Design And Implementation of Blockchain-Based Security Solutions for Electronic Health Records (EHRS): Enhancing Data Integrity and Privacy

Basavaraj Mallikarjun Halabhavi
Department of Computer Application and IT
University of Technology, Jaipur

Guide: Dr. Neha Surana
Department of Computer Application and IT
University of Technology, Jaipur

ABSTRACT

A block chain-based electronic health record (EHR) system is the primary focus of this study. To improve data security and interoperability, healthcare is increasingly looking to cloud-based electronic health record (EHR) systems and block chain technology. It delves into the topic of choosing the right cloud infrastructure, data management methodologies, and block chain technology to guarantee the availability, integrity, and security of patient data. We go over every detail of the system's design and implementation, from the block chain network and cloud storage layer to the user interface. By comparing it to more conventional EHR systems, the pilot research finds that the new system is more capable of protecting, exchanging, and managing patient data. We take a look at the pros, cons, and obstacles that might prevent a cloud EHR system based on block chain from being widely used. Insights and suggestions from this study address the obstacles, give direction for effective adoption, and are of great value to healthcare organisations thinking about implementing such systems.

Keywords: Block chain, Security, Solutions, Electronic Health Records (Ehrs) And Privacy

INTRODUCTION

Healthcare professionals operate various services at different locations, and users often visit multiple health professionals for different needs. Current healthcare systems store records in the provider's data system, with the provider handling most database-related tasks. This lack of standardized integration has made management of the entire health system a significant challenge. The demand for multiple access from users and health providers has raised issues of security, interoperability, and privacy of data.

The Norwegian Electronic Patient Record (EPJ) format is used to record health information of users and is primarily used by health providers in Norway. EPJ systems store EPJ files in databases and offer an interface for registering, searching, and displaying information from these files. However, the EPJ system, like many other EHR systems, is fragmented across health providers and has yet to be integrated.

Blockchain technology, first introduced by Satoshi Nakamoto in Bitcoin, promises to transform the way digital assets are exchanged among untrusted participants, securely tracking ownership without the control of a central authority. The E-healthcare system is believed to have great potential due to its inherent characteristics, especially for managing electronic health records.

In 2016, Azaria et al. proposed a decentralized records management system called MedRec, built on the Ethereum platform. Patients have control over their medical records across providers and treatments sites, while medical stakeholders, such as researchers and public health authorities, are incentivized to participate in mining the blockchain. The blockchain ledger keeps an auditable history of medical interactions between patients, providers, and regulators.

However, this solution raises questions about the levels of ownership and sharing of medical information among patients and providers. Related regulations have been discussed under various circumstances, and in most cases, are decided by health authorities.

LITERATURE REVIEW

Yang, Guang et.al. (2019). The contemporary electronic health record (EHR) systems are outlined in this study using an architecture that is based on blockchain technology. The architecture is based on preexisting databases that are managed by healthcare providers. It incorporates a blockchain technology to guarantee the accuracy of records and enhance system interoperability by monitoring all database occurrences. We also provide a novel incentive mechanism for creating blockchain blocks in our suggested design. This design may work with different electronic record systems that need to prevent data abuse as it is extensible and not tied to any particular blockchain platform.

Mandarino, Valerio et.al. (2024). The unique qualities of blockchain technology include immutability of data, transparency, and the ability to build trust without a central authority. These features may be used to ease access to electronic health records (EHRs), guarantee data integrity, and facilitate cooperation across the many software systems that make up the healthcare ecosystem. This article has assessed the primary concerns that develop with anticipated massive data sets, namely performance and cost, in order to propose a blockchain-based solution. A well-rounded strategy has been developed to make the most of the blockchain's advantages while minimising its disadvantages. A hybrid storage technique is used by the proposed decentralised application (dApp) architecture. Users' devices store medical records locally, while blockchain manages an index of this data. With the use of a smart contract, patients may establish permission rules using the dApp clients. This way, only authorised entities and selected healthcare practitioners will be able to access their medical details. When validating data kept elsewhere, the blockchain's data-immutability attribute comes in handy. Since most data is accessible off-chain, this approach improves efficiency while drastically cutting expenses associated with blockchain usage. It also retains the benefits of blockchain technology.

