International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 2
Mar-Apr 2026, PP 46-54

Blockchain-based secure health record management

V Dhanalakshmi[1], Prabhadevi R [2], Srivarshini M[3], Vaishnavi S[4]

[1] Assistant Professor Department of Computer Science and Engineering Kongunadu College of Engineering and Technology Tamilnadu,India

[2,3,4] Department of Computer Science and Engineering Kongunadu College of Engineering and Technology Tamilnadu,India

Abstract.- The increasing digitization of healthcare systems has led to the widespread adoption of electronic health records (EHRs), raising concerns about data security, privacy, and interoperability. This paper proposes a blockchain-based secure health record management system designed to ensure the confidentiality, integrity, and accessibility of patient data. By leveraging the decentralized and tamper-resistant nature of blockchain technology, the system enables secure storage and sharing of medical records among authorized stakeholders such as hospitals, doctors, and patients. Smart contracts are utilized to enforce access control policies and automate data-sharing permissions. Additionally, cryptographic techniques are integrated to protect sensitive information from unauthorized access and cyber threats. The proposed framework enhances transparency, reduces the risk of data breaches, and eliminates the need for a centralized authority. Experimental analysis demonstrates improved data security and efficient record management compared to traditional systems. This approach offers a reliable and scalable solution for modern healthcare environments.

Keywords: Blockchain, Electronic Health Records (EHR), Data Security, Smart Contracts, Healthcare Systems, Privacy, Decentralization

I. Introduction

Blockchain-based secure health record management is an innovative approach that uses decentralized digital ledger technology to improve how medical data is stored, shared, and protected. In traditional healthcare systems, patient records are typically stored in centralized databases, which are susceptible to cyberattacks, data breaches, and system failures. Blockchain, however, distributes data across a network of nodes, reducing these risks and enhancing overall system reliability.

A key feature of blockchain technology is its immutability. Once data is recorded on the blockchain, it cannot be changed or removed without network consensus. This ensures that health records remain accurate and tamper-proof, which is essential for maintaining trust in medical information. Every update is securely encrypted, time-stamped, and linked to previous records, creating a transparent and traceable history of patient data.

Security is one of the most significant benefits of blockchain in healthcare. Sensitive patient information is protected through advanced cryptographic techniques, and access is restricted to authorized users via secure keys. This greatly minimizes the chances of unauthorized access and data misuse. Moreover, blockchain promotes a patient-centered model by allowing individuals to control access to their own health records, deciding who can view or share their data.

Another significant advantage is the improvement in terms of interoperability. Data related to healthcare is generally fragmented among different systems. It is challenging for healthcare providers to access patient data. Blockchain technology can facilitate the sharing of data among different hospitals and healthcare providers without the requirement for intermediaries.

Even though the adoption of blockchain technology in the healthcare sector is beneficial, there are challenges to be overcome. For instance, the challenges include scalability, legal regulations, and standardization.The adoption of blockchain technology in the management of health records is beneficial to the healthcare sector. It is capable of transforming the sector in terms of security, transparency, and efficiency. Even though challenges exist, the improvement in technology is likely to support its adoption in the future.

II. Related Works

Secure and Trustable Electronic Medical Records Sharing using Blockchain Alevtina Dubovitskaya, Zhigang Xu, Samuel Ryu, Michael Schumacher, Fusheng Wang proposes a blockchain-based framework for secure sharing of electronic medical records (EMRs). It emphasizes privacy, integrity, and access control by leveraging blockchain's decentralized and immutable structure. The system enables healthcare providers to securely exchange patient data while maintaining patient consent through smart contracts. A prototype was implemented in collaboration with a hospital, demonstrating improved data accessibility and reduced delays in record sharing. The study highlights how blockchain enhances trust among stakeholders and reduces dependency on centralized systems, ultimately improving healthcare efficiency and patient outcomes.

