International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(14s) 2026 pp. 386-400
https://doi.org/10.70917/ijcisim-2026-4238
Article

# Heterogeneous Medical Health Record (MHR) Sharing using Blockchain Technology

**Kala L[1]*, A. Rajesh[2]**

[1]Department of Computer Science and Engineering, JAIN (Deemed-to-be-University),Bangalore, Karnataka, India.
Email: kalachandru84@gmail.com
[2]Department of Computer Science and Engineering, JAIN (Deemed-to-be-University),Bangalore, Karnataka, India.
Email :a.rajesh@jainuniversity.ac.in
***Corresponding Author:** Kala L

**Abstract:** The secure and efficient sharing of medical health records across diverse healthcare systems remains a significant challenge due to data fragmentation, varying data standards, and concerns over privacy and interoperability. Heterogeneous medical health record sharing using blockchain technology presents a promising solution by enabling decentralized, tamper-resistant, and patient-centric data exchange across multiple healthcare providers. Leveraging the principles of heterogeneous blockchain systems, this approach facilitates interoperability between different electronic health record (EHR) platforms while maintaining data integrity, security, and compliance with regulatory standards such as HIPAA and GDPR. By utilizing smart contracts, permissioned blockchains, and cross-chain communication protocols, healthcare providers can share patient data in real-time without compromising confidentiality or ownership. This abstract explores the architecture, key components, benefits, and implementation challenges of such a system, highlighting its potential to transform healthcare data management through improved coordination, reduced administrative overhead, and enhanced patient outcomes.

**Keywords**: Blockchain, heterogeneous Healthcare, Integrity, decentralized ,Byzantine Fault Tolerance, Security Analysis..

## 1. INTRODUCTION

Blockchain is a distributed ledger technology (DLT) that makes it possible to record transactions over a decentralized network in a safe, transparent, and unchangeable manner. In contrast to conventional centralized systems, blockchain uses consensus methods and cryptographic algorithms to confirm and record data, doing away with the requirement for a reliable third party.

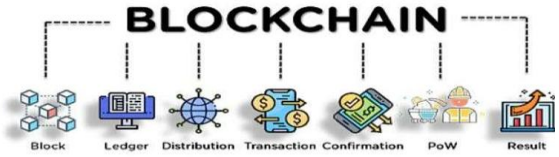



**Figure 1: Blockchain**

A blockchain is made up of a series of blocks, each of which holds a list of transactions and is connected to the one before it by a cryptographic hash. The technology is extremely secure and unchangeable since once data is captured, it cannot be changed without also changing all subsequent blocks. With the introduction of Bitcoin in 2009, blockchain became well-known, but its uses have since grown beyond cryptocurrencies. It is currently being investigated in a number of industries, such as healthcare and finance supply chain, voting systems, and identity management, thanks to its abilityto provide trust, traceability, and automation through smart contracts.

The key characteristics of blockchain include:

**Decentralization** – No single point of control or failure.

**Immutability** – Records cannot be altered retroactively.

**Transparency** – All participants have access to a shared ledger.

**Security** – Uses cryptography and consensus algorithms (e.g., Proof of Work, Proof of Stake) to secure data.

As the technology matures, blockchain is increasingly being integrated with other emerging technologies such as AI, IoT, and cloud computing to build innovative and trustworthy systems for the digital age.

## 2. Introduction to a heterogenous MHR Sharing System using Blockchain

The capacity of various blockchain networks to interact, exchange data, and communicate with one another is known as blockchain interoperability. Transferring assets, data, and value between various blockchain platforms which may have different protocols, consensus processes, and structures is made possible by this capability.

The Heterogeneous Medical Health Record (MHR) Sharing System leverages the power of blockchain technology to revolutionize the landscape of healthcare data management. Rooted in decentralization, this innovative solution harnesses the Ethereum network and IPFS (Interplanetary File System) technology to establish a secure and transparent framework for managing Electronic Medical Records. At its core, this system ensures that individuals have unparalleled control over their sensitive medical data. By utilizing blockchain, a distributed and tamper-resistant ledger, the platform guarantees the integrity and privacy of electronic health records. Access to these records is restricted to only authorized individuals and registered medical institutions, fostering a highly secure and permissioned environment. The integration of Ethereum network and IPFS introduces a robust and scalable architecture, addressing challenges in traditional MHR systems. This cutting-edge approach not only enhances data security but also facilitates seamless and efficient sharing of medical information. Patients can trust that their records are accessible only to those with legitimate authorization, ensuring confidentiality and compliance with privacy standards. In essence, the Heterogeneous MHR Sharing System signifies a paradigm shift in healthcare data management, empowering individuals with ownership of their health information while establishing a network of trust among authorized entities in the medical ecosystem.

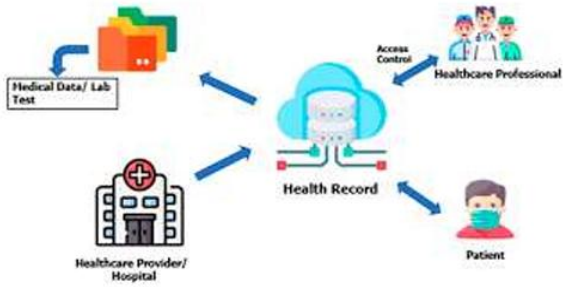



**Figure 2: MHR Sharing System using Blockchain architecture**

## 3. Literature Survey

First , Distributed BIM data sharing system architecture[1] based on blockchain technology is suggested. Second, shared usage of digital resources like rail transit BIM models and on-chain protection are the goals of smart contracts. Third, we develop a prototype of a trusted shared access system with permission control for several departments based on the InterPlanetary File System (IPFS) and the security features of Software Guard Extensions (SGX), and we suggest a BIM data access control mechanism based on attribute-based encryption.

In Paper [2] The proposed mechanism enables secure, efficient, and trustworthy medical data sharing in 6G-IoT healthcare networks while preserving patient privacy and ensuring data reliability across heterogeneous healthcare environments. Compression methods could streamline the processing of large volumes of medical imaging data. To this end, machine learning techniques could enhance the selection process for consensus nodes by tailoring it to historical operational data.

