WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Survey on Hybrid Blockchain model for Solving Storage limitations

V. Madhusudhana Rao

Jntu no : 23341A12C8

ABSTRACT :

Blockchain technology offers significant opportunities to improve the management of healthcare information by enabling secure, transparent, and decentralized data exchange. Despite its advantages in ensuring data integrity and patient autonomy, the technology faces persistent barriers related to scalability and storage capacity. Healthcare organizations routinely generate vast amounts of data such as diagnostic images and electronic health records that current blockchain infrastructures cannot efficiently process or store. To overcome these challenges, this study proposes a hybrid blockchain architecture that integrates blockchain's immutability and auditability with flexible off-chain storage mechanisms. This approach maintains the security and transparency of blockchain while enabling scalable, cost-effective data handling. The paper further explores strategies to enhance interoperability, optimize data distribution, and employ advanced cryptographic techniques to support secure and sustainable healthcare data management.

Keywords : *Block Chain, Off-Chain Storage, Data Security, Interoperability, Hybrid Architecture, Cryptographic Techniques.*

Introduction :

Blockchain has emerged as a transformative technology capable of reshaping healthcare data management by promoting transparency, security, and accountability. Despite these advantages, large-scale adoption remains difficult due to issues of scalability and limited data storage capacity. Modern healthcare systems continuously produce massive datasets from diverse sources such as diagnostic imaging devices, electronic health records (EHRs), and real-time Internet of Medical Things (IoMT) sensors. These data-intensive environments exceed the storage and processing capabilities of current blockchain networks, which are restricted by transaction speed, block size, and overall throughput.

To address these constraints, researchers have proposed hybrid blockchain frameworks that integrate blockchain with external or cloud-based storage solutions. In such systems, blockchain serves as the immutable layer for access control, verification, and auditability, while encrypted patient information is stored off-chain in distributed environments. This hybrid strategy retains the decentralized trust and security of blockchain but eliminates the inefficiencies associated with storing large medical files directly on the ledger. Consequently, it provides a practical foundation for developing scalable, interoperable, and privacy-preserving healthcare data infrastructures.

Advantages of Block Chain Storage:

- **Data Integrity and Permanence:**
  Once information is recorded on a blockchain, it becomes permanent and resistant to unauthorized alterations, ensuring that medical records remain trustworthy over time**.**
- **Transparency and Auditability:**
  Every interaction with stored data is chronologically logged, allowing healthcare institutions to maintain detailed audit trails and trace all access events.
- **Decentralized Infrastructure:**
  By distributing data across multiple network participants rather than a single centralized server, blockchain reduces the likelihood of system-wide outages and enhances operational resilience.
- **Enhanced Security:**
  The use of advanced encryption and consensus algorithms protects patient data from tampering or unauthorized modification.
- **Empowered Patient Participation:**
  Smart contracts can be designed to give patients direct control over how and when their data are shared, promoting consent-based healthcare management.

- **Cross-Organizational Data Sharing:**
  Blockchain's standardized verification processes enable hospitals, laboratories, and insurers to exchange information securely without compromising data confidentiality.
- **Operational Robustness:**
  The distributed nature of the network minimizes vulnerabilities by ensuring that no single node failure can disrupt the entire system.

Literature Review :

Recent studies demonstrate that blockchain and related digital technologies are reshaping the way healthcare data are collected, stored, and shared. Researchers generally agree that blockchain can significantly improve data confidentiality, interoperability, and trust within medical ecosystems. It provides mechanisms for secure information exchange, promotes patient-centric data ownership, and supports transparent audit trails among healthcare providers.

Despite these benefits, the literature also points out several persistent challenges that prevent blockchain's full-scale implementation. Technical barriers include low scalability, high storage demands, and transaction latency, while institutional concerns relate to compliance with healthcare regulations, such as HIPAA and GDPR, and the difficulty of integrating blockchain with legacy hospital information systems.

Methodological landscape :

The methodologies employed to study the challenges of blockchain in healthcare are diverse. A large portion of the literature consists of review papers and descriptive analyses that identify scalability issues, storage limitations, and compliance challenges by surveying existing blockchain platforms and healthcare case studies (Reference 1, 3, 6, 9, 12). Another common approach involves simulation-based and pilot studies, where researchers test blockchain–cloud hybrid models or small-scale healthcare applications to evaluate transaction speed, storage cost, and system usability in real-world scenarios (Reference 4, 7, 10). A more technologically detailed line of research applies empirical experimentation with cryptographic techniques and consensus mechanisms to address issues like privacy, latency, and energy efficiency. For instance, studies have tested IPFS-based off-chain storage for large medical datasets (Reference 8) and layer-2 solutions like rollups to handle high transaction loads (Reference 11). Additionally, regulatory and security-focused research investigates compliance with healthcare standards (HIPAA, GDPR) and potential vulnerabilities in blockchain–cloud integration (Reference 5, 13)..