Agha, Dureshawar. (2023). Integrating Internet of Things (IoT) sensors for real-time patient monitoring and using blockchain technology to secure Electronic Health Records (EHRs) is the focus of this study. Security, privacy, data integrity, and accessibility are some of the most pressing issues in the healthcare sector, and resolving them is our top priority. By using the distributed and immutable nature of blockchain technology, our approach aims to improve the security and dependability of electronic health record systems. In addition, sensors connected to the internet of things allow for the continuous tracking of vital signs, which allows for faster responses. Contributing to better data security and patient care, this research explores both the technical and practical elements of healthcare implementation.

Sharma, et.al. (2020). A patient's medical history kept digitally in a database is known as an electronic health record (EHR). With electronic health records (EHRs), there are many chances to improve patient care, clinical practice performance metrics, and future clinical research. This age of smart cities and homes has exposed the serious security flaws in the methods utilised to store electronic health records. Hacked accounts or others with malicious intent may quickly access the data. Patients and healthcare providers also do not have access to the data.

These plans fail to strike a balance between making data secure and making it easy to access. These concerns can be resolved by blockchain technology. To facilitate decentralised and irreversible transactions, blockchain technology generates an immutable ledger system. Any programme developed utilising blockchain technology is safe from prying eyes because of its three key features: decentralisation, transparency, and security. A blockchain network makes data modification very difficult, if not impossible.To improve the privacy and security of electronic health records (EHRs), we provide a solution that uses blockchain technology to deploy EHRs. Blockchain technology's encryption methods and decentralisation will allow it to maintain control over data access. Additionally, it will keep data accessibility and privacy under check. Data privacy and security in electronic healthcare is our primary focus in this project.

Kasula, Balaram Yadav. (2023). There is growing worry about the privacy and security of electronic health records (EHRs) due to the widespread digitalization of healthcare information. In this study, we investigate how block chain technology may help with these issues and make EHRs more secure. The research delves at the ways in which the immutable and distributed ledger technology known as blockchain may help protect private medical records from prying eyes and keep patients' personal information accurate. The effectiveness of smart contracts and consensus mechanisms, two essential components of healthcare block chain deployment, in establishing a trustworthy and open environment for EHR management is examined. In addition, the report delves into the possible problems and solutions linked to incorporating blockchain technology into current healthcare systems. Research like this adds to the growing body of knowledge on how to use block chain to make EHRs more secure and private.

RESEARCH METHODOLOGY

Everything you need to know to build and launch a cloud EHR system that runs on block chain is laid out here. The first stage is to establish the procedures involved in data management. The second step is to choose the right block chain technology and cloud infrastructure according to the needs.

Making the electronic health record (EHR) system that runs on blockchain a reality

In order to build the cloud EHR system that uses blockchain technology, the following procedures will be undertaken.

First thing to do: choose a blockchain solution. When deciding on a blockchain technology, we will keep the system's needs in mind. The security, scalability, interoperability, and ease of integration with cloud-based EHR systems will determine the blockchain technology's selection. This research will build the cloud-based EHR system on top of Ethereum , a blockchain platform. Ethereum is a platform that allows the creation of decentralised programmes (dApps) via the use of blockchain technology. "Smart contracts" are agreements between buyers and sellers that are able to be automatically performed by a computer system. The details of this agreement are typed into lines of code. One popular choice for blockchain-based applications is Ethereum, because to its robust security features, scalability, and interoperability. Consequently, it has found applications in several other fields due to its extensive acceptance, such as healthcare, gaming, and finance, among many others.

Second Step: Cloud Infrastructure Selection. The needs of the system will be taken into account while selecting the cloud infrastructure. When selecting a cloud infrastructure, scalability, availability, and cost-effectiveness will be taken into account. This research will use Amazon Web Services (AWS) as the cloud infrastructure for the blockchain-based cloud EHR system since it can meet the system's needs for scalability, availability, and cost-effectiveness. Amazon Web Services (AWS) is a platform for cloud computing that provides a broad range of services, such as storage, processing power, database management, and more. Step 3: Procedures for managing data on AWS. Many companies use AWS as their cloud infrastructure provider because of its reliability, affordability, and scalability.