In paper [3] A simulated car monitoring system is coupled with an Internet of Things application. Data storage anonymity is achieved through the use of secure hash algorithms (SHA) and pentatope-based elliptic curve encryption. Technical data, vehicle replies, integrity, and authentication are all stored on the cloud platform. BCN-based transactions also utilize the Ethbalance MetaMask wallet. Clearly, the recommended method helps avoid a number of attacks on sensitive data, including ciphertext and plaintext assaults. In terms of operational cost (2.95 units), scalability (14.98 units), dependability (96.07%), and stability (0.82), the results show the efficacy and safety of the proposed method when compared to the state-of-the-art procedures.

The paper [4] outlines the state of interoperability solutions that have been suggested for blockchain systems that are heterogeneous. Interoperability options are examined for both generic data-based use cases and cryptocurrency. Heterogeneous blockchain interoperability's current open problems are discussed. Furthermore, a few potential research avenues are offered to improve and expand the current blockchain interoperability solutions. It was found that while many solutions have been suggested in the literature, very few have been put into practice in the actual world. The advancement of interoperability has been hampered by the absence of blockchain-specific standards. Additionally, it was discovered that the majority of the suggested solutions were created with cryptocurrency-based applications in mind.

In paper[5] Cross-chain interoperability is difficult to achieve since different IoT networks employ distinct blockchain topologies. The effectiveness of blockchain technology is still a worry, even though it has guaranteed the confidentiality and integrity of IoT data transfers. We suggest a real-time cross-chain transaction system for IoT data sharing in an IoT context as a solution to these problems. The real-time security issues related to cross-chain data interactions are the focus of our plan. First, we used a smart contract model based on collateral and challenge mechanisms to create a safe and equitable resolution process. Additionally, in order to lessen dependency on third-party security assumptions, cryptographic tools are used to improve the expressive capabilities of weakly secure service providers.

In paper [6] Organizations that use digital platforms to accomplish common objectives are referred to as Collaborative Enterprises (CE). The potential of Distributed Ledger Technologies (DLT), like blockchain, in CE depends on how well they can interface with existing technologies to enhance organizational operations. However, a fundamental problem that hinders the widespread use of blockchains in CE is the incapacity of several blockchains to connect with one another. In order to facilitate DLT interoperability and compatibility inside CE, this study offers a standardized architecture.

In Paper [7] The ability to transform international data exchanges and data centers by facilitating safe, decentralized, and effective data sharing across many networks and businesses could be the focus of future research. Global data exchanges might be built on optimal blockchain interoperability, which would increase the effectiveness and transparency of data transfers while lowering the dangers of centralization and data breaches.

The seamless transfer of data between various industries is made possible by interoperability between blockchain networks, which also makes it possible to establish international exchanges that facilitate the transfer of value and data between various sectors and geographical areas. Blockchain interoperability, for instance, would make it easier to establish a worldwide health data exchange, allowing for the safe and decentralized interchange of patient information and medical records among various healthcare providers and geographical areas . Blockchain interoperability can boost international data flows as well as the effectiveness and security of global data centres. Blockchain interoperability can lower the dangers of centralized data storage and increase data centres' resistance to cyberattacks and data breaches by facilitating safe, decentralized access to data across many networks. Additionally, interoperability can improve data management's accountability and transparency, allowing for more effective and efficient data centre monitoring and auditing.

In paper [8] interoperability is a critical feature that enables different agencies to work together effectively. To achieve this, blockchain technology provides a decentralized platform that ensures the verifiability and immutability of all data and communication exchanged between different parties. This can help to build trust and promote collaboration between agencies. In addition, smart contracts can be used to facilitate interoperability by automating the exchange of data between different systems. For example, a smart contract could be programmed to send data from one organization's system to another when a certain trigger condition is met, such as the detection of a potential hazard. This automated process could enable emergency responders to respond to emergencies quickly and effectively.

This paper [9] examines the power dispatching system's block chain cross chain interaction technology, evaluates the primary block chain cross chain technology and its features, suggests a block chain cross chain technology scheme for the dispatching field, and puts the data cross chain interaction between homogeneous and heterogeneous block chains into practice.

The paper [10] presents the heterogeneous privacy-preserving blockchain-enabled federated learning (HPP-BEFL) system, designed to enhance privacy, security, and efficiency in social fintech applications. In response, a novel PKI and identity-based heterogeneous authenticated asymmetric group key agreement (PKI-IB-HAAGKA) protocol was proposed, which resolves crypto system heterogeneity issues. What's more, a PKI and identity-based heterogeneous batch multisignature (PKI-IB-HBMS) was proposed as a building block of PKI-IB-HAAGKA. It effectively mitigates man-in-the-middle and inference attacks while improving overall system performance. Through security analysis and experiment results, it is demonstrated that the proposed PKI-IB-HAAGKA, PKI-IB-HBMS, and HPP-BEFL are provably secure and highly efficient, which can be applied to large-scale heterogeneous privacy-preserving model training scenarios.

This paper[11] examines current domestic and international research on the unified abstraction of heterogeneous blockchain data structures, transformation of smart contracts, proof of data existence, and other technologies. It focuses on fundamental issues like cryptography algorithms, smart contracts, and blockchain data structures, and proposes the technology of transferring heterogeneous blockchain block and transaction data, smart contract code, and status data in order to offer solutions for the issue of heterogeneous blockchain data migration and encourage the advancement of blockchain technology.

In this paper[12], we propose a patient-centric approach for automated medical record exchange that ensures secure data transfer, maintains patient anonymity, and reduces administrative overhead, thereby enabling efficient data sharing across institutions. We implement this approach through a system that leverages blockchain technology with smart contracts for immutable tracking of user actions and automated access permission handling, while specialized database ensures real-time performance, scalability, and flexible off-chain storage for diverse EHR formats.

