive cryptographic methods, including RSA, Proxy Re-Encryption (PRE) and Zero-Knowledge Proofs (ZKPs), introduces performance bottlenecks, particularly for devices of the Internet of Medical Things (IoMT). Current solutions do not account for post-quantum cryptographic resilience, leaving long-term data security vulnerable. In addition, scalable and secure key management—covering key generation, distribution, and revocation—remains an open issue in most proposed architectures.

Regarding performance evaluation, a lack of standardized benchmarks makes it difficult to compare different frameworks fairly. Current assessment methods are predominantly performed in controlled, simulated settings using constrained datasets, which do not adequately reflect the intricate nature of actual healthcare environments. Moreover, the trade-offs between security features and system performance, such as increased latency or storage costs, are rarely quantified. Real-world deployment and validation are minimal, with most systems remaining at the conceptual or prototype stage.

These research gaps emphasize the need for unified, scalable and regulatory compliant blockchain solutions that ensure secure, efficient, and patient-centric healthcare data management. Table 2 provides a summary of the key research gaps identified in the reviewed literature.

**Table 2.** Research gaps identified from categorized related works.

| Category | Authors | Summary of Contributions |
|---|---|---|
| Access Control | Lack of Interoperability in Access Policies<br>Usability and Scalability Challenges<br>Inadequate Real-Time Revocation Mechanisms<br>Regulatory Compliance Gaps | Access control models (ABAC, CP-ABE, IBE) vary widely and lack standardization, limiting system interoperability.<br>Complex smart contract designs and biometric systems are difficult to scale and not user-friendly for non-technical users.<br>Few solutions support dynamic revocation of access rights, critical in emergency and evolving clinical scenarios.<br>Most systems mention compliance (e.g., GDPR, HIPAA) but lack enforceable or auditable mechanisms for verification. |
| Encryption Mechanisms | Heavy Cryptographic Overhead<br>Limited Support for Post-Quantum Security<br>Lack of Integration with Lightweight Devices<br>Key Management Complexity | RSA, ZKP, and PRE incur high computation cost, making them unsuitable for low-power healthcare devices.<br>No encryption models address potential threats from quantum computing on current cryptographic standards.<br>Encryption algorithms are not optimized for use in IoMT or mobile devices with limited resources.<br>Few frameworks provide scalable and secure encryption key management, including key distribution and rotation. |
| Performance Evaluation | Lack of Unified Performance Benchmarks<br>Limited Long-Term Scalability Testing<br>Absence of Security-Performance Trade-off Analysis<br>Real-World Deployment and Evaluation | Diverse and inconsistent performance metrics prevent fair comparisons across systems and frameworks.<br>Most systems are tested with small datasets and short durations, lacking real-world scalability validation.<br>Security features often increase latency/storage overheads, but few works quantify these trade-offs.<br>Majority of works are prototypes or simulations without deployment in real healthcare infrastructures. |

## 4 Proposed Method

Figure 1 presents the proposed blockchain-based architectural framework designed to enhance healthcare data integrity, security, and privacy in cloud computing environments. By integrating distributed ledger technology with secure cloud storage and advanced cryptographic methods, the system establishes a robust, scalable platform for the sharing of trusted data between patients, healthcare providers and medical institutions.

### 4.1 Data Collection Layer

The system starts by gathering health information from many sources, such as patients, hospitals, and medical specialists. Electronic health records (EHRs), prescriptions, diagnostic reports, and treatment histories are examples of typical data that are sent for safe processing. Each data packet is tagged with metadata (e.g., timestamp, source ID) to support traceability and audit logging.

### 4.2 Encryption Layer

To safeguard confidentiality, the data is passed through an encryption mechanism. A cryptographic hash is also generated to preserve integrity and detect any tampering. The resulting encrypted and hashed data is then forwarded to the blockchain network and cloud storage. AES-256-GCM is used to encrypt collected data, guaranteeing its integrity and secrecy. For the purpose of detecting tampering, a SHA-256 hash is generated for every record. The CP-ABE technique, which is used to manage the encryption keys, enables fine-grained access control according to user attributes (e.g., role, department, clearance level).

### 4.3 Blockchain Layer

The blockchain serves as a secure ledger comprising a series of blocks (B1, B2, ..., Bn), each containing metadata and cryptographic hashes that link them sequentially. The blockchain stores data transaction references in an immutable and decentralized manner, providing traceability and trust. The actual medical records are not stored directly on-chain but are linked via hash pointers. The actual data is stored off-chain in a secure cloud repository, referenced via hash pointers. Each block contains: Transaction ID, Timestamp, Encrypted hash pointer, Access policy ID.