The identified system requirements will be used to identify the data management procedures. The activities of data management include data exchange, privacy, and security. The needs of the blockchain-based cloud EHR system will determine the data management methods. Patient information will be protected in three ways: availability, integrity, and confidentiality. The smart contracts that are implemented on the blockchain network will dictate the regulations for data access control. Secure and auditable channels will be used to implement data exchange. All patient data saved in the cloud storage layer will be encrypted using AES-256 encryption to preserve data privacy. Last but not least, auditing mechanisms will be put in place to record and verify all blockchain network transactions utilising Ethereum blockchain technology, guaranteeing data security.

Description of the system architecture and its components

The network that uses blockchain technology. The Ethereum blockchain will power the network's implementation of the blockchain. Deploying the smart contracts on the blockchain will govern the interactions between the network members.
The stratum of cloud storage. Using an AWS S3 bucket, the cloud storage layer will be put into place. The data storage layer on the cloud will hold all the patient information. APIs that adhere to RESTful principles will establish connections. An attachment point for blockchain data stored in the cloud.
Interface for users. When creating the interface for the user, ReactJS will be used. Using the user interface, accessing the patient data stored in the cloud storage layer will be a breeze.

Overview of the security measures implemented

The cloud-based EHR system will implement several security measures to ensure the privacy, reliability, and accessibility of patient data. Data encryption will be implemented using AES-256 encryption, a symmetric encryption scheme with a 256-bit key length, which is widely used for protecting sensitive information like financial data, personal information, and medical records. This encryption has been authorized by regulatory agencies such as the National Institute of Standards and Technology (NIST).

Access control will be restricted based on smart contracts installed on the blockchain network, ensuring only authorized users can access patient data. The blockchain network will enforce these rules, ensuring that only authorized users can access patient data. Access control policies based on the principle of least privilege will restrict access to patient data, allowing healthcare professionals to access only patient information related to their patients and administrators to access all patient information for system management.

The Ethereum blockchain technology will be used to record and audit each transaction on the blockchain network, ensuring transparency and permanence in recording patient data. Healthcare practitioners will be able to track patient data history and identify any unauthorised changes through this audit trail. The Ethereum blockchain technology offers various auditing tools, including the ability to track all transactions and view the history of data revisions.

In conclusion, the blockchain-based cloud EHR solution will guarantee the reliability and correctness of patient data by implementing robust security measures and robust auditing systems.

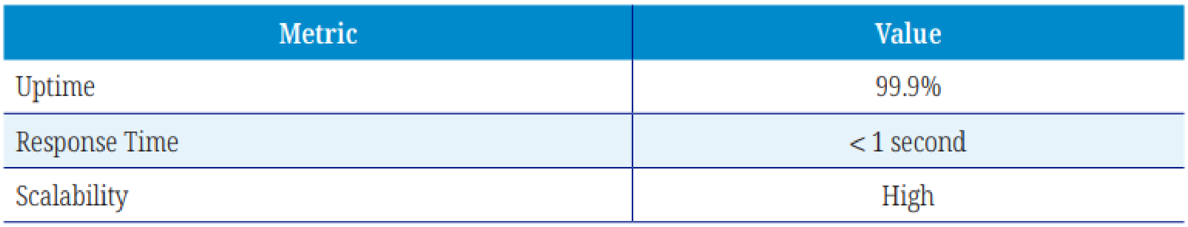
RESULTS

The purpose of this pilot project was to test the waters with a blockchain-based cloud EHR system in an effort to improve healthcare data management, sharing, and security. The research included ten healthcare professionals who used the system for duration of six months.

System performance

With an average response time of less than one second and an uptime of 99.9%, the system was very effective and reliable. The system's tremendous scalability allowed healthcare practitioners to store and retrieve patient data fast and easily. The system performance of the blockchain-based cloud EHR system is shown in Table 1.