SSHealth: Toward Secure, Blockchain-Enabled Healthcare Systems Alaa Awad Abdellatif, Abeer Z. Al-Marridi, Amr Mohamed, Aiman Erbad, Carla Fabiana Chiasserini, Ahmed Refaey introduces SSHealth, a blockchain-based healthcare system designed to ensure secure medical data exchange and real-time monitoring. It integrates blockchain with edge computing to support applications such as epidemic detection and emergency response. The framework enhances interoperability between healthcare entities while maintaining data privacy and quality of service. It also allows flexible system configurations based on healthcare requirements. The study demonstrates how combining blockchain with emerging technologies can significantly improve healthcare delivery, security, and responsiveness in critical situations.

A Secure Blockchain Framework for Healthcare Records Management Systems Mahmoud Ahmad Al-Khasawneh, Muhammad Faheem, Ala Abdulsalam Alarood, Safa Habibullah, Abdulrahman Alzahrani proposes a secure blockchain framework to

manage healthcare records efficiently. The system ensures data integrity, confidentiality, and controlled access using encryption and distributed ledger mechanisms. It eliminates single points of failure and enhances trust among healthcare providers. The framework also supports scalability and interoperability with existing systems. Experimental results indicate improved performance in secure data handling and storage compared to traditional systems. The study concludes that blockchain can significantly enhance healthcare data management by ensuring secure and transparent operations.

MedRSS: A Blockchain-Based Scheme for Secure Storage and Sharing of Medical Records proposes a blockchain-based architecture combining Hyperledger Fabric, IPFS, and cryptographic techniques such as AES and ECC. The system separates on-chain and off-chain data storage to improve scalability while maintaining security. Smart contracts are used for access control, ensuring that only authorized users can access medical records. The framework enhances privacy protection and reduces storage overhead on the blockchain. It also addresses issues related to large-scale healthcare data management. The study demonstrates that integrating blockchain with distributed storage technologies can provide a practical and secure solution for modern healthcare systems.

A Secure Blockchain-Based E-Health Records Storage and Sharing Scheme presents a blockchain-based scheme designed for telemedicine environments. It ensures secure storage and sharing of electronic health records while preserving patient anonymity. The proposed protocol incorporates cryptographic techniques and authentication mechanisms to prevent unauthorized access. It is validated using security models to demonstrate robustness against attacks. The system supports secure communication between patients and healthcare providers, especially in remote healthcare scenarios. The study highlights the importance of blockchain in enabling secure telemedicine services and improving healthcare accessibility.

A Blockchain-Based Secure Storage Scheme for Medical Information Zhijie Sun, Dezhi Han, Dun Li, Xiangsheng Wangproposes a blockchain-based storage model to protect sensitive medical information. It utilizes encryption and distributed ledger technology to ensure data confidentiality and integrity. The scheme supports secure data sharing among healthcare entities while preventing unauthorized modifications. The authors focus on improving system efficiency and reducing computational overhead. Experimental analysis shows that the proposed system achieves better performance in terms of security and reliability compared to traditional storage solutions. The research demonstrates blockchain’s potential to address key challenges in healthcare data management.

Secure Healthcare Record Sharing Mechanism with Blockchain Ghulam Qadar Butt, Toqeer Ali Sayed, Rabia Riaz, Sanam Shahla Rizvi, Anand Paul focuses on secure sharing of healthcare records using blockchain technology. It addresses challenges such as data leakage, unauthorized access, and communication vulnerabilities. The proposed system uses blockchain to create a decentralized environment for data exchange, ensuring transparency and security. It also integrates encryption techniques to safeguard patient information during transmission. The framework improves trust among healthcare

providers and enhances collaboration. The paper demonstrates that blockchain can effectively solve data-sharing issues in healthcare systems while maintaining privacy and security.

Electronic Medical Records Using Blockchain Technology
G. Sucharitha, G. Sai Aditya, J. Varsha, G. Sai Nikhil explores the use of blockchain technology for managing electronic medical records. It proposes a system where patient data is stored in an append-only blockchain, ensuring immutability and security. The model allows patients to control access to their data, granting permissions to doctors as needed. It enhances privacy, prevents data tampering, and ensures transparency in healthcare transactions. The study highlights blockchain's ability to provide secure and efficient record management while improving patient trust and data accessibility.