Key Research Thrusts and Objectives:

A primary objective across the reviewed literature is to investigate how blockchain can empower patients by giving them greater control over their medical data through smart contracts and consent frameworks (References 2, 6). Other objectives include ensuring secure and tamper-proof sharing of health records across providers, enabling real-time IoMT integration for continuous monitoring, and combining blockchain with AI and federated learning for secure data-driven insights (References 5, 9, 13). A recurring emphasis is also placed on aligning blockchain solutions with regulatory frameworks such as HIPAA, GDPR, and India's DPDP Act to ensure compliance and trust (References 10, 14).

Identified Gaps and Persistent Challenges:

Despite the promise of blockchain in healthcare, the literature consistently identifies several persistent challenges. The most prominent is scalability and storage limitations, as storing large medical data directly on-chain is costly and inefficient (References 3, 5, 11). Issues of real-time data sharing remain, as existing blockchain models often struggle to support time-sensitive healthcare needs such as telemedicine (References 4, 9). Privacy and access control challenges also persist, with patients lacking fine-grained control and data security concerns arising from weak consent mechanisms (References 6, 8). Furthermore, integration and regulatory barriers are significant: many solutions fail to align with existing hospital IT systems, while uncertainties in legal compliance slow adoption (References 7, 12, 14). Technical gaps include limited interoperability, lack of robust IoMT device security, and challenges in applying advanced encryption methods like homomorphic encryption at scale.

Comparison Table:

	Title	**Year**	**Performance Metrics**	**Research Objectives**	**Gaps**
Reference 1	Blockchain-Based Healthcare Records Framework	2024	Privacy and Security	Decentralized EHR management	Centralized systems risk, lack of real-time sharing
Reference 2	Harnessing	2024	Conceptual	Explore secure	Explore secure patient

	Blockchain to Transform Healthcare Data			patient data handling	data handling
Reference 3	Hybrid ML + Blockchain in Healthcare	2025	Accuracy, latency	Better decision-making using data	Weak automation, delay in processing
Reference 4	ODMSM-FL for IoMT	2024	Latency, accuracy	Secure large-scale IoT healthcare	Real-time learning, scalability
Reference 5	Hier Chain System	2024	Latency, privacy	Classify & protect health data	Scalability, privacy control
Reference 6	AI + Blockchain Integration	2025	Security rate, ML accuracy	Real-time secure health data	Integration & user awareness
Reference 7	Barriers to Blockchain in GCC	2024	Barrier mapping	Identify blockchain adoption hurdles	Tech skills, regulation gaps
Reference 8	AI + Blockchain + Cloud Integration	2022	Efficiency, scalability	Secure and smart data handling	Fragmented data, legal compliance
Reference 9	BHIIoT Framework	2023	Encryption, latency	Real-time secure IIoT data	Privacy, lifecycle gaps
Reference 10	A Secure and Scalable Permissioned Blockchain for EHR Management	2025	Access control, encrypted storage, low latency	Manage real-time IoMT health data securely and efficiently	Weak real-time IoMT security, poor scalability, limited access control
Reference 11	Blockchain Consent Management	2021	Caliper testbed	Consent-based secure access	Outdated components, lack of detail
Reference 12	Secure PHR for Telemedicine	2024	Latency, throughput	Safe PHR access in telehealth	Access control, throughput
Reference 13	Blockchain in Health	2024	None	Assess blockchain in clinical data	Regulation, technical complexity
Reference 14	Blockchain for Health Management	2025	TPS, integrity, speed	Enhance security & transparency	Usability, integration, complexity

Methodology:

Blockchain in healthcare faces challenges with scalability and storage because medical data, like images and IoMT streams, is extremely large. Storing all of this data directly on the blockchain can be slow and costly .A practical approach is to use off-chain storage—such as cloud storage, while keeping only hashes or metadata on the blockchain. This ensures the data remains secure, traceable, and tamper-proof without overloading the blockchain. To further improve efficiency, real-time sharing of medical data can be achieved using a combination of federated learning and blockchain. With federated learning, hospitals or devices can collaboratively train machine learning models on local data without sharing the raw patient information. Blockchain ensures that the model updates and data exchanges are secure, verified, and traceable. This setup allows doctors and patients to access insights and updated information instantly while maintaining data privacy and integrity. Additionally, layer-2 solutions like sidechains can manage high transaction volumes efficiently, and hybrid blockchain frameworks can be used to balance security, performance, and cost, making blockchain-based healthcare systems practical and scalable.