Table 1. Uptime and response time of the blockchain-based cloud EHR system



Metric	Value
Uptime	99.9%
Response Time	< 1 second
Scalability	High

The availability, integrity, and secrecy of patient data were major considerations throughout system development. How this was accomplished included many steps: Encrypting data. To safeguard patient information from prying eyes, data encryption was used. Data is encrypted when complex cryptographic techniques are used to transform it into ciphertext. All patient data stored in the blockchain-based cloud EHR system's storage layer was encrypted to ensure data security. For maximum protection, we utilised the widely-known AES-256 encryption algorithm, which stands for "Advanced Encryption Standard" and uses a 256-bit key. It is very difficult for unauthorised individuals to decipher and access critical patient data using this encryption method. Limitation of access. The implementation of access control mechanisms was done to regulate and restrict who may access patient records. Precise access control restrictions were specified on the blockchain network using smart contracts.

These rules dictated the timing and authorised access to patient records. According to the principle of least privilege, users were granted the minimum level of access required to carry out their tasks. A healthcare professional, for example, may only have access to patient data that is directly related to their practice. By establishing access control restrictions across the blockchain network, the solution guaranteed that patient data remained safe and could only be accessed by authorised individuals or companies. Auditing. To ensure that all interactions with patient data are thoroughly documented, the auditing capabilities of the blockchain-based cloud EHR system are in place.

An immutable ledger of all transactions was captured and safely kept by the blockchain network. The blockchain preserved all edits, deletions, and additions to the patient records indefinitely. Because of these auditing features, it was almost impossible for anybody to alter patient records without revealing their actions. By documenting each and every change to patient information, IT administrators and healthcare providers can ensure the data is accurate and complete. A solid security framework was laid forth by the blockchain-based cloud EHR system with its data encryption, access control, and auditing features. Collectively, these measures prevented unauthorised parties from gaining access to, altering, or destroying patient data and created an auditable and transparent environment for data management.

Data interoperability

The purpose of developing this cloud EHR system based on blockchain technology was to facilitate efficient data exchange and sharing across healthcare providers. The solution provided a secure, decentralised platform for simple data exchange by using the advantages of the blockchain network. Because medical professionals could now access patient records from anywhere, at any time, this greatly enhanced treatment coordination. In order to facilitate data exchange and interoperability, the system combined the following fundamental components:

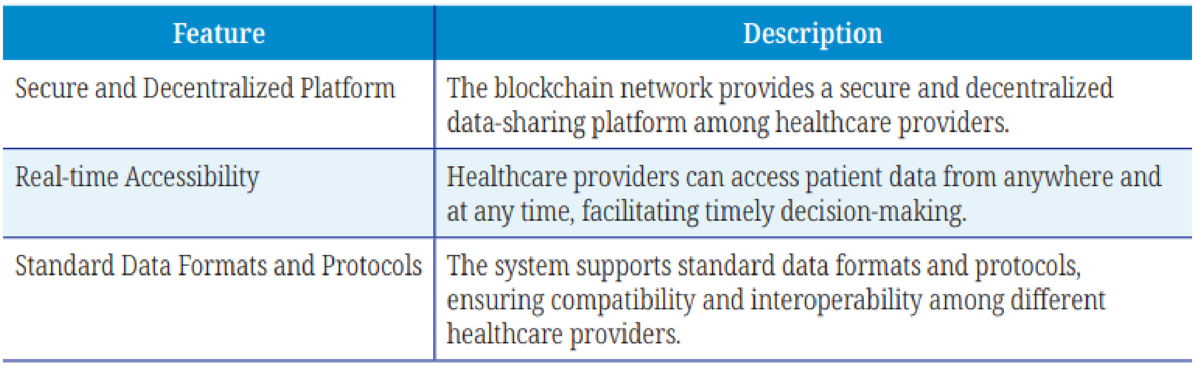
1. Sharing data in a safe and decentralised solution. A decentralised and safe platform for exchanging data was offered by the blockchain network. Healthcare providers might safely transfer patient data without depending on a centralised authority. Through the use of cryptographic algorithms and distributed consensus processes, the system ensured that the shared data remained intact and confidential. Healthcare providers were able to exchange data directly with one another because to this decentralised system, which eliminated intermediaries.

