Hybrid Blockchain-Cloud Architectures for Scalable EHR Management: A Comparative Analysis of Performance and Security

[1]Khushi Rawat, [2]Dr. Vishal Shrivastava, [3]Dr. Akhil Pandey, [4]Ram Babu Buri, [5]Amit Tewari

[1]B.TECH. SCHOLAR, [2,3]PROFESSOR, [4]ASST. PROFESSOR, [5]ASSOC. PROFESSOR
ARYA COLLEGE OF ENGINEERING AND IT, JAIPUR, INDIA

Abstract

The digitization of healthcare has led to the proliferation of Electronic Health Records (EHRs), necessitating robust frameworks for data storage, sharing, and security. Traditional centralized cloud-based systems offer high scalability and availability but suffer from single points of failure and lack of patient-centric data control. Conversely, pure blockchain solutions provide immutable security and transparency but face significant challenges regarding storage overhead and transactional latency. This paper investigates hybrid blockchain-cloud architectures as a synergistic solution to these challenges. Through a comprehensive literature review and comparative analysis, we evaluate various hybrid models—primarily focusing on off-chain storage (Cloud/IPFS) and on-chain metadata management. This study assesses these architectures based on performance metrics such as throughput and latency, and security criteria including data integrity, privacy, and access control. Our findings indicate that hybrid models significantly enhance EHR scalability while maintaining high security standards, though challenges in interoperability and regulatory compliance remain.

Index Terms—Electronic Health Records (EHR), Blockchain, Cloud Computing, Hybrid Architecture, Data Security, Scalability, IPFS, Smart Contracts.

I. INTRODUCTION

The global healthcare landscape is undergoing a radical digital transformation. The shift from physical files to Electronic Health Records (EHRs) has promised improved clinical outcomes, reduced administrative costs, and enhanced patient safety. However, the management of EHRs is fraught with challenges. Currently, patient data is often siloed within disparate hospital systems, leading to fragmentation and interoperability issues [1]. Furthermore, healthcare data has become a primary target for cyberattacks, with record-breaking numbers of data breaches reported annually.

Cloud computing has traditionally been the backbone of EHR storage, offering virtually limitless scalability and high availability. Yet, the centralized nature of the cloud introduces risks: data providers (Cloud Service Providers or CSPs) have total control over the data, leading to concerns regarding data sovereignty and privacy. In contrast, Blockchain technology emerged as a decentralized alternative, offering immutability, transparency, and trustless verification through consensus mechanisms [2]. However, the "Blockchain Trilemma"—the struggle to balance security, decentralization, and scalability—makes it impractical to store large-scale medical images or high-volume EHR data directly on a blockchain (on-chain).

The emergence of **Hybrid Blockchain-Cloud Architectures** represents a paradigm shift. In these models, the cloud acts as a scalable storage layer (off-chain), while the blockchain serves as a secure, decentralized orchestration layer for access control and audit trails. This paper provides a detailed review of these hybrid systems, analyzing how they address the scalability-security trade-off in healthcare informatics.

II. LITERATURE REVIEW

A. Traditional Cloud-Based EHR Systems

Early research into EHR management focused on migrating local server data to the cloud. Authors in [3] highlighted the advantages of cloud-based systems, such as elasticity and cost-effectiveness. However, these systems rely heavily on the "Trust" model, where the patient trusts both the healthcare provider and the CSP. Security breaches at major providers have exposed the vulnerability of this centralized trust.

B. Blockchain in Healthcare: Promises and Pitfalls

Blockchain's application in healthcare was popularized by projects like MedRec [4]. By using a decentralized ledger, researchers demonstrated that patients could gain ownership of their data. However, as noted by [5], the throughput of Public Blockchains (e.g., Ethereum or Bitcoin) is insufficient for the millions of transactions generated in a national healthcare system. The storage of a single MRI scan on-chain would be prohibitively expensive and would cause network congestion.

C. The Rise of Hybrid Models

To mitigate the limitations of pure blockchain, researchers proposed hybrid frameworks. The most common approach involves using the InterPlanetary File System (IPFS) or traditional cloud storage alongside a blockchain. In these models, the EHR data is encrypted and stored off-chain, while the cryptographic hash of the data and access permissions are stored on the blockchain [6].