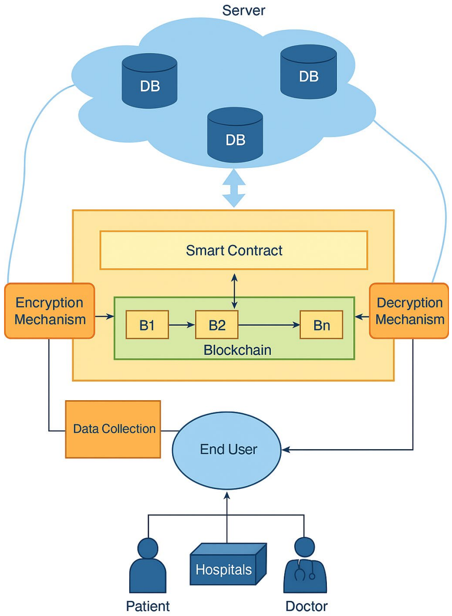


**Fig. 1.** Proposed architecture diagram.

### 4.4 Smart Contract Module

Smart contracts act as autonomous agents enforcing access policies on the blockchain. These programmable scripts define rules for data access and authentication, ensuring that only authorized users can retrieve or manipulate data. This eliminates reliance on centralized authorities. These tools, written in Solidity for Ethereum or Chaincode for Hyperledger, validate user attributes against CP-ABE regulations. Log access events to provide auditability.

### 4.5 Cloud Storage Layer

The actual encrypted data is kept in a distributed cloud storage system to allow scalability and to manage massive amounts of healthcare data. This off-chain storage enhances the blockchain by providing great performance and availability while maintaining encryption security.

### 4.6 Decryption Layer

Authorized users retrieve data based on smart contract validation. If access is granted, the corresponding encrypted files are fetched from cloud storage and decrypted using a secure decryption mechanism, thereby ensuring controlled data access.

### 4.7 End User Interaction

The architecture supports various end users, including patients, healthcare providers, and hospitals. These users interact with the system through secure interfaces, where all actions, such as data requests or uploads, are governed by the smart contracts of the blockchain.

### 4.8 Advantages of the Proposed Model

- Data Security: Encryption and immutability of the blockchain ensure protection against unauthorized access and manipulation.
- Access Control: Smart contracts provide automated enforcement of access policies, preserving data privacy.
- Transparency: All transactions are logged on the blockchain, ensuring auditability.
- Scalability: Cloud storage enables efficient handling of large datasets while offloading the blockchain.

## 5 Results and Discussion

The proposed blockchain-based architecture effectively addresses key challenges in securing healthcare data within cloud environments. The solution guarantees enhanced data accessibility, privacy, and integrity by fusing cutting-edge encryption techniques with decentralized blockchain control. Reliance on centralized authorities is decreased and security is improved by using smart contracts to automate permission management and enforce preset access policies. By providing restricted and transparent access to electronic health records (EHRs), this architecture encourages a patient-centric approach to healthcare data management.

The system has significant drawbacks in spite of its advantages. Its compatibility with different healthcare infrastructures is affected by the lack of standardized access control models such as attribute-based access control (ABAC) or ciphertext policy attribute-based encryption (CP-ABE). Furthermore, there are still gaps in the methods for instantly rescinding access permissions, which are crucial in emergency situations. The features related to regulatory compliance, including audit ready tracking for HIPAA or GDPR compliance, also need to be improved to more fully satisfy legal and industry requirements. The metric-based comparison of the proposed and existing system is shown in Table 3.

From a performance perspective, the use of off-chain cloud storage and IPFS helps address scalability limitations typically associated with blockchain systems. However, the architecture has not been tested on a formal basis in real world environments. Essential performance metrics such as latency, throughput, and energy efficiency have not yet been explored. Furthermore, potential trade-offs between enhanced security and system overhead need to be quantified. Extensive simulation and deployment in healthcare settings are necessary to validate the scalability, resilience, and practicality of the architecture for operational use.

**Table 3.** Metric-based comparison of proposed framework with existing approaches.

| Work / Framework | Security Mechanism | Processing Time | Storage Cost | Scalability | Throughput | Remarks |
|---|---|---|---|---|---|---|
| Hariharan et al. [7] | Keyless Signature + Blockchain | ↓ 55% | ↓ 25% | Medium | Moderate | Strong integrity, reduced latency |
| Roshan et al. [3] | Multilayer Blockchain | Moderate | High | Low | Moderate | High immutability, limited scalability |
| Mainuddin et al. [13] | Blockchain+ IPFS+AES/RSA | Moderate | Low | High | High | Strong privacy, improved storage |
| Proposed Framework | CP-ABE + AES-256-GCM+ Smart Contracts | To be evaluated | Low (cloud off-chain) | To be High | Expected High | Improves patient centric access, enhances auditability |

## 6 Conclusion and Future Scope

This study provides an in-depth review and architectural proposal for blockchain-based healthcare data security in cloud environments. It underscores the potential of blockchain to achieve decentralization, immutability, and transparent access management. Through critical analysis, the study identifies and addresses limitations in the current literature, particularly access control, encryption scalability, and performance evaluation.

The proposed framework leverages smart contracts, encryption, and distributed storage to improve data integrity, privacy, and patient autonomy. While it offers a substantial advancement over conventional systems, gaps remain in regulatory compliance, post-quantum cryptographic preparedness, and standardized performance assessments.

