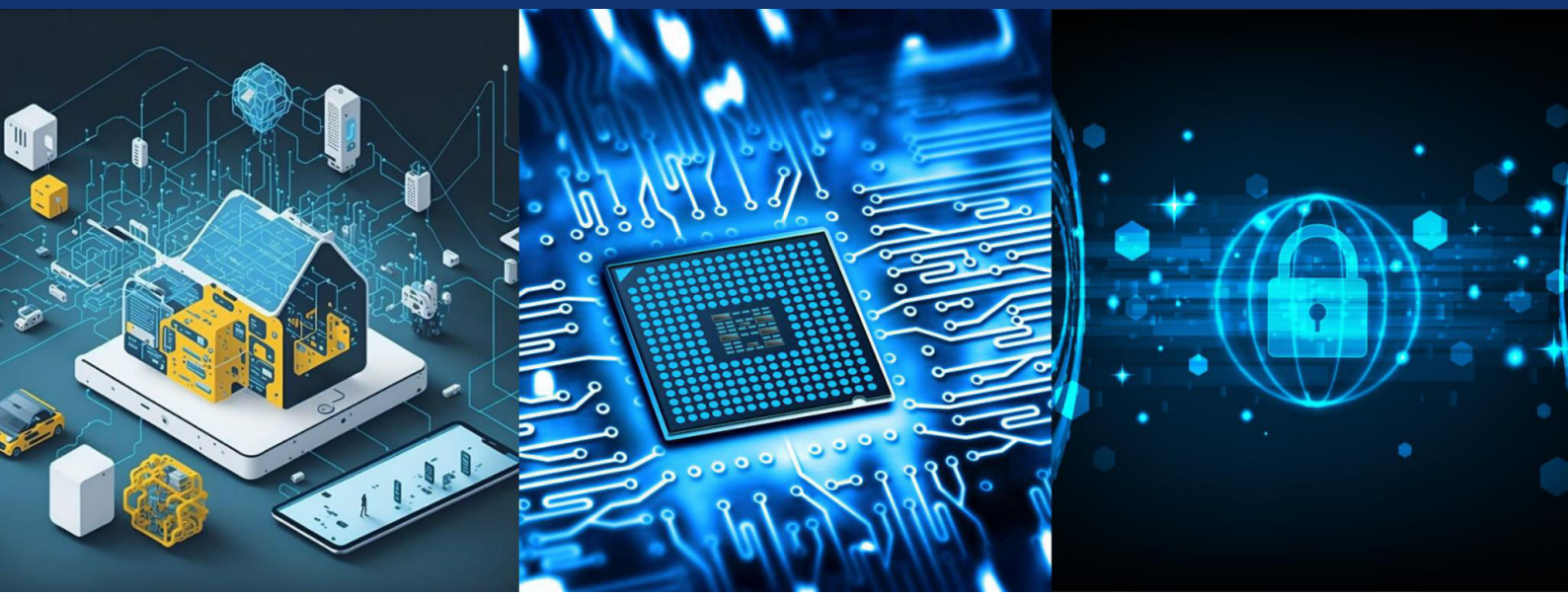
IJIRCCE

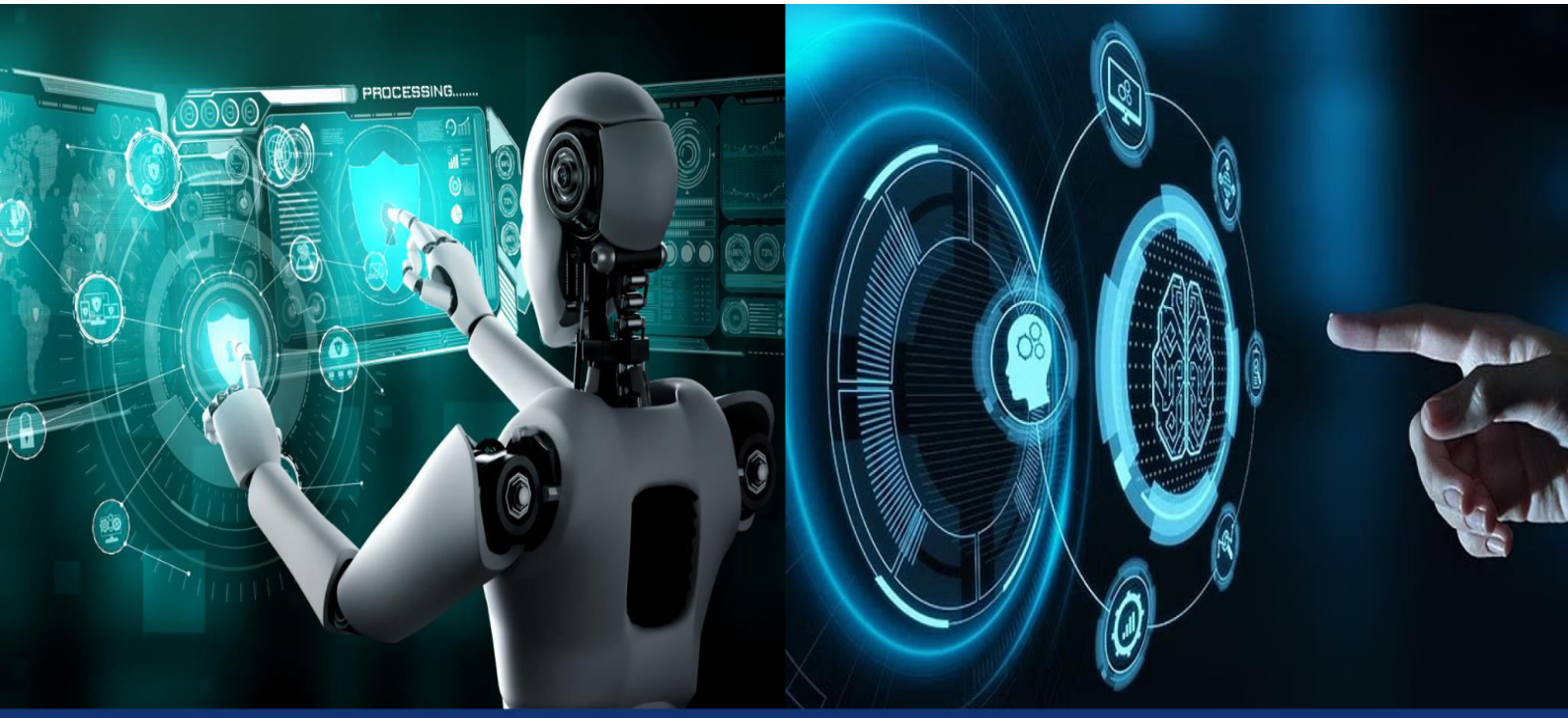
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 5, May 2025

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305163

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Role of Blockchain in Enabling Secure and Transparent Access to Health Data over Distributed Cloud Systems

N. Tamiloli, S. Kavi Priya

Professor, Department of Mechanical Engineering, PERI Institute of Technology, Mannivakkam, Chennai, India

Assistant Professor, Department of Computer Science Engineering, PERI Institute of Technology, Mannivakkam, Chennai, India

ABSTRACT: The rapid digitization of healthcare systems has led to an unprecedented increase in the volume and sensitivity of electronic health records (EHRs). While cloud computing has enabled scalable and cost-effective storage and access to health data, it poses significant concerns about privacy, data breaches, and centralized control. To address these challenges, blockchain technology has emerged as a transformative solution due to its decentralized, immutable, and transparent nature. When integrated with distributed cloud systems, blockchain offers a robust hybrid architecture that enables secure, patient-centric, and verifiable access to health data. This paper investigates the role of blockchain in enhancing the security and transparency of health data access over distributed cloud infrastructures. It reviews the current state of cloud-based health information systems, outlines the limitations of centralized data models, and discusses how blockchain can overcome these issues through smart contracts, cryptographic access control, and tamper-proof audit trails. A novel architecture is proposed that leverages blockchain for access management while utilizing distributed cloud systems for encrypted data storage. The study also addresses implementation challenges, including scalability, interoperability, and compliance with data privacy regulations. Finally, it highlights future research opportunities involving AI, federated learning, and quantum-resilient blockchain protocols in the healthcare domain.

KEYWORDS: Blockchain, storage, scalability, health, compliance.

I. INTRODUCTION

Blockchain is a decentralized, distributed ledger technology that records transactions across a network of computers in a secure, transparent, and tamper-proof manner. Originally developed as the foundation for cryptocurrencies like Bitcoin, blockchain has since evolved into a versatile technology with applications across various domains, including finance, supply chain, and healthcare. Each transaction or data entry on a blockchain is grouped into a block, cryptographically secured, and linked to the previous block, forming a continuous chain. This structure ensures data integrity, as altering any record would require consensus from most of the network and modification of all subsequent blocks.