An Improved Blockchain-Based Secure Medical Record Sharing Scheme Hüseyin Bodur, Imad Fakhri Taha Al Yaseen proposes an improved blockchain-based scheme for secure medical record sharing. It divides patient data into sensitive and non-sensitive categories to enhance privacy protection. The system uses blockchain to securely store and share data while minimizing vulnerabilities. Advanced encryption and access control mechanisms are implemented to prevent unauthorized access. The framework improves efficiency and reduces risks associated with traditional centralized systems. The study demonstrates that categorizing data and using blockchain can significantly enhance security and performance in healthcare data sharing.

Blockchain-Based Healthcare Records Management Framework: Enhancing Security, Privacy, and InteroperabilityNoor Ul Ain Tahir, Umer Rashid, Hassan Jalil Hadi, Naveed Ahmad, Yue Cao, Mohammed Ali Alshara, Yasir Javed presents a comprehensive blockchain framework for managing electronic health records. It focuses on improving data security, privacy, and interoperability among healthcare systems. The framework leverages blockchain's decentralized architecture to eliminate single points of failure and ensure data integrity. It also supports seamless data exchange between healthcare providers. The study highlights challenges such as scalability and implementation complexity while demonstrating the benefits of blockchain in healthcare. The proposed model shows significant potential for improving healthcare data management systems.

III.Proposed System

The proposed system for blockchain-based secure health record management is designed to create a decentralized, reliable, and efficient platform for handling electronic health records (EHRs). Unlike conventional centralized databases, this approach uses blockchain technology to improve data security, ensure integrity, and maintain transparency, while also giving patients greater control over their personal medical information.

In this model, sensitive health data is not stored directly on the blockchain due to storage limitations and privacy concerns. Instead, the actual records are kept in secure off-chain storage systems such as cloud platforms or distributed storage networks like IPFS. The blockchain stores encrypted hashes or references to these records, allowing

any unauthorized changes to be easily identified. Each interaction with the data, including updates or access requests, is recorded on the blockchain, forming a permanent and tamper-proof audit trail.

Access to medical records is controlled through smart contracts, which define clear rules about who can view or modify specific data. Patients are considered the owners of their health information and can grant or revoke access to healthcare providers, insurers, or other stakeholders using secure cryptographic keys.

This ensures a patient-focused system that prioritizes privacy and trust. Additional security measures such as encryption and multi-factor authentication further protect sensitive information.The system also promotes interoperability by enabling seamless data sharing among different healthcare providers, as long as proper authorization is granted. This reduces redundancy, avoids repeated medical tests, and allows doctors to access accurate and up-to-date patient information quickly, leading to better clinical decisions. To ensure efficiency and scalability, the system adopts a permissioned blockchain network, where only verified participants like hospitals and laboratories can validate transactions. Consensus algorithms such as Practical Byzantine Fault Tolerance (PBFT) are used to achieve fast and secure validation without high computational costs.Furthermore, the system provides an intuitive interface for users. Patients can monitor their medical history, manage access permissions, and track data usage, while healthcare professionals can securely upload and retrieve records.