Future Scope

- Integration with Standardized Access Models: Incorporating CP-ABE or ABAC to enhance policy interoperability across diverse health systems.
- Real-world Deployment: Conducting pilot implementations in healthcare institutions for empirical validation.
- Benchmark Testing: Developing standardized testbeds to evaluate system latency, throughput, and fault tolerance.

With these advancements, blockchain can serve as the cornerstone of next-generation, secure, and patient-centric healthcare data systems.

## References

1. B. Arunkumar, G. Kousalya, Blockchain-based decentralized and secure lightweight e-health system for electronic health records, in Proceedings of the 5th International Symposium on Technology for Asia (ISTA), Springer, May 06 (2020) 273-289
2. M. Azath, Healthcare services monitoring in cloud using secure and robust healthcare-based blockchain (SRHB) approach. Mobile Netw. Appl. **25**, 1330-1337 (2020). https://doi.org/10.1007/s11036-020-01551-1
3. J. Roshan, H. Kaur, M.A. Alam, A blockchain-based multi-layer infrastructure for securing healthcare data on cloud, In Congress on Intelligent Systems, Springer, Singapore, June 02 (2021), 383-395
4. J.K. Bowles, T. Webber, E. Blackledge, A.F. Vermeulen, A blockchain-based healthcare platform for secure personalised data sharing. Stud. Health Technol. Inform. **275**, 136-140 (2021). https://doi.org/10.3233/shti210150
5. U. Hariharan, V. Dhanakoti, K. Rajkumar, J. Jeyavel, Safeguarding e-healthcare documents utilizing advanced keyless signature infrastructure blockchain within the cloud, in Proceedings of the International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE, Pune, India, April 22 (2022), 1-6
6. M. Wang, H. Zhang, H. Wu, G. Li, K. Gai, Blockchain-based secure medical data management and disease prediction, in Proceedings of the ACM Symposium on Applied Computing (SAC), Pisa, Italy, May 30 (2022), 71-82
7. F.A. Shamsabadi, S.B. Chehelcheshmeh, M. Alipour, A new identity-based encryption scheme for secure sharing of medical data in the cloud using blockchain. (2022). https://doi.org/10.21203/rs.3.rs-1214605/v1
8. K.N. Thasni, B. Narayamparambil, Advanced unified encrypting methodology to enhance the security of health information in cloud storage employing blockchain. Int. J. Soft Comput. Sci. Eng. Inf. Technol. **8**, 122-128 (2022). https://doi.org/10.32628/CSEIT228416
9. Z. Sun, L. Chen, H. Wang, Y. Li, A blockchain-based secure storage scheme for medical information. EURASIP J. Wirel. Commun. Netw. **2022**, 40 (2022). https://doi.org/10.1186/s13638-022-02122-6

10. A. Amanat, M. Rizwan, C. Maple, Y.B. Zikria, A.S. Almadhor, S.W. Kim, Blockchain and cloud computing based secure electronic healthcare records storage and sharing. Front. Public Health. **10,** 938707 (2022). https://doi.org/10.3389/fpubh.2022.938707
11. M. Mainuddin, S. Rahman, A. Karim, T. Alam, Blockchain-enabled IPFS cloud solution for storing and sharing patient data securely and efficiently, in Proceedings of the International Conference on Emerging Information and Communication Technologies (EICT), IEEE, Khulna, Bangladesh, February 13 (2023), 1-6
12. O. Ussatova, A. Bekzhanova, D. Abdirassilova, A. Nurtayeva, Enhancing healthcare data security: A two-step authentication scheme with cloud technology and blockchain. East. Eur. J. Enterp. Technol. **126**, 6 (2023). https://doi.org/10.15587/1729-4061.2023.289325
13. S. Sutradhar, P. Das, R. Paul, A blockchain privacy-conserving framework for secure medical data transmission in the Internet of Medical Things. Decis. Anal. J. **10**, 100419 (2024)
14. D.N. Varshitha, Blockchain solutions for secure healthcare data management: A comprehensive survey. Indian Sci. J. Res. Eng. Manag. (2024)
15. M. Mahalingam, M. Sankara, S. Kumar, P. Raj, A cloud-based approach to secure electronic medical records, in Proceedings of the International Conference on Expert Clouds and Applications (ICOECA), IEEE, Bengaluru, India, August 05 (2024), 263-270
16. A. Shahzad, S. Ali, H. Rehman, F. Khan, A robust algorithm for authenticated health data access via blockchain and cloud computing. Plos One **19**, e0307039 (2024). https://doi.org/10.1371/journal.pone.0307039
17. A.K. Hebballi, R. Kumar, P. Shetty, S. Rao, Securing medical data records using blockchain in a cloud computing environment, in Proceedings of the Third International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), IEEE, Bhilai, India, May 15 (2023), 1-5
18. K. Murugeswari, G. Ganesan, Introduction to blockchain technology for securing healthcare. In Cybersecurity and Data Management Innovations for Revolutionizing Healthcare, IGI Global, Hershey, PA, USA, July 23 (2024), 197-210