This paper [13] suggests a decentralized architecture intended to improve access control and data sharing security in untrusted cloud environments. Our method presents a decentralized system for trust-based authentication and authorization and uses blockchain technology to create a transparent and unchangeable record for data transfers. To safeguard cloud-stored data from a variety of attack methods, the architecture incorporates multiple strong encryption algorithms. Before being uploaded to the Interplanetary File System (IPFS), files are locally encrypted using the Advanced Encryption Standard (AES), and their information is stored on the blockchain through smart contracts. Replay attacks are prevented and illegal data alterations are detected by a data verification technique based on timestamps and the Elliptic Curve Digital Signature Algorithm (ECDSA).

The focus of a research paper[14] is on the deployment of Smart Contracts along with blockchain technologies. The fundamental vision is to improve healthcare infrastructure's security. Blockchain is transforming healthcare systems for the better by eliminating inefficiencies caused by fraud and outdated technologies, allowing for the efficient, transparent, and secure issuance of Smart Contracts. The challenges of confidentiality, data security, and access to relevant patient information for medical professionals have been a problem in the healthcare sector. Most of the existing EHR systems do not have adequate mechanisms for enforcing security access controls, which hampers cooperation between healthcare institutions. These security concerns pose risks for patients' privacy and cripple the adoption of modern information technology within the health sector. Simulation works shows that Transaction processing time in case of proposed model is below 1.5 second where as it is 2.5 in case of conventional model. Security breach probability of proposed model has been reduced to 0.05 that was 0.35 in case of conventional model. Data integrity verification time in case of proposed model is below 1.0 that is above 1.75 in case of conventional model. While with the existing Electronic Health Record (EHR) systems face limitations in security, privacy enforcement, and interoperability, this study addresses the lack of automated, decentralized access control mechanisms. It proposes a blockchain powered Smart Contract model to fill these gaps and enhance healthcare data governance and trust.

Thus, this study [15] aims to compare the development of interoperability frameworks for smooth data sharing between Australian and US healthcare systems. The study used a systematic review design, which uses the Preferred Reporting Items for Systematic Reviews and Meta-analyses (PRISMA) to conduct an organized, scientific literature review. According to the study, the US healthcare system is more fragmented than Australia's, with different degrees of interoperability between states and institutions. Despite being centralized, Australia's interoperability system

nevertheless faces certain difficulties. Among these difficulties are underutilization of current resources as a result of privacy regulations and administrative costs. It was discovered that US healthcare facilities use a variety of proprietary systems as their interoperability frameworks.In the meanwhile, fragmentation caused by clinical decision support systems (CDSS) frequently poses a problem for interoperability in Australian healthcare facilities. The analysis comes to the conclusion that both Australia and the United States have serious interoperability issues. Australia faces vendor control and policy mismatch, whereas the US has regulatory fragmentation. Therefore, it is advised that future frameworks focus on national alignment, regulatory uniformity, and utilizing cutting-edge technologies like blockchain technology for improved healthcare data interchange.

This paper[16] introduces a hybrid model combining Federated Learning (FL) and Blockchain technology to offer a decentralized, privacy-preserving approach for AI model training across multiple healthcare providers. The proposed framework uses smart contracts for adaptively dynamic patient consent and deploys adaptive optimization techniques, including asynchronous updates and gradient sparsification, while maintaining tamper-proof auditability via Blockchain. We evaluate our system in a multi-node cloud setting (Amazon Web Services Elastic Compute Cloud [AWS EC2]) using the Medical Information Mart for Intensive Care III (MIMIC-III) dataset and show that our model behaves similarly to centralized learning, having increased privacy and lowered communication overhead. The hybrid framework ensures responsible use of healthcare data following established Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) practices, bridging the gap between technological advancement and healthcare. The architecture lays the foundation for scalable, secure, and collaborative digital health ecosystems, promoting patient trust and regulatory compliance.

In this paper[17] all patients' EHRs (Electronic Health Records) are used and shared with different institutes and research facilities without their consent. To protect and overcome pitfalls of generic systems, we introduce a new hybrid system called Hybrid Patient Data Vault (HPDV). This hybrid system can help patients securely share their health information in a manner that could allow them to share only what is necessary or in need to-know basis. We detail the system's components, workflows, and emergency protocols, emphasizing patient-centric design. Through a STRIDE-based threat model and simulations of key metrics like transaction latency and ZKP generation time, we demonstrate HPDV's security and feasibility. Our evaluation shows it outperforms monolithic approaches in auditability and privacy, with ZKP proofs generated in under 7 seconds on standard devices. This work demonstrates a practical modern approach for secure, patient-controlled health data exchange.

Blockchain [18] has evolved from its initial use in cryptocurrency into a foundational infrastructure that enables secure, transparent, and decentralized applications across diverse domains such as finance, healthcare, supply chain management, and the Internet of Things (IoT). By integrating distributed ledgers, consensus protocols, and cryptographic primitives, blockchain eliminates the need for centralized intermediaries and provides tamper-resistant data sharing among untrusted participants. However, the technology faces persistent challenges, including scalability limitations, high energy consumption, privacy leakage, and a lack of interoperability among heterogeneous platforms. This survey presents a comprehensive review of blockchain technology, systematically examining the evolution of consensus mechanisms, scalability optimization strategies, and privacy-preserving frameworks. In addition, it highlights key application domains, industrial adoption trends, and the integration of blockchain with emerging paradigms such as artificial intelligence, federated learning, and edge computing. The paper further discusses open challenges related to performance, security, compliance, and socio-technical adoption, offering insights into the future research directions needed to enable secure, scalable, and sustainable decentralized systems.