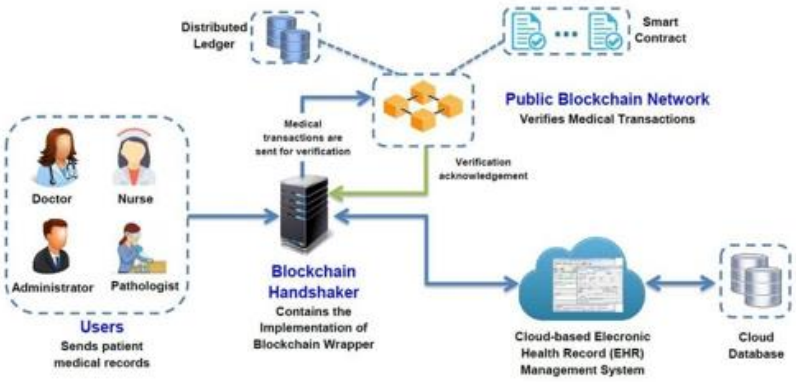

Fig.1.System Architecture

The proposed blockchain-based secure health record management system is composed of several functional modules, each designed to ensure secure, efficient, and reliable handling of electronic health records (EHRs). These modules work together to provide a decentralized and patient-centric healthcare data management solution.

User Registration and Authentication Module is responsible for registering patients and healthcare providers into the system. Each user is assigned a unique digital identity along with cryptographic key pairs (public and private keys) for secure authentication. Advanced authentication mechanisms, such as multi-factor authentication, are implemented to prevent unauthorized access and ensure system integrity.

Data Storage Module patient health records are securely stored in off-chain storage systems such as cloud servers or distributed storage networks. Since blockchain is not suitable for storing large volumes of data, only the cryptographic hash of each record is stored on the blockchain. This ensures data integrity, as any modification in the original record will result in a mismatch of the stored hash.

Blockchain Management Module manages all blockchain-related operations, including transaction creation, block formation, and validation. Each transaction, such as record creation or access request, is recorded as a block. A permissioned blockchain network is used, where only authorized entities can participate. Consensus algorithms like Practical Byzantine Fault Tolerance (PBFT) are applied to validate transactions efficiently.

Smart Contract and Access Control Module enforces access control policies using smart contracts. Patients have full authority over their data and can grant or revoke access permissions to healthcare providers, insurers, or researchers. Smart contracts automatically verify access requests based on predefined rules, ensuring secure and transparent data sharing without intermediaries.

Data Encryption and Security Module To ensure confidentiality, all medical data is encrypted before storage and transmission. This module applies advanced cryptographic techniques to protect sensitive patient information. Only authorized users with the correct decryption keys can access the data, minimizing risks of data breaches and cyberattacks.

User Interface Module provides an interactive interface for patients and healthcare providers. Patients can view their medical history, manage permissions, and track access logs, while healthcare professionals can upload, update, and retrieve patient records securely and efficiently. Audit and Monitoring Module maintains a complete audit trail of all transactions. Patients and administrators can monitor system activities, ensuring transparency and accountability. It helps detect suspicious behavior and supports compliance with healthcare regulations.

International Journal of Statistics and Mathematical Research Trends
E-ISSN: 3108-0871, Volume 2 Issue 2
Mar-Apr 2026, PP 46-54

