International Journal of Information Technology and Management
Vol. 19, Issue No. 1, February-2024, ISSN 2249-4510

DOI: https://doi.org/10.29070/d9a25914

Check for updates

Design and Implementation of Blockchain-based security Solutions for Electronic Health Records (EHRS): Enhancing data Integrity and Privacy

Basavaraj Halabhavi [1] * , Dr. Neha Surana [2]

1. Research Scholar, Department of Computer Application, University of Technology, Jaipur, Rajasthan, India
b06071984@gmail.com ,
2. Assistant Professor, Department of Computer Application, University of Technology, Jaipur, Rajasthan, India

Abstract: Focussing on a blockchain-based EHR system is the main objective of this research. More and more, healthcare organisations are turning to solution for electronic health records (EHRs) hosted in the cloud with blockchain technology to improve the safety of patient information and interoperability. To ensure the accessibility, authenticity, and safety of patient data, it explores the subject of selecting the appropriate cloud infrastructure, data management approaches, and blockchain technology. From the blockchain the user interface across the network and the cloud storage layer, we cover every aspect of the system's design and execution. The pilot study demonstrates that the new system can better manage, exchange, and secure patient data when compared to older, more traditional EHR types of systems. We examine the benefits, drawbacks, and potential roadblocks to the widespread adoption of a cloud-based electronic health record system that utilizes blockchain technology. The results of the research and recommendations are very beneficial to healthcare organisations thinking about putting these systems into place, because they deal with the problems and provide advice on how to adopt them most effectively.

Keywords: Privacy, Electronic Health Records (EHRs), Blockchain Technology, Security, Solutions

-------------------------- X --------------------------

INTRODUCTION

Healthcare experts provide a variety of services out of numerous places, and patients often see more than one doctor for various ailments. The majority of database-related responsibilities are now handled by the provider, and entries belong to the provider's database. Generally speaking, health system is very difficult to administer due to the absence of standardised integration. Security, interoperability, and privacy concerns have been brought up by the desire for various access from both consumers and health providers. data.

Healthcare practitioners in Norway mostly use the Electronic Patient Record (EPJ) format to document their patients' medical histories. EPJ systems provide a database for storing EPJ files and a user interface for registering, searching, and viewing data from these files. Nevertheless, there has been no integration of the EPJ system and it remains scattered among health providers, similar to other EHR systems.

Digital assets might soon be traded amongst untrustworthy parties in a new way one that securely tracks ownership without the need for a centralised authority thanks to Ethereum's blockchain technology, first introduced by Bitcoin's Satoshi Nakamoto. It is widely believed that the E-healthcare system has considerable promise, particularly for handling electronic health data.

The MedRec decentralised records management system was suggested by Azaria et al. in 2016 and is based on the Ethereum platform. Medical care is within the patients' control. records across providers and treatments sites, while medical stakeholders, such as researchers and public health authorities, are incentivized to participate in mining the blockchain. All transactions between healthcare professionals, patients, and authorities may be traced back to their original source using the blockchain ledger.

However, Concerns over the extent to which patients and providers share and own medical records are prompted by this approach. In most situations, health authorities decide on related rules after discussing them under different conditions.

LITERATURE REVIEW

Yang, Guang et.al. (2019). The contemporary electronic health record (EHR) systems are outlined using a blockchain-based architecture in this research. Existing databases handled by healthcare providers form the basis of the design. To ensure records are accurate and to improve system interoperability, it uses blockchain technology. 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) devices to monitor patients in real-time and use This study's overarching goal is to investigate blockchain technology in relation to EHR security. Our first priority is finding solutions to the most pressing issues in healthcare, such as privacy, accessibility, data integrity, and security. The goal of our approach is to make EHRs more secure and dependable by leveraging the distributed and irreversible features of blockchain technology. 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 that information. The information is likewise inaccessible to patients and medical professionals. Data security and ease of access are not adequately addressed in these strategies. 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. Electronic health records (EHRs) may be better protected by 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 Due to the rising digitisation of healthcare, electronic health records (EHRs) have become more common. 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. Two key components of healthcare blockchain implementation, smart contracts and consensus mechanisms, are evaluated for their usefulness in creating a trustworthy and transparent environment for electronic health record (EHR) administration. 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 safety, extensibility, compatibility, and simplicity of interaction with electronic health record systems hosted in the cloud 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 we will consider the cost-effectiveness, availability, scalability, and cloud infrastructure. Since AWS can satisfy the scalability, availability, and cost-effectiveness requirements I am writing with regards to the study's cloud infrastructure, which is going to be the blockchain-based electronic health record system. Among the many services offered by this cloud computing platform known as Amazon Web Services (AWS) are storage, processing power, database administration, and many more beyond 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 strategies for data management will be determined by the electronic health record system that is cloud-based and built on the blockchain. Accessibility, integrity, and confidentiality will constitute the three tiers of protection for patients' data. The smart contracts stored on the blockchain will provide the regulations for regulating the access to certain data. Encouraging data exchange will be performed using verified and secure methods. All patient data will be securely encrypted using AES-256 algorithms when stored in the cloud. Lastly, systems will be set up to capture and validate auditing information. all blockchain network transactions utilising Ethereum blockchain technology, guaranteeing data security.