Additionally, there are other fascinating areas for additional study in the crucial expanding field of blockchain interoperability and interoperability. The goal of future research is to use the created architecture in other fields, like smart city environments that link two distinct blockchain networks that offer digital services powered by digital assets and open data. This will act as a guide for future studies on interoperability and related problems within the blockchain ecosystem. Due to the incapacity of various blockchains to communicate with one another, blockchain architecture has limited usefulness in the creation of novel digital services. This is because different vendors and communication protocols are used by these blockchain systems. This may restrict the potential influence of the standardized design and has put pressure on the widespread implementation of blockchains in CE. Future research will therefore look for ways to deal with this crucial problem. More research is required to be used in other areas, even if the majority of potential interoperability and intraoperability technologies proposed within the standardized architecture are still in the early stages of development.

## 4. Proposed System

Our proposed approach cultivates a diverse inter-hospital MHR sharing system using blockchain technology. The main goal of this system is to make the transfer of Medical Health Records (MHRs) between healthcare facilities safe, effective, and compatible.

## *4.1 System Architecture*

The architecture of our proposed system consists of the following key components:

The proposed system architecture includes several essential components:
• Blockchain Centre: Operated by a public health facility, this blockchain center serves as the primary hub for the administration of medical and personal mobile devices. All patients and hospitals must register with the blockchain center, utilizing mobile devices and institutional medical devices to facilitate mutual verification.

Patient:The patient possesses a personal mobile device utilized for storing identification verification messages. Individuals utilize personal devices to authenticate their identity to both healthcare facilities and themselves during the process of obtaining medical care. The medical index of the hospitals previously visited by the individual is also stored on the personal mobile device, facilitating access for additional hospitals in the future.

Hospital A: The physicians there use medical devices to diagnose patients. When a patient exhibits symptoms, mutual authentication occurs between Hospital A and the patient. Hospital A has medical records on file on its system in addition to examining patients. Patients obtain diagnosis results from Hospital A, which they store on their mobile device along with the medical index.

Hospital B: The doctors there use medical devices to diagnose patients. When a patient comes to Hospital B for treatment of symptoms observed at Hospital A, both Hospital B and the patient mutually authenticate. Hospital A's medical index is obtained by Hospital B via the patient's mobile device. Hospital B receives the patient's medical records from Hospital A and stores them on its system following the diagnosis. Patients keep their medical index and the results of their diagnosis on the mobile device after receiving them from Hospital B.

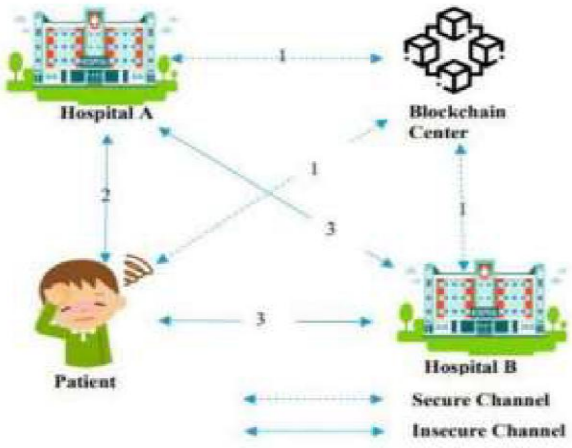



**Fig 3: Architecture of the Proposed System**

## *4.2 System Workflow*

The workflow of the proposed system is as follows:

The suggested system's workflow is as follows:

MHR Generation and Encryption: Newly created electronic medical records (MHRs) are encrypted for patient use in medical institutions using strong encryption techniques.

Decentralized Storage: The encrypted MHR is then routed to the system for decentralized storage.

View Request: A request for access to a person's electronic medical record (MHR) from another healthcare facility or other approved organization is made through the blockchain network.

Smart Contract Execution: Smart contracts in the blockchain confirm access requests in compliance with predetermined rules and authorization.

Decryption: Following validation, the necessary MHR is encrypted and delivered to the designated individual.

Data Exchange: A designated person may access, modify, or add new data to the MHR as needed.

On the blockchain, every transaction is documented for accountability and transparency.

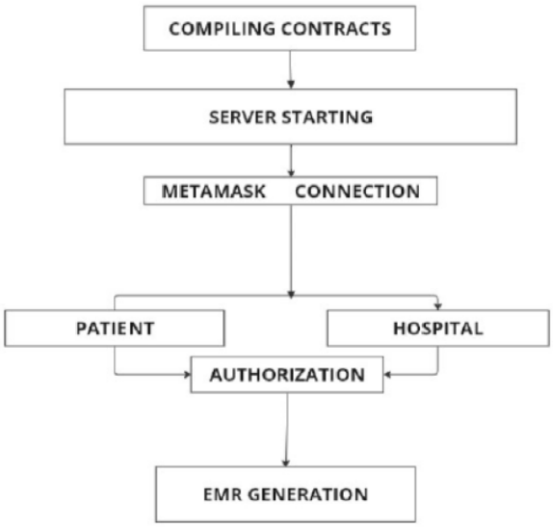



**Fig 4: System Workflow**

## 5. Implementation

The following security and privacy features are included in our system:

### *5.1 Encryption:*

Before being stored, MHRs are encrypted, and in order to decrypt the data, access authorization is needed.

**The Encrypt algorithm** secures plaintext MHRs using the Advanced Encryption Standard (AES) encryption algorithm with a secret key. AES is chosen for its strong encryption capability and efficiency. AES encryption involves a series of transformations, including substitution, permutation, and mixing, which convert the plaintext into a seemingly random ciphertext.

Function:

*function Encrypt(plaintext, key):*

*ciphertext = AES_encrypt(plaintext, key)*

*return ciphertext*

• Input: plaintext (MHR data), key (secret encryption key).

• Output: ciphertext (encrypted MHR data).


Implementation in MHR Sharing System:

• Data Creation/Update: When an MHR is created or updated at a hospital, the plaintext MHR data is first encrypted using AES with a unique encryption key specific to that hospital.

• Storage on Blockchain: The resulting ciphertext is then stored on the blockchain. This ensures that even if unauthorized parties gain access to the blockchain, they cannot read the MHR data without the encryption key.

**The Decrypt algorithm** converts ciphertext MHRs back into plaintext using the AES decryption algorithm with the secret key. The decryption process is essentially the reverse of the encryption process.