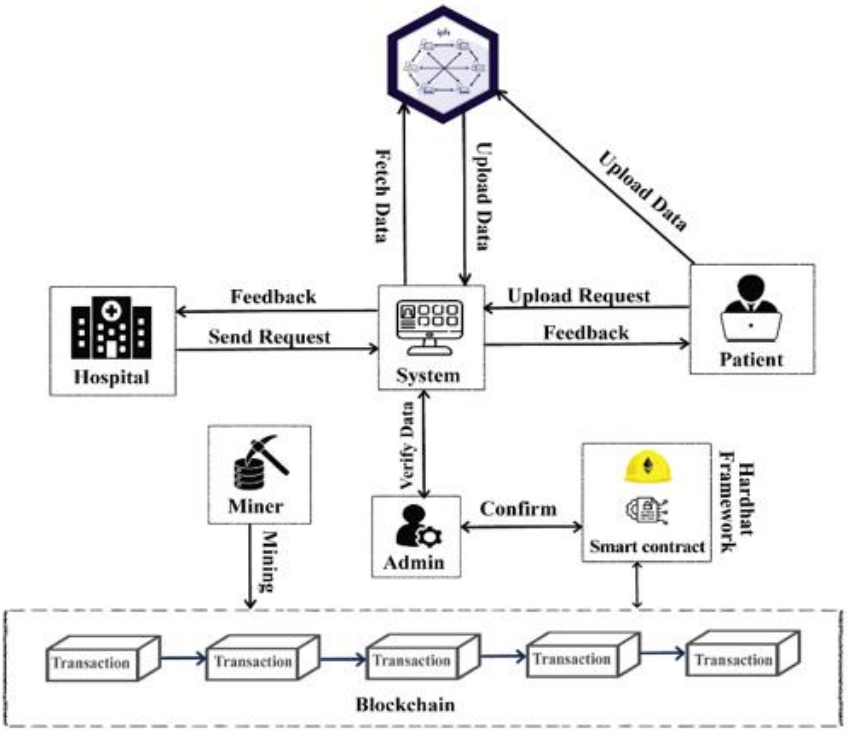

Fig.2.Methodology workflow of the Blockchain-based secure health record management

Overall Working Flow of the Proposed System:
The workflow methodology of the proposed blockchain-based secure health record management system follows a structured and decentralized process to ensure data security, integrity, and controlled accessibility. Initially, the patient registers in the system and is provided with a unique digital identity along with a pair of cryptographic keys (public and private keys). These keys are essential for authentication and secure communication within the network.

Once registered, healthcare providers such as hospitals and clinics are also authenticated and authorized to participate in the permissioned blockchain network. When a patient visits a healthcare provider, the provider generates medical records, which are encrypted and stored in an off-chain storage system such as a cloud database or distributed storage network. A cryptographic hash of the record is then created and stored on the blockchain along with a timestamp, ensuring immutability and traceability.

Access control is managed using smart contracts. When a healthcare provider or third party requests access to a patient's medical records, a request is sent through the blockchain network. The smart contract verifies the request based on predefined rules and patient permissions. If approved, the requester is granted access to the encrypted data

using secure key mechanisms. Otherwise, access is denied, ensuring strict privacy control.

Every transaction, including data creation, access requests, and modifications, is recorded as a block in the blockchain. These blocks are validated using a consensus mechanism such as Practical Byzantine Fault Tolerance (PBFT), which ensures fast and reliable agreement among authorized nodes without high computational overhead. Additionally, patients can monitor all activities related to their data through a user interface, including who accessed their records and when. This enhances transparency and trust in the system.

Overall, the workflow ensures a secure, transparent, and efficient process for managing electronic health records, minimizing risks associated with centralized systems while improving interoperability and patient control.