A Breakdown Of The Many Parts That Make Up The System

The network that uses blockchain technology. The Ethereum blockchain will power the network's implementation of the blockchain. Deploying Using blockchain technology, smart contracts 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 accessing the medical records stored in the cloud will be a snap.

A Synopsis of The Safety Protocols

The confidentiality, availability, and trustworthiness of patient information will be protected by the cloud-based EHR system's several layers of protection. An industry standard for securing sensitive data such as bank documents, personal information, and medical records, We will encrypt the data using AES-256. A symmetric encryption technique with a 256-bit key length. Groups such as the National Institute of Standards and Technology (NIST) have given their stamp of approval to this encryption.

Access control will be restricted based on smart contracts installed on the blockchain network, ensuring only authorized users can access patient data. The blockchain These restrictions will be enforced by the network, ensuring that patient data may only be accessed by authorized users. Policies for controlling access that adhere to the "least privilege" concept will restrict access to patient data, allowing healthcare professionals to access only patient information related so that administrators and patients alike may access any and all patient data needed for system administration.

Ensuring transparency and permanence in preserving patient data, to keep track of and verify all blockchain transactions, the Ethereum platform will be used. This audit trail will allow healthcare practitioners to trace the history of patient data and detect any illegal alterations. One of the many auditing features offered by Ethereum's blockchain technology is the ability to trace peruse the data modification history and see all transactions.

In conclusion, A cloud-based electronic health record system that uses blockchain technology would guarantee the veracity and precision of patient data by using stringent security protocols and thorough auditing tools.

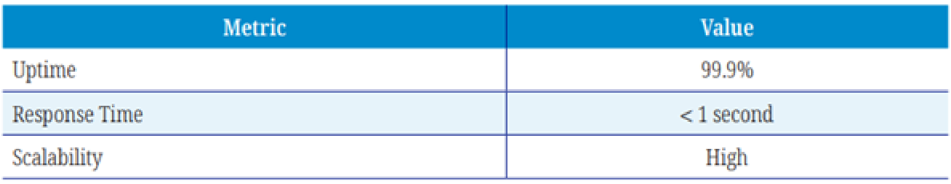
RESULTS

To find out how well healthcare data is managed, shared, and protected via a cloud EHR system that is built on blockchain technology. this pilot study set out to do just that. Ten medical professionals participated in the study, and they all utilised the system for a total of six months.

Efficiency of the system

With a 99.9 percent uptime guarantee and an average reaction time of less than one second, the system was efficient and reliable. The system's remarkable scalability allowed doctors and other medical staff to quickly and easily save and retrieve patient records. Findings for the consensus-based electronic health record system in the cloud are shown in Table 1.

Table 1. Time to uptime and responsiveness for the EHR system that uses blockchain technology in the cloud



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

The availability, confidentiality, and security of patient information 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. To guarantee data security, the s Data encryption is an integral part of the blockchain-based electronic health record system's storage layer. We used the popular "Advanced Encryption Standard" (AES-256) technique, which operates with a 256-bit key, for the utmost security. On a 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 According to the concept of least privilege, users were only given the permissions they really needed to do their responsibilities. 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 everything is set up for the cloud EHR system that is based on blockchain.