• Function:

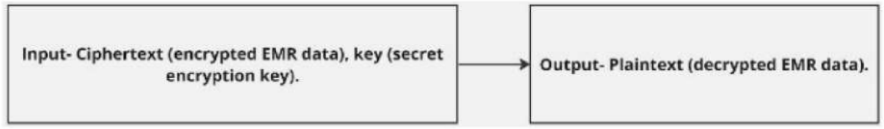
*function Decrypt(ciphertext, key):*

*plaintext = AES_decrypt(ciphertext, key)*

*return plaintext*

• Input: ciphertext (encrypted MHR data), key (secret encryption key).

• Output: plaintext (decrypted MHR data).




Implementation in MHR Sharing System:

• Data Retrieval: When a hospital requests access to a patient's MHR, the encrypted ciphertext is retrieved from the blockchain.

• Decryption: The hospital uses its unique decryption key to convert the ciphertext back to the readable plaintext MHR data. This ensures that only authorized hospitals can access the actual medical data.

**Access control:** Only certified persons are able to read or alter MHRs thanks to the enforcement of access control restrictions using smart contracts.

**The Access Control** algorithm verifies the permissions of a hospital to access a patient's MHR. Permissions are validated based on predefined access control policies.

• Function:

*function AccessControl(patientID, hospitalID, permissions):*

*if ValidatePermissions(patientID, hospitalID, permissions):*

*GrantAccess()*

*else:*

*DenyAccess()*

• Input: patientID (ID of the patient), hospitalID (ID of the hospital), permissions (requested access permissions).

• Output: GrantAccess (if permissions are valid), DenyAccess (if permissions are invalid).


Implementation in MHR Sharing System:

• Permission Validation: When a hospital requests access to a patient's MHR a smart contract on the blockchain checks if the hospital has the necessary permissions. These permissions could be based on roles, patient consent, and legal requirements.

• Access Decision: If the permissions are valid, access to the MHR is granted; otherwise, it is denied. This ensures that only authorized entities can access or modify MHRs.

**The Sign algorithm** generates a digital signature for MHR data using the Elliptic Curve Digital Signature Algorithm (ECDSA) with a private key. ECDSA ensures that the signature is unique to both the data and the private key used to sign it.

• Function:

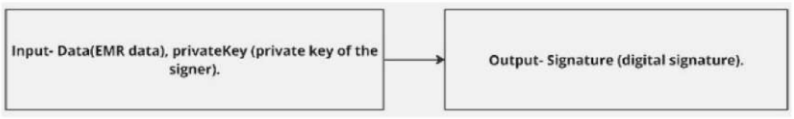
*function Sign(data, privateKey):*

*signature = ECDSA_sign(data, privateKey)*

*return signature*

• Input: data (MHR data), privateKey (private key of the signer).

• Output: signature (digital signature).




Implementation in MHR Sharing System:

• Data Integrity and Authentication: When an MHR is created or modified, the hospital signs the data using its private key. This digital signature is then stored along with the MHR on the blockchain.

• Proof of Origin: The digital signature provides proof that the data was generated by the hospital and has not been tampered with.

**The Verify algorithm** checks the authenticity of MHR data using the ECDSA verification algorithm with the public key of the signer. Verification ensures that the data has not been altered and that the signature is valid.

• Function:

*function Verify(data, signature, publicKey):*

*if ECDSA_verify(data, signature, publicKey):*

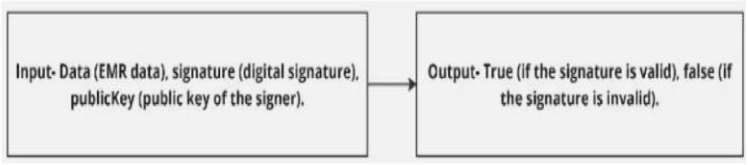
*return true*

*else:*

*return false*

• Input: data (MHR data), signature (digital signature), publicKey (public key of the signer).

Output: true (if the signature is valid), false (if the signature is invalid).




Implementation in MHR Sharing System:

• Signature Verification: When a hospital retrieves an MHR, the system verifies the digital

signature using the hospital's public key.

• Data Integrity Check: If the signature is valid, it confirms that the data has not been altered

since it was signed and that it originates from the correct hospital.

**The Hash algorithm** generates a hash value for MHR data using the SHA-256 hashing algorithm. A hash function produces a fixed-size string of characters that uniquely represents the data.

• Function:

*function Hash(data):*

*hashValue = SHA256_hash(data)*

*return hashValue*

• Input: data (MHR data).

• Output: hash Value (hashed value).

Implementation in MHR Sharing System:

• Data Integrity: When an MHR is stored on the blockchain, a hash of the data is also stored.

The SHA-256 hash serves as a digital fingerprint of the data.

• Tamper Detection: Any alteration in the MHR data results in a different hash value. By

comparing the stored hash with a freshly computed hash of the retrieved data, the system can

detect any tampering.

These algorithms collectively ensure the security and privacy of electronic medical records

in our blockchain-based inter-hospital MHR sharing system. The use of encryption and decryption algorithms protects data confidentiality, while access control algorithms ensure that only authorized entities can access sensitive information. Digital signatures and verification algorithms guarantee the authenticity and integrity of the data, and hashing algorithms provide a means for quickly verifying data integrity. By employing these algorithms, our system offers a robust framework for the secure and private sharing of sensitive medical information across hospitals.

## 6. Results

The implementation of the inter-hospital MHR sharing system using blockchain technology has resulted in a secure, transparent, and efficient mechanism for managing and sharing electronic medical records (MHR) among hospitals. By integrating MetaMask for secure user interactions, configuring Truffle for smart contract management, and utilizing Ganache for a local blockchain environment, we created a robust development and testing infrastructure. This setup allowed us to deploy three essential smart contracts.

By employing advanced cryptographic algorithms, including AES for encryption and decryption, ECDSA for digital signatures, and SHA-256 for hashing, the system ensures the confidentiality, integrity, and authenticity of medical records. This comprehensive security framework protects against unauthorized access, data tampering, and ensures the authenticity of records.