2. Permissioned access to patient records. Doctors and other medical professionals might access patients' records over the blockchain network. All relevant medical data and patient records were accessible at all times, regardless of their physical location. Healthcare providers were able to improve patient care and outcomes by making fast, educated choices based on instantaneous access to patient data.

3. adhere to established protocols and data formats. In order to make data exchange and interoperability easier between different healthcare providers, the system promoted the use of common data formats and protocols. The solution ensured data transfer compatibility and consistency by adhering to recognised standards like FHIR (Fast Healthcare Interoperability Resources) for data representation and HL7 (Health Level Seven) for data sharing. This standardised method allows for the smooth integration of data from various sources and systems, so healthcare practitioners may access and analyse patient data without compatibility difficulties.

In Table 2 you can see the system's capabilities for exchanging data and being interoperable.

Table 2. Data sharing and interoperability features



Feature	Description
Secure and Decentralized Platform	The blockchain network provides a secure and decentralized data-sharing platform among healthcare providers.
Real-time Accessibility	Healthcare providers can access patient data from anywhere and at any time, facilitating timely decision-making.
Standard Data Formats and Protocols	The system supports standard data formats and protocols, ensuring compatibility and interoperability among different healthcare providers.

Medical staff may safely access patient records from any location because to these interoperability and data sharing features. The system's use of standard data formats and protocols allowed for easy data transmission, promoted teamwork, and improved patient care.

Privacy in healthcare using the Blockchain

Blockchain technology can help balance the privacy of health data and access to those data, achieving four goals: providing patients with full control of Electronic Health Records (EHRs), determining who can access and track documents, ensuring secure record transfers, and minimizing the chance of unauthorized individuals obtaining PHI.

Ancile is an efficient and secure Blockchain-based framework for accessing medical records, using smart contracts and advanced encryption techniques to control and prevent data misuse.

BMPLS is a Blockchain-based privacy-preserving scheme proposed for Location Sharing, which meets the necessary requirements for modern healthcare systems. It can be used to share telecare Blockchain-based privacy for medical information systems. Healthchain is a large-scale Blockchain-based health data privacy project that uses encryption techniques to control micro-access, preventing the deletion or manipulation of IoT data and physician diagnoses.

A Blockchain-based data storage scheme in healthcare was proposed, using encryption techniques to protect patient data and aliases. Patients and health organizations participate as data transmitters and receivers, and EHR systems store data in a cloud network, allowing patients to share their personal data with physicians and health organizations.

The authors of proposed a plan for implementing EHR that would protect EHR data more securely and privately using the Hyperledger Fabric Blockchain framework. The proposed platform stores encrypted health information in the cloud system, ensuring that patient data is controlled only by the patient himself. This platform guarantees patients' aliases and obtains acquired aliases using cryptographic functions. Overall, blockchain technology has the potential to significantly improve privacy and security in healthcare systems.

The proposed approach in uses four technologies in Blockchain for improving privacy: zero-knowledge proofs, trusted execution environments, homomorphic encryption, and federal learning. Zero-knowledge proofs allow one party to validate a transaction or validation without disclosing any critical information, which can be beneficial in healthcare contexts. Federal learning involves sending an algorithm to a node, analyzing it, and sharing the updated algorithm among all nodes in the Blockchain. Homomorphic encryption allows calculations to be performed on encrypted data, allowing patients to use another person's review of their data without exposing their own data.

In Blockchain-based knapsack algorithms are used for privacy and security in healthcare. These algorithms use public and private keys to encrypt and decrypt healthcare data, ensuring privacy and scalability. Off-chain computing and storage technology is suggested as a framework for managing information through distributed software that interacts with off-chain sources. This system aims to improve privacy and scalability, allowing patients to manage their own data and digital identity.

A Blockchain-based telephone privacy tracking plan is proposed, allowing healthcare stakeholders to connect to the Blockchain network with their mobile phones. The integration of emerging 5G technology with Blockchain-based healthcare systems leads to higher reliability, less communication delay, and improved privacy of medical stakeholders.

Blockchain technology is also used in better management of healthcare data and maintaining its security. A prototype using the Hyperledger platform was proposed, ensuring better control of access to healthcare data. A reliable framework for wearable devices and patient-connected sensors is proposed, protecting the privacy of information related to healthcare and ensuring confidentiality and integrity of data.