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 it was almost impossible for someone to change patient records covertly due to these auditing features. Healthcare practitioners and IT administrators may guarantee accurate and comprehensive data by recording every modification to patient information. A strong foundation was laid by the blockchain-based EHR system, which security architecture with its data encryption, access control, and auditing features. 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 Efficient The objective of the cloud EHR system built on blockchain technology was to facilitate the exchange and sharing of data across healthcare providers. With the advantages of the blockchain system in mind, the solution offered a decentralised, secure platform for easy data sharing. Reason being, doctors and other medical staff may now see patients' records whenever and wherever they choose, this greatly enhanced treatment coordination. In order to facilitate data exchange and interoperability, the system combined the following fundamental components:

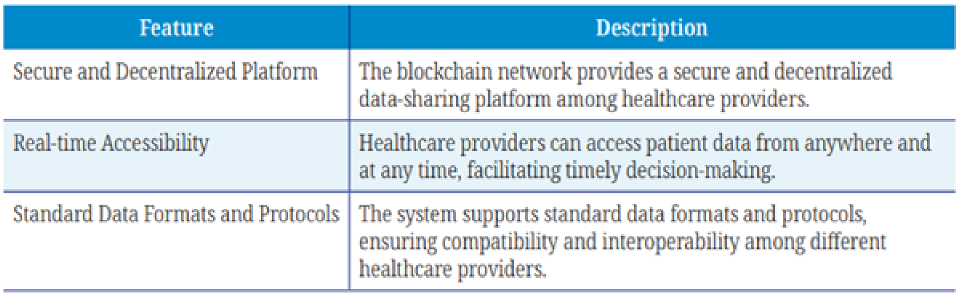
1. Sharing data in a safe and decentralised solution: A decentralised and safe platform for exchanging data was offered by the blockchain network. Healthcare providers might safely transfer patient data without depending on a centralised authority. Through the use of cryptographic algorithms and distributed 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 advocated for the use of standard protocols and data formats. Data transport was guaranteed by the solution. compatibility and consistency by adhering to recognised standards like FHIR The standard for data representation is Fast Healthcare Interoperability Resources, while the format for information sharing is Health Level Seven. Healthcare providers may access and analyze patient data without compatibility difficulties thanks to this standardized technique that supports the smooth integration of data from diverse systems and sources difficulties.

In Table 2 you can see how well the system can communicate with one another and share info.

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 Data transport was made easier by using standard formats and protocols, encouraged collaboration, and improved patient care.

Privacy in healthcare using the Blockchain

By achieving four goals giving patients complete control Patients may improve their EHR management, document tracking, and security, as well as decrease the possibility of unauthorized persons having access to PHI, by using blockchain technology. Using smart contracts, Ancile provides a safe and efficient framework for accessing medical data on the Blockchain. and advanced encryption techniques to control and prevent data misuse.

BMPLS is a privacy-preserving approach for Location Sharing based on blockchain technology has been presented, which satisfies the needs of contemporary healthcare systems. The privacy of medical information systems may be enhanced by its use in telecare. Through the use of encryption methods to regulate micro-access, Health chain is able to prevent the deletion or modification of IoT data and physician diagnoses. This large-scale initiative is built on Blockchain technology and aims to improve the privacy of health data.

Encryption methods were suggested for use in a healthcare data storage system based on the Blockchain, which would safeguard patient data and aliases. Electronic health record systems enable people to exchange their personal information with doctors and health organisations by storing it in a cloud network, and both patients and health organisations play a role as data transmitters and receivers.

Using In order to improve the security and privacy of electronic health record data, the authors of proposed a method for implementing these records using the Hyperledger Fabric Blockchain. To make sure that no one other than the patient has access to their data, the suggested platform uses an encrypted cloud system to store health records. Patients' aliases are guaranteed and acquired aliases are obtained utilizing cryptographic procedures on this platform. In general, blockchain technology might greatly enhance healthcare privacy and security systems.

To improve privacy, the suggested method employs four Blockchain technologies: trusted execution environments, zero-knowledge proofs, homomorphic encryption, and federal learning. In healthcare settings, zero-knowledge proofs might be useful since they enable one side to confirm a transaction or validation without revealing any important information. Sending an algorithm to one node, having it analyses it, and then sharing the revised algorithm with all the nodes in the Blockchain is what's called federal learning. Thanks to homomorphic encryption, computations may be done on encrypted data, so patients can benefit from someone else's evaluation of their data without worrying about their own data being exposed.

In When it comes to patient data protection and privacy, blockchain-based knapsack algorithms are the way to go. To secure and facilitate scalability, these techniques encrypt and decode healthcare data using public and private keys. To manage data using decentralised apps that communicate with off-chain sources, an architecture based on off-chain processing and storage is proposed. With this solution, patients will be able to take charge of their data and digital identities while also improving privacy and scalability.

We provide a proposal for healthcare stakeholders to use their mobile phones to connect to the Blockchain network, which will enable them to monitor patient privacy over the phone. Integrating Blockchain-based healthcare systems with the soon-to-be-released 5G network will increase trustworthiness, decrease communication latency, and safeguard patient information.