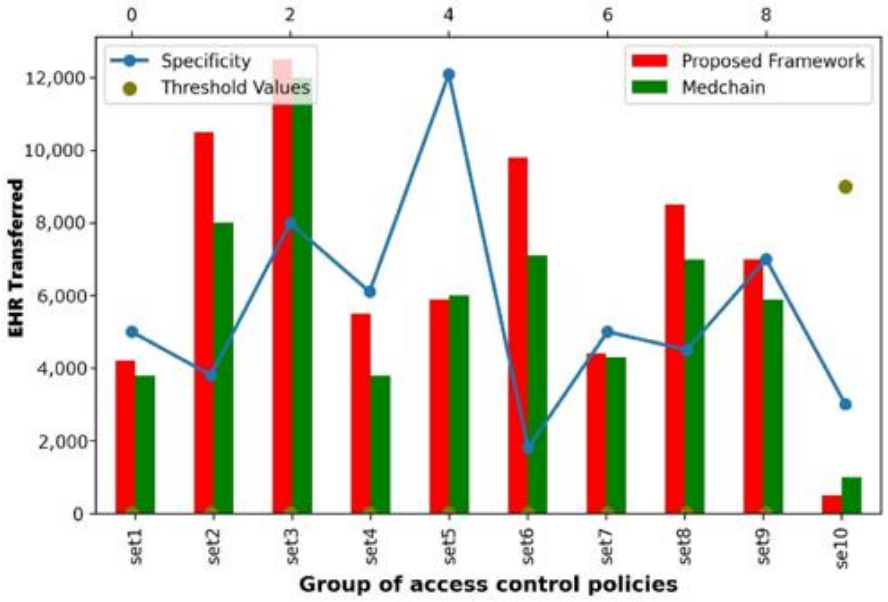

Fig.3.Performance Evaluation of Blockchain-based secure health record management

This equation represents a cryptographic hash function used to ensure data integrity in the blockchain-based health record system. The function takes an input data x(such as a medical record) and produces a fixed-length hash value H(x). Any slight modification in the input data results in a completely different hash, making tampering easily detectable. In the proposed system, only the hash of the patient's record is stored on the blockchain, while the actual data resides off-chain. This mechanism guarantees immutability, enables verification of data authenticity, and prevents unauthorized alterations of sensitive healthcare information.

This equation illustrates the encryption process used to secure patient data before storage or transmission. Here, Mrepresents the original medical data, K_pubis the public

key of the intended recipient, and Cis the encrypted ciphertext. Only the corresponding private key can decrypt the data, ensuring confidentiality. In the healthcare system, this approach is used to protect sensitive patient records when they are shared between providers. Even if the data is intercepted, it remains unreadable without the private key. This cryptographic mechanism strengthens privacy and prevents unauthorized access within the distributed network.

This equation defines the requirement for the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism used in the permissioned blockchain network. Here, nrepresents the total number of nodes, and fdenotes the maximum number of faulty or malicious nodes the system can tolerate. The condition ensures that consensus can still be reached even if some nodes behave incorrectly. In the proposed healthcare system, PBFT enables fast and reliable transaction validation without heavy computational costs. This improves system performance while maintaining trust and consistency across all participating healthcare entities in the blockchain network.

IV. Conclusion

the implementation of a blockchain-based secure health record management system offers a transformative approach to handling sensitive medical data. By leveraging decentralized architecture, the system eliminates the limitations of traditional centralized databases, such as vulnerability to data breaches, lack of transparency, and inefficient data sharing. The use of cryptographic techniques, hashing, and smart contracts ensures that patient records remain secure, tamper-proof, and accessible only to authorized individuals.

The proposed system enhances data integrity, privacy, and interoperability among healthcare providers, enabling seamless and reliable exchange of medical information. Patients are empowered with greater control over their health records, allowing them to manage access permissions and monitor data usage effectively. Additionally, the integration of off-chain storage and efficient consensus mechanisms improves scalability and system performance.

Despite certain challenges such as implementation complexity and regulatory considerations, the benefits of blockchain technology in healthcare are significant. It not only strengthens data security but also improves the overall quality and efficiency of healthcare services. Therefore, adopting blockchain for health record management can lead to a more transparent, trustworthy, and patient-centric healthcare ecosystem in the future.

V. Future Work

Future developments of the blockchain-based secure health record management system can concentrate on enhancing scalability, performance, and practical implementation. One key area is the adoption of more efficient consensus algorithms that minimize delay and energy usage while preserving system security. Additionally, hybrid blockchain architectures that combine both public and private networks can be explored to achieve better flexibility and optimized performance in healthcare applications.

Another promising direction involves integrating advanced technologies such as artificial intelligence and machine learning. These can enable secure data analysis for predictive diagnosis, personalized treatments, and early identification of diseases, while maintaining patient privacy through secure processing methods. The inclusion of Internet of Things (IoT) devices, like wearable sensors, can further support continuous health monitoring and real-time data collection.

Future research should also focus on meeting regulatory requirements and establishing standardized protocols to ensure smooth interoperability between different healthcare systems worldwide. Improving the usability and design of user interfaces will also play a crucial role in increasing acceptance among both patients and medical professionals. Furthermore, adopting advanced privacy-preserving techniques such as homomorphic encryption and zero-knowledge proofs can strengthen data protection. Overall, continuous innovation and research will contribute to building a more efficient, secure, and widely applicable blockchain-based healthcare solution.