The outcome is a decentralized, blockchain-based MHR sharing system that significantly improves interoperability between hospitals while maintaining high standards of data security and patient privacy. This system not only streamlines the sharing of medical records but also builds trust among stakeholders by providing a transparent and tamper-proof record of all transactions. Overall, the project demonstrates the potential of blockchain technology to revolutionize healthcare data management by enhancing security, privacy, and efficiency in medical record sharing.

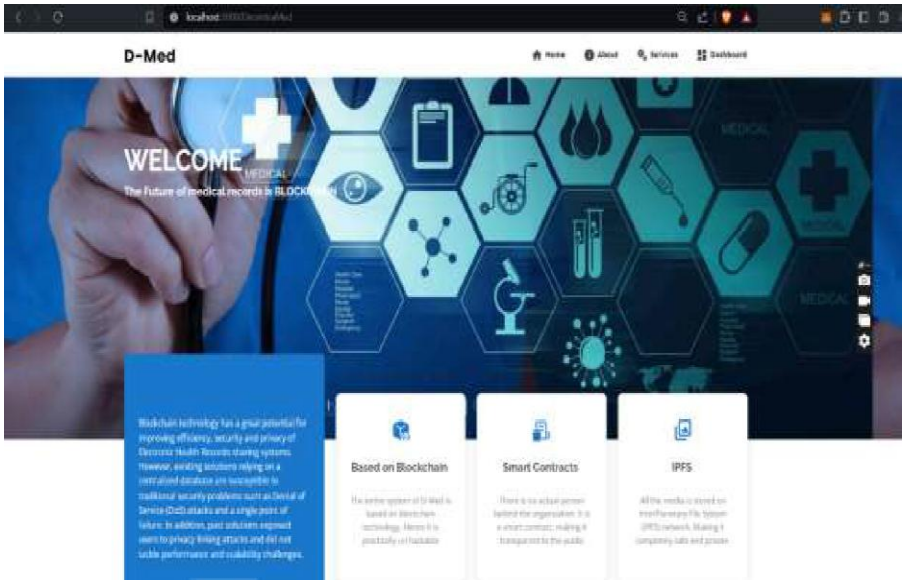



**Figure 5: Shows home page of the Hospital**

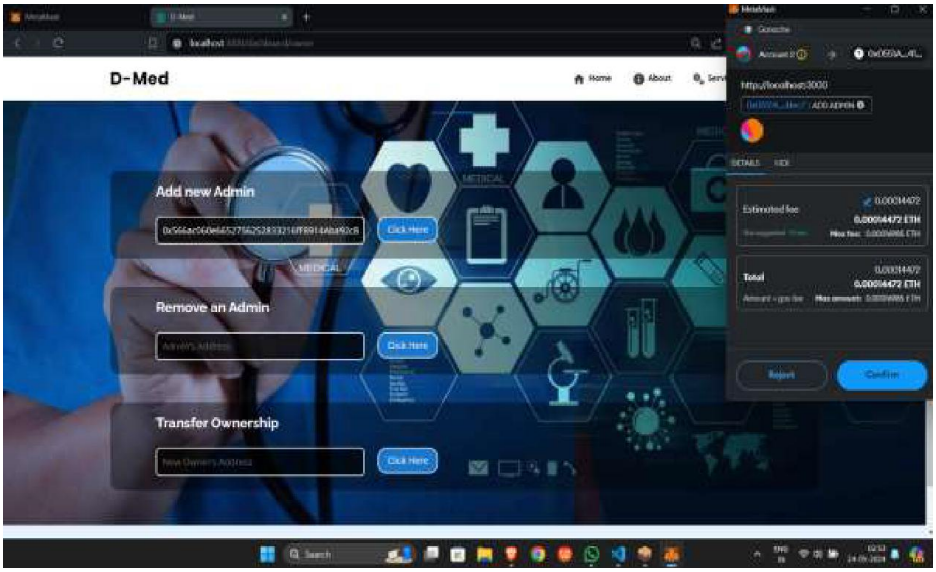



**Figure 6: Shows Owner's Dashboard**

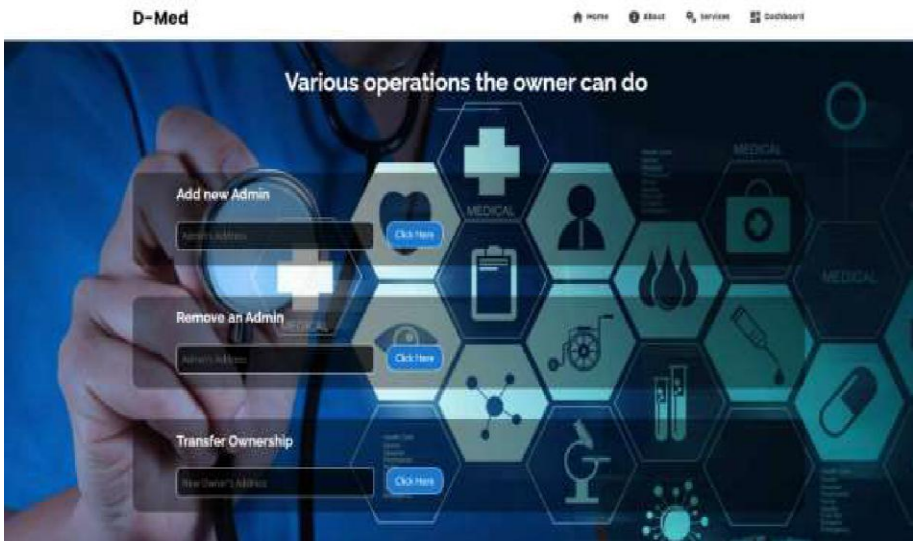



**Figure 7:Shows Owner's Dashboard Transaction**

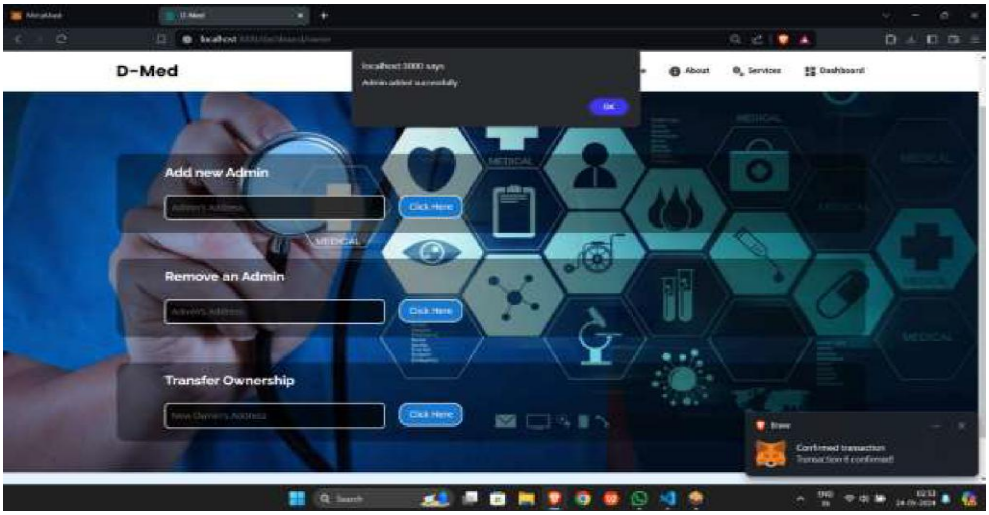



**Figure 8: shows Admin Addition Transaction**


**Figure 9: Shows the details of the admin and owner**


**Figure 10: shows the details of the Hospital enrolled in blockchain**

## 7. Conclusion

With the development of medical technology, the importance of medical data, including patient identities, payment histories, and medical records, has increased dramatically. It is now crucial to research patient privacy protection and medical data security. Additionally, under the current healthcare system, patients' medical records are not easily accessible between hospitals. This lack of interoperability leads to the underutilization of medical resources and needless examinations. Therefore, it is necessary to enable access to medical records between hospitals. Our study proposes a secure inter-hospital Medical Health Record (MHR) sharing system based on blockchain technology to address these problems. Given that hospitals and patients belong to the same group, our suggested method has the blockchain centre give identity verification keys to medical alliance members.

As a result, alliance members can lawfully communicate and share data, and patient medical records are accessible to all companies. This approach prevents medical resource waste while improving the efficacy and quality of medical care. We are certain that our proposed strategy satisfies a number of security requirements. When evaluated using the BAN logic proof model, the proposed approach performs well in terms of computing and communication costs. In conclusion, there is a growing likelihood that the medical sector will employ blockchain-based technology. Our proposed approach challenges the efficacy of blockchain transactions while simultaneously protecting individual privacy and facilitating the sharing of medical resources. This opens up possibilities for comparison blockchain-based systems in terms of performance assessment through further research.