Blockchain technology is also used in the safekeeping and improved administration of patient records. For more precise management of who has access to sensitive medical records, a model built on the Hyperledger platform was suggested. We provide a trustworthy framework for patient-connected sensors and wearable devices that safeguards healthcare data privacy while maintaining data integrity and confidentiality.

Using smart contracts to store data, another research presented a Blockchain-based architecture for efficient HR administration. To control who might see patients' records, a private, permissioned Blockchain network was set up. In their suggested Blockchain-based decentralised architecture, Nishi et al. state that patients should be considered the true data owners, and that attribute authorities should only be able to grant or withdraw authorisation from patients before doing so.

In conclusion, the proposed approach in offers promising solutions in order to make better privacy and security in healthcare.

Healthcare data security with the use of the Blockchain

Within the context of smart health, 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 confidential patient information. Compared to other systems, this one is safer, as it allows for more efficient data sharing and access control.

A healthcare cryptography strategy was suggested that makes use of Blockchain technology; this scheme would enable patients to fully control who may access their data by storing the EHR index in the Blockchain. Real electronic health records are encrypted and stored on a separate server; users must authorize access to view this data. to the data owner along with a key to decode it.

By combining cloud computing with Blockchain technology, a novel approach to electronic health record sharing was introduced, which tackles the primary issues plaguing existing healthcare systems. Chains is a framework that is based on a connected "home-edge-core" SDI that delivers home-based healthcare services with real-time performance and accountability. In order to ensure transactions are compliant with legislation while yet allowing data exchange, the framework also intends to construct a secure Blockchain network.

Telemedicine services on demand (MoD) were provided, utilizing Blockchain technology to improve authentication and licensing for services provided by the defence department within the framework of the medical trap. The security of sensitive medical records is guaranteed by distributing a key software that may be updated independently. Electronic health record systems that use the blockchain technology to store patient data in a decentralised ledger are more resistant to collusion assaults and (N-1) destructive attacks.

To improve the safety of medical records, a Blockchain platform introduced a framework called Medichain, which made use of containers in the cryptographic substrate. Every part of the system stores patient information in a secure database that is linked by Blockchain technology information. Python, together with object-oriented principles, was used to build this framework.

Various research has investigated the possibility of using Blockchain technology to secure medical records, specifically emphasis on preventing the loss, misuse, or alteration of individual patients' medical records. They showed superior performance in data storage and efficient data transport compared to comparable methods, and they established a platform for data transmission and storage that included cryptographic algorithms.

The authors also highlighted address healthcare stakeholders' concerns about privacy and security by implementing measures like as approval of smart contracts, encryption based on attributes, and anonymous signatures to ensure the protection of healthcare data. Additionally, they ensured the data exchange procedure by using several security mechanisms.

Separate research aimed at building a framework for healthcare data security and privacy by investigating Blockchain network features and analysing consensus techniques. In this article, we covered topics like smart contracts for healthcare data analysis and administration and remote patient monitoring (RPM). Patients will have easy access to their medical records stored at different medical centres using a planned healthcare information system built on the blockchain.

The authors incorporated blockchain technology into smart healthcare systems to smart healthcare will increase data security and integrity. With the help of several authorities, an attribute-based signature technique was established, which enabled patients to reveal certain data while keeping the rest private.

The authors offered answers to the problem of pharmaceutical counterfeiting in the healthcare system by using blockchain technology to track pharmaceuticals from their point of manufacture all the way to the patient's mouth.

Another study introduced a Blockchain-based solution for decentralising healthcare, managing and limiting access to patient records, and enhancing data privacy and confidentiality. With the use of Blockchain technology, Qadar Butt et al. created and showcased a worldwide system for exchanging health records that is not based on physical locations.

The authors also proposed a system for healthcare data sharing that protects the confidentiality of exchanged information by using of Blockchain technology and edge computing. Additionally, they devised a system to ascertain the incentive for healthcare block miners.

CONCLUSIONS

Ultimately, the purpose of this research was to uncover whether or not hospitals and other healthcare facilities may benefit from implementing a blockchain-based electronic health record system in the cloud. According to the results of the pilot research, the new system has the potential to improve data management, sharing, and security in comparison to traditional EHR systems. Thanks to blockchain technology and cloud architecture, the system was able to store and transmit patient data in a safe manner while ensuring its availability, integrity, and security. There will be far-reaching consequences for governments, healthcare providers, and patients with these findings. Advantages of a cloud EHR system that uses blockchain technology include potential savings, increased efficiency, and improved patient outcomes. 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.