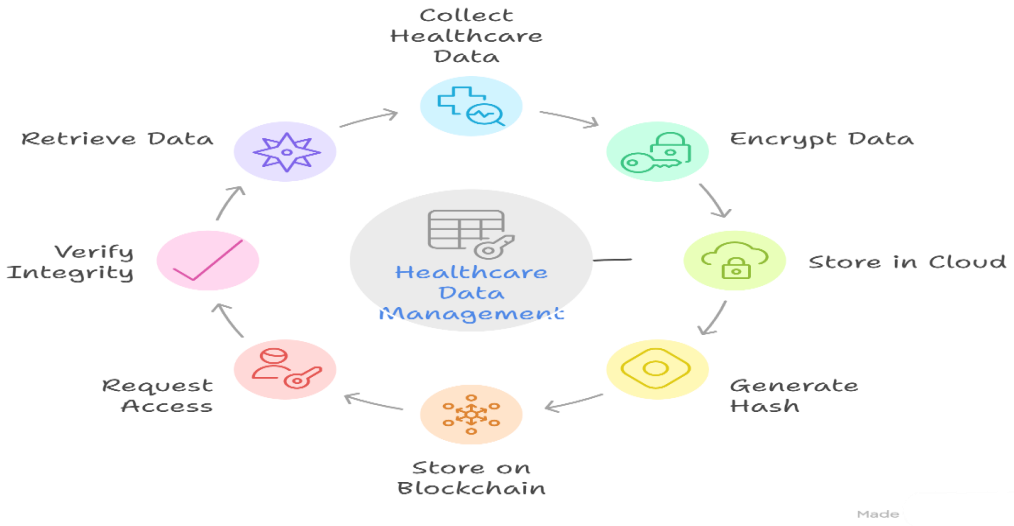
- **Hybrid Block Chain Model:**

Store bulk data off-chain (e.g., in cloud or distributed storage) while keeping only hashes on-chain for security. Using hybrid blockchain frameworks further improves efficiency, scalability, and performance.

Techniques Used :

- **Data Encryption :** To securely store medical records in the cloud.
- **Hashing :** To generate a tamper-proof fingerprint of cloud-stored data on-chain.
- **Access Control :** To ensure only authorized parties can access patient data.

- **Hybrid Blockchain Frameworks :** Combining blockchain (for security) with cloud (for scalable storage).
- **Real Time Data Sharing:**

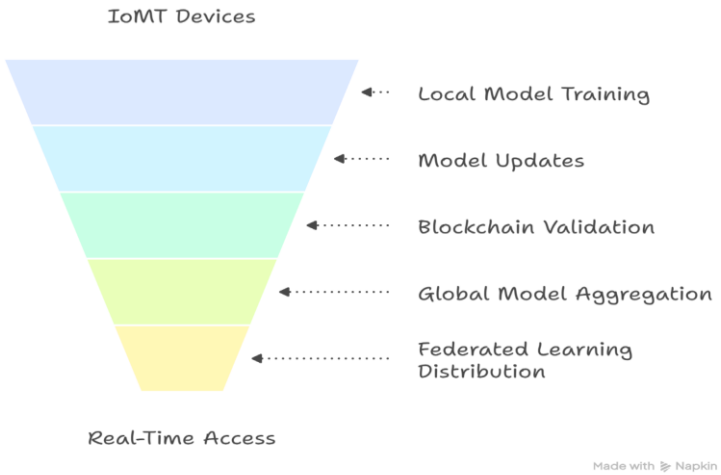


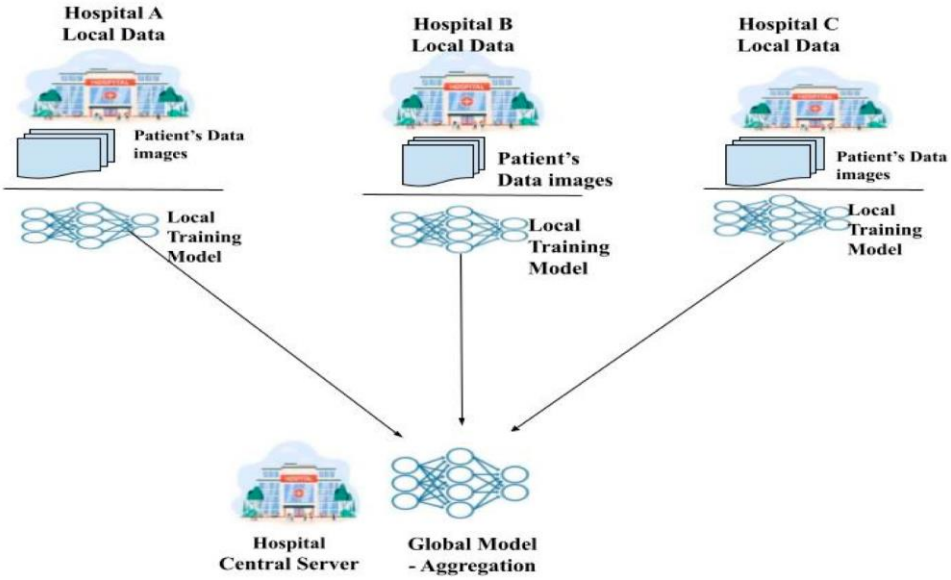
Integrating Federated Learning with a permissioned blockchain, which enables real-time, privacy-preserving data sharing and collaboration across healthcare providers without moving sensitive patient data.