**Future Enhancements**

To further improve the inter-hospital MHR sharing system, several future enhancements can be considered. First, scalability can be addressed by implementing techniques like sharding or sidechains, allowing the blockchain network to handle a larger volume of transactions. Second, interoperability can be enhanced by integrating with other healthcare systems and standards, such as HL7 FHIR, to facilitate seamless data exchange between different healthcare providers. Third, standardized data formats and protocols should be developed to ensure consistency and compatibility across different MHR systems, enabling easier data sharing and integration. Granular control over data access can also be obtained through more complex access control mechanisms like attribute-based access control (ABAC) or role-based access control (RBAC). Computation on encrypted data can be made possible via privacy-preserving methods like homomorphic encryption and zero-knowledge proofs, which allow data analysis without sacrificing privacy. Improved patient outcomes and healthcare decision-making can result from the integration of artificial intelligence (AI) and data analytics tools to extract insights from shared MHR data. By enabling patients to safely access and manage their medical records, mobile applications can be created, encouraging patient empowerment and engagement. Lastly, the implementation of suitable privacy rules and data protection mechanisms in conformity with healthcare standards, such as GDPR in the EU and HIPAA in the US, should guarantee regulatory compliance. By implementing these future enhancements, the inter-hospital MHR sharing system can become even more robust, scalable, and user-friendly, further advancing healthcare interoperability and patient care.

**FUNDING INFORMATION**

No funding involved

## AUTHOR CONTRIBUTIONS STATEMENT

| Name of Author | C | M | So | Va | Fo | I | R | D | O | E | Vi | Su | P | Fu |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Kala L | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | | |
| A Rajesh | | | | | ✓ | | | | | ✓ | | ✓ | | |

## CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

## DATA AVAILABILITY

Data supporting the findings of this study are available from the corresponding author upon reasonable request..

## BIOGRAPHIES OF AUTHORS

**Kala L,** was born in Bangalore, India in the year 1984.She completed her Bachelor of Engineering (B.E) Degree in Information Science and Engineering in Vivekananda Institute of technology Bangalore, India in 2005 .She completed her Master of Technology (MTech) degree In Computer Science and Engineering in RV College of Engineering in 2011 and Pursuing PHD in Computer Science and Engineering in 2014. She is a research scholar in the Department of Computer Science and Engineering , in Jain University, Bangalore, Karnataka, India. And also Working as Assistant Professor in Department of Computer Science and Engineering in R V College of Engineering, Bangalore, Karnataka, India. She is a life member of International Association of Engineers IAENG and Quality Circleforum of India(QCFI). Her area of interest is Image processing, Artificial Intelligence, Blockchain Technology, Network Security. She may be contacted at email: kalacl@rvce.edu.in.