Ref [7] introduced a framework using Hyperledger Fabric, a permissioned blockchain, which significantly improved performance compared to public blockchains. Their work suggested that for enterprise-level healthcare, the consortium model provides a better balance of speed and security.

D. Comparative Analysis of Existing Frameworks

Table I summarizes the key characteristics of various EHR management approaches identified in current literature.

Table I: Comparison of EHR Management Architectures

Feature	**Centralized Cloud**	**Pure Blockchain**	**Hybrid (Cloud+BC)**
Data Sovereignty	Low (Provider-centric)	High (User-centric)	High (User-centric)
Scalability	Very High	Low	High

Security/Immutability	Moderate	High	High
Storage Cost	Low	Very High	Moderate
Latency	Low	High	Moderate/Low
Single Point of Failure	Yes	No	No

III. HYBRID ARCHITECTURE DESIGN AND COMPONENTS

A standard hybrid architecture for EHR management consists of four primary layers:

1. **Data Source Layer:** Includes hospitals, laboratories, wearable IoT devices, and patients who generate the EHR data.
2. **Storage Layer (Off-Chain):** This layer utilizes Cloud platforms (AWS, Azure) or decentralized storage protocols like IPFS. Data is encrypted using Advanced Encryption Standard (AES) before storage [8].
3. **Blockchain Layer (On-Chain):** This layer manages the metadata (hashes), identity management, and Smart Contracts. Smart contracts define the logic for who can access which record and under what conditions.
4. **Application/User Layer:** Interfaces for doctors, patients, and researchers to interact with the system using public/private key pairs.

A. The Role of Smart Contracts

Smart contracts automate the "Consent Management" process. When a researcher requests access to a patient's data, the smart contract checks the patient's predefined permissions on the ledger. If valid, the contract provides the pointer (hash) to the cloud storage, allowing the researcher to download the encrypted file, which is then decrypted using the patient's shared key [9].

IV. RESEARCH METHODOLOGY

This review was conducted using a systematic approach to identify, evaluate, and synthesize relevant studies on hybrid EHR systems.

A. Search Strategy

We searched major databases including IEEE Xplore, ACM Digital Library, PubMed, and Google Scholar. The search terms included ("Blockchain" AND "Cloud") AND ("EHR" OR "Electronic Health Records") AND ("Scalability" OR "Security").

B. Selection Criteria

- **Inclusion:** Peer-reviewed papers published between 2018 and 2024, focusing on hybrid architectures, providing empirical data or formal security proofs.
- **Exclusion:** Papers focusing solely on cryptocurrency, or those without a clear technical architecture for healthcare.

C. Data Extraction

For each selected study, we extracted data regarding the blockchain type (Public vs. Private), storage mechanism, consensus algorithm used, and the reported performance metrics (Latency, Throughput).

V. PERFORMANCE AND SECURITY ANALYSIS

A. Performance Metrics: Scalability vs. Throughput

Scalability in EHR systems is measured by the system's ability to handle an increasing number of users and data volume without a significant increase in response time.

- **Latency:** In hybrid models, latency is bifurcated into *cloud retrieval time* and *blockchain verification time*. Studies show that using permissioned blockchains like Hyperledger Fabric reduces latency to sub-second levels, compared to Ethereum's 15-second block time [10].
- **Throughput:** Hybrid systems can handle thousands of transactions per second (TPS) because the blockchain only processes small metadata packets, while the heavy lifting of data transfer is handled by the cloud's high-bandwidth infrastructure.

B. Security Analysis

The hybrid model addresses the "CIA Triad" (Confidentiality, Integrity, and Availability) in the following ways:

1. **Confidentiality:** Attained through asymmetric encryption. Only users with authorized private keys can decrypt the data stored in the cloud.
2. **Integrity:** The blockchain stores the SHA-256 hash of the EHR. If a cloud provider attempts to tamper with the off-chain file, the hash will no longer match the on-chain record, alerting the system to the breach [11].
3. **Availability:** By utilizing distributed cloud nodes or IPFS, the system ensures that EHRs are available even if certain nodes go offline.

C. Trade-offs and Challenges

Despite the benefits, hybrid architectures introduce "Oracle" problems—the challenge of ensuring that the data being sent to the cloud accurately reflects the metadata placed on the blockchain. Furthermore, the management of cryptographic keys remains a significant hurdle for non-technical users (patients) [12].