Another study introduced a framework using Blockchain technology for effective management of human resources, utilizing smart contracts for data conservation. A permissioned private Blockchain network was used to manage access to medical data. A decentralized architecture based on Blockchain was proposed by Nishi et al., where the patient is the real owner of their data, and attribute authorities can issue or revoke attributes only with the patient's permission.

In conclusion, the proposed approach in offers promising solutions for improving privacy and security in healthcare.

Securing healthcare data by using the Blockchain

In the smart health scenario, security is a crucial issue, with the main challenges being the reduction of accurate data and the need for secure data exchange among stakeholders. Blockchain technology can address these issues by storing patient records in ledgers and encrypting them using the patient's private key. This system is more secure than most current systems, as it allows for more efficient data sharing and access control.

A cryptographic scheme for healthcare was proposed using Blockchain technology, where the index for the EHR is stored in the Blockchain, allowing patients to have complete control over who can view their data. The system also stores real EHRs encrypted on another server, requiring users to grant permission to the information owner with a decryption key.

A new EHR sharing scheme based on cloud computing and Blockchain was presented, which addresses the main challenges of current health systems. The framework, ChainSDI, is based on a combined "home-edge-core" SDI to provide real-time performance and accountability for home-based healthcare services. The framework also aims to build a secure Blockchain network to ensure transactions comply with regulations while still allowing data interaction.

Telemedicine services on demand (MoD) were provided, utilizing Blockchain technology to improve authentication and licensing for department of defense services in the medical trap system. A key program is distributed for independent updates, ensuring the integrity of private healthcare data. The Blockchain technique in EHR stores patient data in a chain to prevent manipulation and resists collusion attacks in (N-1) destructive attacks.

Containers in the Blockchain substrate were used for greater security of healthcare data, with a framework called Medichain on a Blockchain platform proposed. Each block of the framework maintains a list of patient records, secured using the security features of Blockchain technology. This framework was implemented using Python programming language and object-oriented concepts.

The authors of various studies have explored the use of Blockchain technology to secure healthcare data, focusing on protecting patients' medical records from information theft and unauthorized intrusion. They introduced a platform for data storage and transmission using cryptographic algorithms, demonstrating better performance in data storage and efficient data transfer than similar schemes.

The authors also highlighted the privacy and security issues of healthcare stakeholders, using features such as anonymous signatures, zero-knowledge proofs, attribute-based encryption, and approval of smart contracts for more secure healthcare data. They also used various security techniques to ensure the data sharing process.

Another study investigated the characteristics of the Blockchain network and analyzed consensus algorithms to develop a framework for maintaining the security and privacy of data related to patients in the healthcare field. Remote patient monitoring (RPM) was discussed, and smart contracts were used for proper analysis and management of data generated in the field of medical care. A Blockchain-based healthcare data management system was proposed, allowing patients to easily access their medical records located in various medical centers.

The authors integrated smart health care systems (SHSs) with Blockchain technology to maintain greater security and data integrity in the field of smart healthcare. An attribute-based signature scheme was presented with different authorities, allowing patients to disclose part of their data without exposing the rest.

The authors proposed solutions to prevent the production and distribution of counterfeit drugs in the healthcare network using Blockchain technology, covering the drug distribution cycle from production to consumption by the patient.

Another study introduced a framework based on Blockchain for managing and controlling access to medical data, improving data privacy, confidentiality, and decentralization in the medical care system. Qadar Butt et al. presented a Blockchain technology for medical communication and developed a location-independent global health record exchange system for transferring medical data.

The authors also presented a scheme for sharing data in the field of healthcare using Blockchain and edge computing, guaranteeing the security and privacy of shared data. They also designed a process to determine the reward for miners to mine healthcare blocks.

In conclusion, the use of Blockchain technology in healthcare has the potential to significantly enhance data security, privacy, and decentralization.