**Rajesh Appusamy** Dr. A. RAJESH, was born in Salem, India in the year 1973. He completed his B.E degree in Electronics and Communication Engineering from Government College of Engineering, Salem, India in 1997. He completed his M.E degree in Computer Science and Engineering from Sathyabama Institute of Science and Technology, Chennai, India in 2005. He received his PhD degree in Computer Science and Engineering from Dr. MGR Educational and Research Institute, Maduravoyal , India in 2011. He started his career as a Commissioning cum Service Engineer in Electronics Consultancy and Engineering Services, Chennai in 1997. Later he joined C .Abdul Hakeem College of Engineering and Technology as Lecturer in the department of Computer Science and Engineering in 2000. He went on to become the Head of Computer Science and Engineering in 2006. Under his leadership the department was accredited twice by National Board of Accreditation for the duration 2007 – 10 and 2013 – 15. As HOD of CSE he also actively participated and contributed in the accreditation of the institution by NAAC with A Grade for the duration 2015 – 2019. Later, he took charge as the Principal of the institution in 2015. He contributed to the development and growth of the institution as Principal till 2020. He joined Jain University, Bangalore, India as Professor in the department of Computer Science and Engineering in 2020. Since then he has taken up various roles such as Program Coordinator BTech and MTech AI, Deputy HOD CSE and is currently the Program Head of CSE AI. He has published around 71 research papers in Peer-reviewed/Scopus/SCIE indexed journals. He has also published 9 books and 5 patents. He has produced 10 Doctorates under his guidance. His research interests include Intelligent

| | |
|---|---|
| | Systems, AI, Machine Learning, Deep learning, and Data mining . He may be contacted at Email: a.rajesh@jainuniversity.ac.in |

**References:**


1. Xiaogang Wang, Chenhao Wang, Jie Yang, Jianhai Chen, Xiang Chen, Gang Li, Butian Huang, and Shoujun Peng, "A blockchain-based trusted sharing method for railway transportation BIM data," Blockchain: Research and Applications, vol. 6, no. 3, Sep. 2025.
2. Qiang Zhang, Xingsi Xue, and Jing Yang, "Blockchain-Enabled Trustworthy Healthcare Data Sharing Mechanism for Reliable 6G-IoT Networks," IEEE Internet of Things Journal, 2025.
3. Abdullah Aljumah, Tariq Ahamed Ahanger, and Imdad Ullah, "Heterogeneous Blockchain-Based Secure Framework for UAV Data," Mathematics, vol. 11, p. 1348, 2023.
4. Seth Djanie Kotey, Eric Tutu Tchao, Abdul-Rahman Ahmed, Andrew Selasi Agbemenu, Henry Nunoo-Mensah, Axel Sikora, Dominik Welte, and Eliel Keelson, "Blockchain interoperability: the state of heterogeneous blockchain-to-blockchain communication," IET Communications, vol. 17, pp. 891–914, 2023.
5. Zhikai Lin, Kexing Wang, Yongdong Wu, and Dingcheng L., "Fast payments across heterogeneous blockchains for Internet of Things," IEEE Access, vol. 11, 2023.
6. Bokolo Anthony Jnr, "Enhancing blockchain interoperability and intraoperability capabilities in collaborative enterprise—a standardized architecture perspective," Enterprise Information Systems, vol. 18, no. 3, pp. 297–337, 2024.
7. "The current state of interoperability between blockchain networks," EU Blockchain Observatory and Forum, 2023.
8. Blockchain Technology for Public Safety: An IEEE Public Safety Technology Initiative Report, 2024.
9. Xiong Wan, Lei Guo, Can Cui, Fangchun Di, Lei Tao, and Qiong Feng, "Research on blockchain cross chain interaction technology suitable for power dispatching system," IEEE Conference, Jan. 26, 2023.
10. Hu Xiong, Ye Xia, Yaxin Zhao, Abubaker Wahaballa, and Kuo-Hui Yeh, "Heterogeneous Privacy-Preserving Blockchain-Enabled Federated Learning for Social Fintech," IEEE Transactions on Computational Social Systems, Feb. 13, 2025.
11. Yutong Xie, Shuai Chen, and Xinnan Wang, "Research Progress of Heterogeneous Blockchain Data Migration Technology," in Proceedings of the 4th International Conference on Economic Management and Model Engineering (ICEMME 2022), pp. 548–554.
12. Vladimir Jovanović, Nikola Todorović, Miroslav Tomić, Milan Čeliković, and Vladimir Dimitrieski, "A Blockchain-Based Software System for Automated Medical Record Exchange," 2025.
13. Houaida Ghanmi, Nasreddine Hajlaoui, Haifa Touati, Saadi Boudjit, Mohamed Hadded, and Paul Muhlethaler, "A blockchain-based framework for secure data sharing and access control using IPFS and ECC," Cluster Computing, Springer Nature, Oct. 2025.
14. Dr. Naim Shaikh, Dr. Mamatha G., Kukati Aruna Kumari, Dr. M. S. Giridhar, Dr. Krishna Nand Mishra, Dr. A. Pankajam, Dr. Ganesh Kumar R., and Swati Gupta, "Journal of Theoretical and Applied Information Technology," vol. 103, no. 19, Oct. 15, 2025.
15. Qazeem Faniran, "Analyzing the Progress of Interoperability Frameworks in Enabling Seamless Data Exchange across Healthcare Systems in the US and Australia," JMSCR, vol. 13, no. 7, Jul. 2025.
16. Amrutha B. K. and B. Gomathy, "Hybrid Blockchain Federated Learning Framework for Privacy-Preserving, Scalable and Ethical AI in Multiprovider Healthcare Networks," in 2025 International Conference on Next Generation Computing Systems (ICNGCS), Aug. 21–22, 2025.
17. Sahil Fruitwala and Purva Desai, "A Proposed Hybrid Blockchain-DID-ZKP Approach to Secure, Auditable, and Private Healthcare Interoperability," The American Journal of Engineering and Technology, vol. 7, no. 10, 2025.
18. Corwin Desrosiers, "From Distributed Consensus to Privacy-Preserving Federated Learning: Technical Advances and Open Challenges in Blockchain Systems," Journal of Computer Technology and Software, ISSN: 2998-2383, vol. 4, no. 9, 2025.