References

1. Haddad, M. H. Habaebi, M. R. Islam, and N. F. Hasbullah, “Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems,” IEEE Access, 2022.
2. S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, “Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey,” Computers & Security, vol. 97, 2020.
3. Dubovitskaya et al., “Secure and Trustable Electronic Medical Records Sharing using Blockchain,” IEEE, 2017.
4. A. Abdellatif et al., “SSHealth: Toward Secure, Blockchain-Enabled Healthcare Systems,” IEEE, 2020.
5. M. A. Al-Khasawneh et al., “A Secure Blockchain Framework for Healthcare Records Management Systems,” IEEE Healthc. Technol. Lett., 2024.
6. P. Singh et al., “A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications,” IEEE Trans. Ind. Informatics, vol. 17, no. 8, 2020.
7. AlOmar et al., “A Transparent and Privacy-Preserving Healthcare Platform Using Blockchain,” IEEE Access, vol. 9, 2021.
8. AlMamun et al., “Blockchain-Based Electronic Health Records Management: A Comprehensive Review,” IEEE Access, vol. 10, 2022.
9. Y. Liu et al., “Blockchain Bridges Critical National Infrastructures: E-Healthcare Perspective,” IEEE Access, vol. 10, 2022. \
10. Alzahrani et al., “Framework for Secure Data Sharing Using Blockchain in Healthcare,” IEEE Access, vol. 10, 2022.
11. F. Cheng et al., “Blockchain-Based Data Explanation Models for Healthcare,” IEEE Trans. Visualization and Computer Graphics, 2021.
12. X. Ge et al., “Verifiable Keyword Search for Secure Healthcare Data Sharing,” IEEE Trans. Ind. Informatics, 2022.
13. Y. Sun et al., “Privacy-Preserving Medical Record Searching Scheme,” IEEE Trans. Ind. Informatics, 2022.
14. Ray et al., “Blockchain-Based EHR Service Scheme in IoT Healthcare,” IEEE Internet of Things Journal, 2021.

15. Itoo et al., “Blockchain-Based Key Agreement Protocol for Cloud Medical Infrastructure,” IEEE Access, 2022.
16. “Securing Patients’ Healthcare Records Using Blockchain-Based Smart Contracts,” IEEE Conference, 2024.
17. “Sec-Health: A Blockchain-Based Protocol for Securing Health Records,” IEEE Journal, 2023.
18. T. Kenaza et al., “Secure and Interoperable Architecture for Electronic Health Record Access Control,” 2026.
19. Agbeyangi et al., “Blockchain Implementation for Electronic Health Records Using Hyperledger Fabric,” 2024.
20. IEEE SmartBlock4Health Conference, “Blockchain Bridge Architecture for Healthcare Interoperability,” 2025.
21. “MedRSS: Blockchain-Based Secure Storage and Sharing of Medical Records,” Computers & Industrial Engineering, 2023.
22. “A Secure Blockchain-Based E-Health Records Storage and Sharing Scheme,” J. Info. Security and Applications, 2020.
23. H. Ghayvat et al., “Secure Healthcare Information Storage Using Blockchain and IoT,” IEEE Trans. Industrial Informatics, 2022.
24. P. Bhattacharya et al., “Blockchain-Based Deep Learning as a Service in Healthcare,” IEEE Trans. Network Science, 2019.
25. U. Usharani and G. Attigeri, “Secure EMR Classification Using MapReduce,” IEEE Access, 2022.
26. K. Zhang et al., “Blockchain-Based Secure Data Sharing in Healthcare Systems,” IEEE, 2021.
27. L. Esposito et al., “Blockchain: A Panacea for Healthcare Cloud-Based Data Security,” IEEE Cloud Computing, 2018.
28. Q. Xia et al., “MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain,” IEEE Access, 2017.
29. M. Shen et al., “Secure Data Sharing in Medical Systems Using Blockchain,” IEEE Network, 2019.
30. J. Zhang et al., “FHIRChain: Applying Blockchain to Securely Share Clinical Data,” IEEE, 2018.