One of the key strengths of blockchain is its ability to eliminate the need for centralized authorities by enabling peer-to-peer trust and consensus. The use of cryptographic techniques, such as hashing and digital signatures, further enhances data security and authenticity. Smart contracts—self-executing programs stored on the blockchain—automate transactions and enforce rules without third-party involvement.

In the healthcare sector, blockchain offers promising solutions for data sharing, patient privacy, and system interoperability. Its inherent transparency and immutability make it ideal for managing sensitive data like electronic health records, ensuring that access is secure, auditable, and patient-controlled. This foundational capability sets the stage for secure digital health ecosystems. computing is a technology that enables on-demand access to a shared pool of computing resources- such as servers, storage, databases, software, and networking—over the internet. These resources can be rapidly provisioned and released with minimal management effort, offering organizations a flexible and cost-effective alternative to traditional on-premises infrastructure. Cloud computing is typically offered in service models

such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), each catering to different levels of control and customization.

The key advantages of cloud computing include scalability, high availability, remote accessibility, and operational efficiency. In the healthcare sector, cloud computing enables the storage and processing of large volumes of Electronic Health Records (EHRs), real-time collaboration between healthcare providers, and integration of advanced technologies such as telemedicine and health analytics. However, despite its benefits, cloud computing also presents challenges-particularly regarding data security, privacy, and regulatory compliance. Since patient health data is sensitive and legally protected, ensuring confidentiality, integrity, and availability in cloud environments is critical. These concerns have led to increased interest in hybrid models that combine cloud scalability with emerging technologies like blockchain for secure, transparent, and patient-controlled data management.

II. LITERATURE REVIEW

The healthcare sector has steadily grown over the past decade and is projected to continue expanding. National Health Statistics report an average annual increase of 5.80% in public hospital discharges from 2018 to 2022 [1, 2]. This growth raises treatment costs and processing times, putting pressure on existing infrastructure. Consequently, healthcare organizations are turning to IT solutions to boost productivity, lower costs, and improve care quality [3, 4]. Shahzad et al studied that in modern healthcare, integrating blockchain with cloud systems enhances EHR security, access control, and auditing. Using CP-ABE and smart contracts, this approach ensures scalable, tamper-proof data sharing, dual authentication, and efficient resource management for secure health data exchanges [5]

Amjad Aldweesh proposed a blockchain-based data authentication algorithm for secure communication between electric vehicles, ensuring high authentication rates, low latency, and improved trust through decentralization, transparency, and non-repudiation in Internet of Vehicles networks [6].Abid Haleem analyzed the role of blockchain in healthcare, highlighting its potential to enhance data security, transparency, and performance. The study outlines blockchain's capabilities in securely managing health records, preventing data manipulation, and supporting global healthcare workflows[7].

K. Anil and Megha Kamble proposed HealthBlock, a blockchain-based system for secure healthcare data storage and retrieval in cloud environments. Using smart contracts on Ethereum and the HToB algorithm, their solution ensures data integrity, non-repudiation, and user-friendly access without requiring blockchain expertise [8]. Aarti Punia studied how blockchain enhances cloud computing access control by providing decentralized, transparent, and tamper-proof security. Through a review of 118 papers, twelve blockchain-based access control models were identified, addressing scalability, compatibility, and security challenges, and highlighting future research directions [9]. Ginavanee A. and S. Prasanna proposed a Hybrid Healthcare Data Management System (HDMS) combining blockchain and cloud computing to ensure secure, scalable health data storage and management. Using Ethereum smart contracts, Google Cloud, IPFS, and advanced privacy methods like decentralized identifiers and homomorphic encryption, HDMS improves data integrity, security, and efficiency-outperforming traditional encryption methods in processing times—aiming to enhance patient outcomes through better data handling [10]. Venkatesh Upadrista et al. reviewed the application of blockchain technology in Remote Health Monitoring (RHM) to address data security and privacy challenges. By leveraging blockchain's decentralization, immutability, and transparency, their study highlights how blockchain can help meet strict regulations like GDPR and HIPAA, enabling secure and compliant RHM deployment [11].