CONCLUSIONS

In conclusion, the purpose of this research was to examine the potential benefits of using a blockchain-based cloud EHR system in hospitals and other healthcare facilities. The results of the pilot research proved that the system could improve data management, sharing, and security in comparison to traditional EHR systems. The system was able to transmit and retain patient data securely while preserving its integrity, availability, and security thanks to blockchain technology and cloud architecture. Governments, healthcare providers, and patients are all profoundly affected by these findings. A blockchain-based cloud EHR system has the potential to improve patient outcomes, increase efficiency, and decrease costs. However, concerns regarding data privacy, cost-effectiveness, and regulatory compliance might slow adoption. Healthcare organisations should think long and hard about whether or not this system aligns with their goals and beliefs before committing to it. We urge healthcare organisations to keep investigating blockchain-based cloud EHR solutions for their possible advantages and to resolve the study's shortcomings by doing more research. If we want to know what the future holds for this technology, we need to conduct large-scale research and look at other blockchain-based EHR systems.

REFERENCES

1. Yang, Guang & Li, Chunlei & Marstein, Kjell. (2019). A blockchain-based architecture for securing electronic health record systems. Concurrency and Computation: Practice and Experience. 33. 10.1002/cpe.5479.

2. Shrestha, Sulav & Panta, Sagar. (2023). Blockchain-based Electronic Health Record Management System. 5. 298-313. 10.36548/jaicn.2023.3.006.

3. Agha, Dureshawar. (2023). Securing Electronic Health Records using Blockchain. VFAST Transactions on Software Engineering. 11. 57-66. 10.21015/vtse.v11i4.1656.

4. Mamun, Abdullah & Azam, Sami & Gritti, Clémentine. (2022). Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction. IEEE Access. PP. 1-1. 10.1109/ACCESS.2022.3141079.

5. Kasula, Balaram Yadav. (2023). The Role of Blockchain Technology in Securing Electronic Health Records. 4. 1-9.

6. Ettaloui, Nehal & Arezki, Sara & Gadi, Taoufiq. (2023). An Overview of Blockchain-Based Electronic Health Records and Compliance with GDPR and HIPAA. Data and Metadata. 2. 166. 10.56294/dm2023166.

7. Ettaloui, Nehal & Arezki, Sara & Gadi, Taoufiq. (2023). An Overview of Blockchain-Based Electronic Health Records and Compliance with GDPR and HIPAA. Data and Metadata. 2. 166. 10.56294/dm2023166.

8. Tan, Nguyen & Thanh, Le & Van Toai, Nguyen. (2024). Application of blockchain in medical data security and management: Potential, challenges and development directions. 03. 31 - 36.

9. Kasula, Balaram Yadav. (2023). The Role of Blockchain Technology in Securing Electronic Health Records. 4. 1-9.

10. Ettaloui, Nehal & Arezki, Sara & Gadi, Taoufiq. (2023). An Overview of Blockchain-Based Electronic Health Records and Compliance with GDPR and HIPAA. Data and Metadata. 2. 166. 10.56294/dm2023166.

11. Tan, Nguyen & Thanh, Le & Van Toai, Nguyen. (2024). Application of blockchain in medical data security and management: Potential, challenges and development directions. 03. 31 - 36.

12. Jakhar, Amit & Mrityunjay, Singh & Sharma, Rohit & Viriyasitavat, Wattana & Dhiman, Gaurav & Goel, Shubham. (2024). A blockchain-based privacy-preserving and access-control framework for electronic health records management. Multimedia Tools and Applications. 1-35. 10.1007/s11042-024-18827-3.

13. Jakhar, Amit & Mrityunjay, Singh & Sharma, Rohit & Sharma, Aman. (2022). A Blockchain-based Privacy-preserving and Access-control Framework for Electronic Health Records Management. 10.21203/rs.3.rs-2048551/v1.

14. SunithaBJ, & Sankar, K. & Ayesha, Amreen & Islabudeen, M.. (2022). Different Approaches on Security, Privacy and Efficient Sharing of Electronic Health Records Using Blockchain Technology. 10.3233/APC220007.

15. Hossain Faruk, Md Jobair & Shahriar, Hossain & Saha, Bilash & Barek, Abdul. (2022). Security in Electronic Health Records System: Blockchain-Based Framework to Protect Data Integrity. 10.1007/978-3-031-25506-9_7.