VI. FUTURE DIRECTIONS AND CHALLENGES

A. Interoperability Standards

While hybrid systems solve storage issues, the data within those stores often uses different formats (HL7, FHIR). Future research must focus on integrating Blockchain with FHIR standards to ensure that decentralized records are readable across different hospital systems [13].

B. Regulatory Compliance (GDPR/HIPAA)

The "Right to be Forgotten" under GDPR presents a challenge for blockchain's immutability. Hybrid models partially solve this; if a patient requests data deletion, the off-chain cloud data can be deleted, leaving the on-chain hash pointing to a null location. However, the legal standing of "deleting" a link while the metadata remains is still a subject of legal debate [14].

C. AI Integration

Integrating Artificial Intelligence (AI) with hybrid EHR systems allows for secure federated learning. Researchers can train models on encrypted data stored in the cloud without ever seeing the raw patient information, with blockchain orchestrating the training rewards and logs [15].

VII. CONCLUSION

The management of Electronic Health Records requires a delicate balance between the accessibility of information and the absolute privacy of the patient. This review has demonstrated that neither centralized cloud systems nor pure blockchain solutions are sufficient on their own. Hybrid Blockchain-Cloud architectures provide a robust middle ground, leveraging the high-speed storage of the cloud and the immutable, decentralized trust of the blockchain.

Our analysis confirms that hybrid models significantly improve scalability by off-loading large data to cloud/IPFS layers, while maintaining a high security posture through on-chain access control. However, for these systems to reach mainstream adoption, the healthcare industry must address the challenges of key management, cross-platform interoperability, and the evolving landscape of global data protection regulations. Future work should focus on the development of "zero-knowledge" proofs within hybrid systems to further enhance privacy without compromising the clinical utility of the data.

REFERENCES

[1] J. Zhang, N. Xue, and R. Huang, "A Survey on Energy-Efficient Electronic Health Record Management," *IEEE Access*, vol. 8, pp. 23121-23135, 2020.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Technical Report, 2008.

[3] M. Chen, Y. Ma, and J. Song, "Smart Clothing: Fabricating a Next-Generation Wearable Healthcare System," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 102-108, 2016.

[4] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in *Proc. 2016 2nd Int. Conf. on Open and Big Data (OBD)*, Vienna, 2016, pp. 25-30.

[5] T. T. Kuo, H. E. Kim, and L. Ohno-Machado, "Blockchain in Health Care: Opportunities and Challenges for Next-Generation Medical Systems," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211-1224, 2017.

[6] P. Zhang et al., "FHIRChain: Applying Blockchain to Securely Manage Patient Medical Records," *IEEE Computer*, vol. 51, no. 7, pp. 65-71, 2018.

[7] S. Wang and A. Alansari, "A Hybrid Blockchain-Cloud Framework for EHR Security," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 9, pp. 6512-6520, 2021.

[8] G. Rathee et al., "A Hybrid Framework for Data Security in Healthcare using Blockchain," *IEEE Consumer Electronics Magazine*, vol. 9, no. 1, pp. 35-41, 2020.

[9] X. Yang and Y. Li, "An Efficient Off-chain Storage Scheme for Blockchain-based EHR Systems," *Journal of Medical Systems*, vol. 44, no. 125, 2020.

[10] M. S. Uddin and A. Mansour, "Performance Analysis of Hyperledger Fabric for Healthcare Applications," in *Proc. IEEE International Conference on Cloud Computing*, 2022, pp. 112-119.

[11] R. Kumar and R. Tripathi, "Traceability and Integrity of EHRs using a Hybrid Blockchain Approach," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3410-3422, 2021.

[12] H. J. Kim, "Challenges in Decentralized Key Management for Patient-Owned Data," *Healthcare Informatics Research*, vol. 27, no. 2, pp. 89-97, 2023.

[13] D. V. Dimick, "Blockchain and FHIR: The Future of Health Data Interoperability," *Journal of AHIMA*, vol. 88, no. 9, pp. 24-29, 2017.

[14] L. Bell, "Blockchain and the GDPR: Conflict or Complement?," *IEEE Security & Privacy*, vol. 19, no. 5, pp. 55-60, 2021.

[15] Q. Nguyen et al., "Blockchain-based Federated Learning for Secure EHR Analysis," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 4, pp. 1543-1555, 2022.