Through an extensive review of existing literature, we analyzed the contributions of various scholars working on the integration of blockchain with healthcare and cloud systems. While previous studies have focused on enhancing security, privacy, and data interoperability, we identified certain research gaps—particularly in the implementation of patient-controlled access mechanisms, real-time data sharing over distributed clouds, and standardized integration with existing healthcare infrastructures. Our work aims to address these gaps by proposing a hybrid blockchain-cloud framework that ensures secure, transparent, and patient-centric access to health data.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305163

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. PROPOSED ARCHITECTURE AND WORKFLOW

Proposed Architecture

The proposed system architecture integrates blockchain technology with distributed cloud systems to achieve secure, transparent, and efficient management of Electronic Health Records (EHRs). The architecture consists of four key components:

1. **Patient Node:**
2. Patients act as primary data owners, uploading their encrypted health records to distributed cloud storage. They control access permissions through blockchain-based smart contracts.
3. **Healthcare Provider Node:**
4. Authorized healthcare providers (doctors, hospitals, insurance companies) request access to patient data. Their access requests are validated and logged via blockchain.
5. **Blockchain Network:**
6. The blockchain acts as a decentralized ledger that stores transaction metadata such as data hashes, access policies, and audit logs. It enables immutable, tamper-resistant record-keeping and facilitates trust without relying on a central authority. Smart contracts enforce access control rules and automate key management.
7. **Distributed Cloud Storage:**
8. Actual EHR data is stored off-chain on encrypted, distributed cloud servers to ensure scalability and efficient storage management. The blockchain stores only data hashes to verify integrity.

Workflow

1. **Data Upload:**
2. Patients encrypt their health data using their private keys or attribute-based encryption (e.g., CP-ABE) and upload the encrypted records to distributed cloud storage. The system generates a unique hash of each record.
3. **Blockchain Registration:**
4. The generated hash, along with metadata (e.g., patient ID, access policies), is recorded immutably on the blockchain via smart contracts. This step creates a verifiable fingerprint of the health data.
5. **Access Request:**
6. Healthcare providers submit access requests to the blockchain network. The smart contract verifies the provider's credentials against predefined access policies.
7. **Authentication and Authorization:**
8. A dual authentication mechanism confirms the identity of the requester and verifies patient consent. Only authorized providers receive decryption keys or permission tokens.
9. **Data Retrieval:**
10. Upon authorization, providers retrieve the encrypted EHR data from the cloud storage and decrypt it using the provided keys.
11. **Audit Logging:**
12. All access events and transactions are automatically logged on the blockchain, ensuring transparency and enabling comprehensive auditing of data usage.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305163