Techniques Used :

- **Federated Learning (FL**): For decentralized model training without moving raw patient data.
- **Blockchain:** To record model updates securely and provide transparency.
- **IoMT Devices:** For continuous real-time health data collection.
- **Encryption Techniques:** To protect sensitive medical data during sharing.

Work Flow :





Conclusion :

Blockchain technology holds immense potential to revolutionize healthcare by ensuring data security, transparency, and integrity. However, its scalability and storage constraints limit its ability to handle large healthcare datasets such as medical images and IoMT streams. The proposed hybrid blockchain model, which integrates blockchain with cloud-based off-chain storage, addresses these challenges by maintaining only hashes or metadata on-chain while storing bulk data securely off-chain. This approach not only improves system scalability and cost efficiency but also ensures tamper-proof data integrity. Moreover, the integration of federated learning and IoMT devices enables real-time, privacy-preserving data sharing and collaborative analytics across healthcare providers. Through encryption, access control, and consensus mechanisms, the model ensures that sensitive medical information remains secure, traceable, and efficiently managed. Hence, the hybrid blockchain framework provides a practical and scalable pathway toward secure, interoperable, and intelligent healthcare data systems of the future.

REFERENCES :

- Tahir, N. U. A., Rashid, U., Hadi, H. J., Ahmad, N., Cao, Y., Alshara, M. A., & Javed, Y. (2024). Blockchain-Based Healthcare Records Management Framework: Enhancing Security, Privacy, and Interoperability.
- Treiblmaier, H., Rejeb, A., & Gault, M. (2024). Harnessing Blockchain to Transform Healthcare Data Management: A Comprehensive Research Agenda.
- Rathee, G., & Iqbal, R. (2025). Enhancing Decision-Making and Data Management in Healthcare: A Hybrid Ensemble Learning and Blockchain Approach.
- Ramani, R., Mary, A. R., Raja, S. E., & Shunmugam, D. A. (2024). Optimized Data Management and Secured Federated Learning in the Internet of Medical Things (IoMT) with Blockchain Technology.
- Agarwal, V., & Pal, S. (2024). HierChain: A Hierarchical Blockchain-Based Data Management System for Smart Healthcare.
- Tanveer, H., Faheem, M., & Khan, A. H. (2025). Blockchain and AI Integration for Secure Healthcare Data Management.
- Mutambik, I., Lee, J., Almuqrin, A., & Alharbi, Z. H. (2024). Identifying the Barriers to Acceptance of Blockchain-Based Patient-Centric Data Management Systems in Healthcare.
- Tatineni, S. (2022). Integrating AI, Blockchain, and Cloud Technologies for Data Management in Healthcare.
- Khan, A. A., Bourouis, S., Kamruzzaman, M. M., et al. (2023). Data Security in Healthcare Industrial Internet of Things (IIoT) With Blockchain.
- Alruwaili, M. N., Mohanty, S. P., & Kougianos, E. (2025). hChain 4.0: A Secure and Scalable Permissioned Blockchain for EHR Management in Smart Healthcare.
- Kakarlapudi, P. V., & Mahmoud, Q. H. (2021). Design and Development of a Blockchain-Based System for Private Data Management.
- Murthy, C. V. N. U. B., & Shri, M. L. (2024). Secure Sharing Architecture of Personal Healthcare Data Using Private Permissioned Blockchain for Telemedicine.
- Albiol-Perarnau, M., & Belmonte, I. A. (2024). Blockchain in Health: Transforming Security and Clinical Data Management.
- Perwej, Y., Waghodekar, P., Bewoor, M. S., Singh, S., Jaiswal, S., & Garg, A. (2025). Blockchain for Healthcare Management: Enhancing Data Security and Transparency.