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

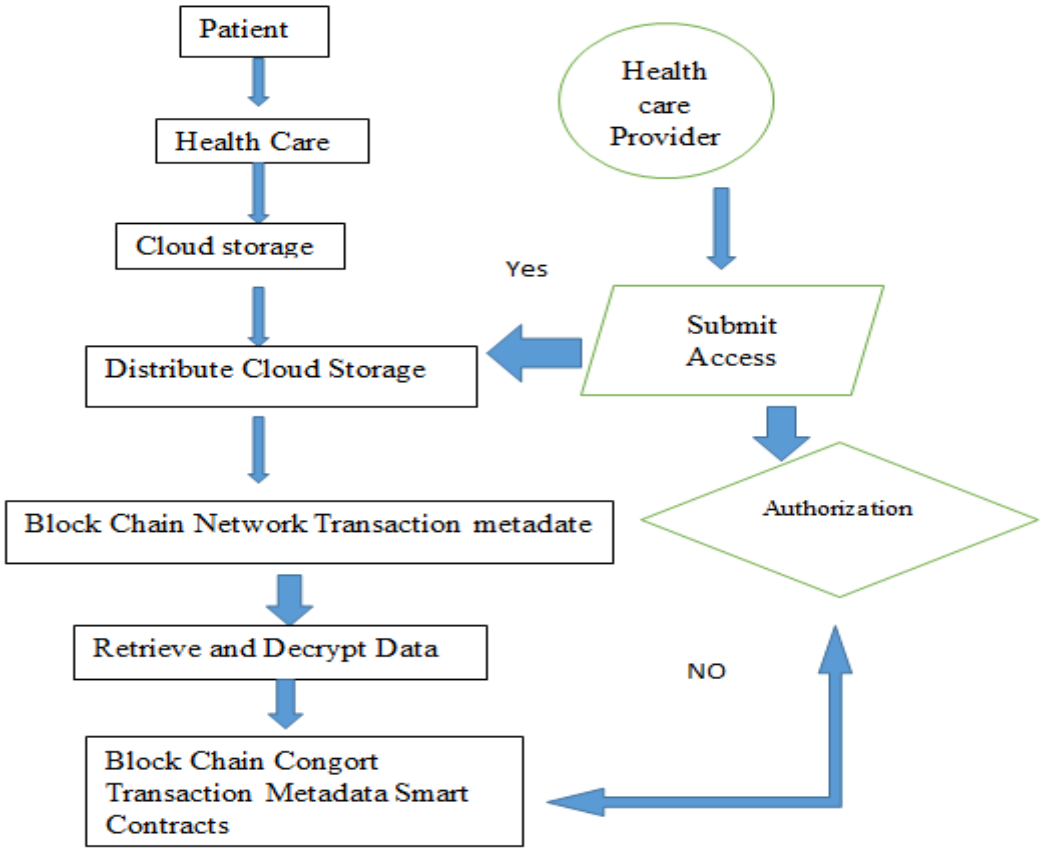


Figure 1. Block Chain steps

From Figure 1, Block blockchain is a decentralized digital ledger system used to securely record, store, and manage data across a distributed network of computers. Unlike traditional centralized systems, where data is controlled by a single authority, blockchain operates without a central governing body, ensuring transparency, security, and immutability. At the core of blockchain technology lies the "block" and the "chain." A block is a digital container that holds a list of transactions. These blocks are linked together chronologically to form a chain. Each block contains key components: transaction data, a timestamp, a nonce (a number used once during the mining process), the hash of the current block, and most importantly, the hash of the previous block. This structure ensures that any modification to a previous block alters its hash, thereby breaking the chain and making tampering easily detectable.

Each transaction on the blockchain is verified by a consensus mechanism, which ensures that all nodes (computers in the network) agree on the validity of the transactions. The most commonly used consensus algorithm is Proof of Work (PoW), where miners solve complex mathematical problems to validate and add new blocks to the chain. This process is energy-intensive but provides a high level of security. One of the critical components of a block is the Merkle Root, which is the top hash of a binary tree composed of all transaction hashes in the block. This structure ensures data integrity and allows quick verification of individual transactions within a block. Additionally, the use of cryptographic hash functions (such as SHA-256) makes it practically impossible to reverse-engineer the original data from the hash, further enhancing security.

Another important aspect is the decentralized nature of blockchain. Since the ledger is copied and distributed across many nodes, it is highly resistant to data loss, manipulation, and unauthorized access. Even if one or several nodes fail or are compromised, the data remains safe and accessible from other nodes. Blockchain's immutability means that once data is recorded, it cannot be altered without altering all subsequent blocks and gaining consensus from the majority of the network. This property makes blockchain ideal for applications requiring trust and transparency, such as

cryptocurrency (e.g., Bitcoin), supply chain management, voting systems, healthcare records, and financial transactions.

Furthermore, blockchain technology enhances transparency, as all participants have access to the same information and can independently verify data. It also reduces the need for intermediaries, thereby increasing efficiency and lowering transaction costs. In summary, blockchain is a revolutionary technology that offers a secure, transparent, and decentralized way to record digital transactions. Its structure—comprising linked blocks with cryptographic hashes, consensus protocols, and distributed storage—ensures data integrity and trustworthiness. As blockchain continues to evolve, its potential applications are expanding beyond cryptocurrency into many sectors, promising to reshape how information is managed and shared across the globe.

IV. RESULTS AND DISCUSSION

The integration of blockchain technology with distributed cloud systems offers a promising solution to long-standing challenges in healthcare data management, particularly around security, privacy, transparency, and interoperability. Traditional health data systems are often centralized, making them vulnerable to cyberattacks, unauthorized access, and single points of failure. Blockchain, by contrast, provides a decentralized and immutable ledger that ensures data integrity and trust. Blockchain's primary advantage in this context is its ability to secure health records through cryptographic techniques. Each transaction involving a patient's health data is recorded in a block and linked chronologically with previous blocks, creating a tamper-proof chain. This ensures that any unauthorized modification attempts are immediately detectable.

Additionally, smart contracts can be used to automate access control, allowing patients to manage who can view or edit their data. This patient-centric approach empowers individuals with ownership over their medical information, a crucial step toward personalized and consent-driven healthcare. By storing sensitive health data off-chain in encrypted cloud storage and recording metadata and access permissions on-chain, the system achieves both scalability and security. This hybrid architecture reduces the storage burden on the blockchain while maintaining transparency and auditability. Furthermore, blockchain's distributed nature ensures high availability and fault tolerance, even if parts of the system fail. Healthcare providers, researchers, and insurers can securely share and access data in real time without compromising privacy. Blockchain enables a secure, transparent, and efficient framework for managing health data over distributed cloud systems. It addresses key concerns in the healthcare sector while paving the way for compliant, interoperable, and resilient data sharing ecosystems.

V. CONCLUSION

The integration of blockchain technology with distributed cloud systems presents a transformative approach to addressing the critical challenges of healthcare data management. By leveraging blockchain’s inherent features—such as decentralization, immutability, cryptographic security, and transparent access control—this system enables a secure and efficient framework for storing, accessing, and sharing sensitive health information. The study demonstrated that blockchain can effectively eliminate the risks associated with centralized data repositories by providing tamper-proof audit trails and decentralized access management. Patients gain enhanced control over their health data through smart contracts, ensuring privacy, consent, and ownership are upheld. Moreover, the hybrid model—storing encrypted health records in cloud systems while maintaining access logs and metadata on the blockchain—proves to be both scalable and secure. This balance ensures that the system can handle growing volumes of data while maintaining performance and integrity. However, challenges such as latency in public blockchains, lack of standardization, and integration with legacy EHR systems still need to be addressed for large-scale adoption. Continued research and collaboration between blockchain developers, cloud service providers, and healthcare stakeholders are essential for realizing the full potential of this technology. In conclusion, blockchain offers a robust, transparent, and patient-centric solution for health data management over distributed cloud systems. It not only enhances data security and trust but also lays the foundation formore interoperable, compliant, and innovative digital healthcare ecosystems.

Acknowledgement

The authors gratefully acknowledge the support and guidance provided by our faculty and PERI institution in the successful completion of this research. We also thank the technical experts and peers who contributed valuable insights on blockchain and cloud systems, helping to shape the direction and depth of this study.

REFERENCES

1. Lee, S., Kim, D.: Enhancing ehr system performance with blockchain: A case study. J. Healthcare IT 45, 98–108 (2023)
2. Liang, X., Zhao, J., Shetty, S., Li, D., Liu, J.: Integrating blockchain for data sharing and collaboration in mobile healthcare applications. IEEE Network 35(1), 14–19 (2021)3.
3. Garcia, M., Johnson, E.: Comparative study of blockchain and traditional EHR systems in healthcare: Efficiency and security perspective. Health Informat. J. 29, 132–144 (2023).
4. Wang, X., Li, Q., Zhang, L.: Blockchain-based ehr system for privacy-preserving data sharing. J. Med. Informat. Res. 42, 145–155 (2023).
5. Shahzad, Ali, Wenyu Chen, Momina Shaheen, Yin Zhang, and Faizan Ahmad. "A robust algorithm for authenticated health data access via blockchain and cloud computing." *Plos one* 19, no. 9 (2024): e0307039.
6. Aldweesh, Amjad. 2023. "A Blockchain-Based Data Authentication Algorithm for Secure Information Sharing in Internet of Vehicles" *World Electric Vehicle Journal* 14, no. 8: 223. https://doi.org/10.3390/wevj14080223
7. Bid Haleem, Mohd Javaid, Ravi Pratap Singh, Rajiv Suman, Shanay Rab, Blockchain technology applications in healthcare: An overview, International Journal of Intelligent Networks, Volume 2,2021, Pages 130-139,https://doi.org/10.1016/j.ijin.2021.09.005.
8. Anil, K. & Kamble, Megha. (2023). Health Block: A Blockchain-Based Secure Healthcare Data Storage and Retrieval System for Cloud Computing. International Journal on Recent and Innovative Trends in Computing and Communication. 11. 96-104. 10.17762/ijritcc.v11i9.8324.
9. Ghassan Husnain et al. introduced HealthChain, a blockchain-based EHR system offering advanced encryption, consent management, and cross-platform interoperability. It improves data access speed, enhances security, and increases patient control, significantly outperforming traditional and existing blockchain EHR systems.
10. S. Prasanna, G. A. . (2024). Integration of Ethereum Blockchain with Cloud Computing for Secure Healthcare Data Management System. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(21s), 1250–1260. Retrieved from https://www.ijisae.org/index.php/IJISAE/article/view/5591
11. Upadrista, V., Nazir, S. & Tianfield, H. Secure data sharing with blockchain for remote health monitoring applications: a review. *J Reliable Intell Environ* **9**, 349–368 (2023). https://doi.org/10.1007/s40860-023-00204-w

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details