iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** I **Month of publication:** January 2023

DOI: https://doi.org/10.22214/ijraset.2023.48922

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue I Jan 2023- Available at www.ijraset.com

Blockchain Based Storing and Sharing of Medical Record

Khushi Itankar[1], Gauri Deshpande[2], Mahek Sehgal[3], Mithila Ghyar[4], Prof. Rupali Vairagade[5]
Department of Information Technology, G.H Raisoni College of Engineering Nagpur, India

Abstract: ***A decentralized electronic health record (EHR) storage system is a system for storing and managing electronic health records (EHRs) in a decentralized manner. This means that, rather than storing EHRs on a centralized server or database, the records are distributed across a network of nodes, each of which stores a portion of the overall data. This allows for greater security, as it makes it much harder for the data to be lost or corrupted due to a single point of failure. It also gives patients more control over their own health data, as they can choose which nodes to store their records on. Additionally, a decentralized EHR storage system can provide better privacy and confidentiality, as the data is not stored in a single location that can be easily accessed by unauthorized parties.***

Keywords: decentralized, electronic health record (EHR), privacy, confidentiality, unauthorized.

I. INTRODUCTION

The current rapid development of information technology has increased the use of electronic information systems in medical treatment. A significant amount of medical data is generated every day, including electronic medical records, medical images, diagnostic reports, infectious diseases, etc. With the proper exploitation of these medical data, infectious diseases can be predicted in advance and prepared for protection, as well as used as legal evidence. The possibility of data leakage or alteration throughout the operational procedure makes it extremely difficult for participants to share medical records. A blockchain-based electronic medical records system is the primary answer to these problems. Where patients can store their medical records with security. This technology enables the doctor and the patient to store and access medical data within the blockchain network.

A decentralized file storage system using IPFS (Interplanetary File System) and Web3Storage is a system that utilizes decentralized technologies to store and manage files in a distributed manner. This means that the files are not stored on a central server, but are instead distributed across multiple nodes on a network. IPFS is a peer-to-peer protocol that allows users to store and access files on a decentralized network. It uses a hash-based addressing system to identify and locate files, allowing for secure and efficient retrieval. Web3Storage is a decentralized storage platform built on top of IPFS. It allows users to store and manage files on the Ethereum blockchain, providing additional security and immutability. Using these technologies, a decentralized file storage system can provide a more secure and resilient way to store and manage files, as it is not dependent on a central server and is resistant to tampering and censorship.

II. RELATED WORK

Muhammad Usmana, Usman Qamar The Paper, "Secure Electronic Medical Records Storage and Sharing .Using Blockchain Technology", discuss about a developed system based on permissioned block chain for efficient storage and sharing of electronic medical records (EMRs) which provides better security and privacy of data. The application focuses three types of users: Patients, Healthcare-Providers and Health Administration. Health Administration will be responsible for the registration of patients and doctors. The application framework includes Membership Management, user interfaces to interact with the application, nodes for consensus mechanism that also holds smart contracts (business logic), Chain and World-State database. In membership management the health administrator registers users i.e. Patients and Healthcare-Providers to the membership service based on their roles. During registration, health administration should make sure that only valid user should be register in membership service. For example, in case of Healthcare-Provider registration they should ensure that he/she is a qualified doctor and must be registered with the government health organization. The membership service also hosts a certification authority that generate key pair for signing and encryption key pair for every user. Patient is issued with a symmetric encryption key (Patient Key) which is used for encryption/decryption of medical records. When a patient wants to share medical records with a Healthcare-Provider, the patient can share his/her patient key using the public key of that Healthcare-Provider. Healthcare-Provider can also request this key from patient and when provided he/she can access patients' medical records and can add new records. The system also provides a user interface for every user through which they can interact with the system.

The frontend web application is written in HTML, CSS and JavaScript. All the users are provided with their own separate web user interface. Both patients and Healthcare-Providers will use their login credentials (provided by the admin) to login to the system [1].
"Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS", by Jin Sun, Xiaomin Yao, Shangping Wang, And Ying Wu. In this paper, based on the ciphertext policy attribute-based encryption system and IPFS storage environment, combined with block chain technology, we constructed an attribute-based encryption scheme for secure storage and efficient sharing of electronic medical records in IPFS storage environment. Our scheme is based on ciphertext policy attribute encryption, which effectively controls the access of electronic medical data without affecting efficient retrieval. Meanwhile, we store the encrypted electronic medical data in the decentralized Inter-Planetary File System (IPFS), which not only ensures the security of the storage platform but also solves the problem of the single point of failure. Besides, we leverage the non-tamperable and traceable nature of block chain technology to achieve secure storage and search for medical data. The security proof shows that our scheme achieves selective security for the choose keyword attacks. Performance analysis and real data set simulation experiments shows that our scheme is efficient and feasible [2].
Xiaoguang Liu, Ziqing Wang, Chunhua Jin, Fagen Li, Gaoping Li the Paper, "Using Blockchain for Electronic Health Records". In the paper, we propose a medical data sharing and protection scheme based on the hospital's private block chain to improve the electronic health system of the hospital. Firstly, the scheme can satisfy various security properties such as decentralization, openness, and tamper resistance. A reliable mechanism is created for the doctors to store medical data or access the historical data of patients while meeting privacy preservation. Furthermore, a symptoms-matching mechanism is given between patients. It allows patients who get the same symptoms to conduct mutual authentication and create a session key for their future communication about the illness. The proposed scheme is implemented by using PBC and Open SSL libraries. The motivation of this paper is to design a medical data sharing scheme based on block chain. It is helpful to the storage, management, and sharing of the medical data. The scheme should satisfy the security requirements in medical data sharing schemes. Also, it should have low computational and communication cost.

The main contributions of this paper are listed as follows.

1) A lightweight medical data sharing and protection model is proposed, which is based on block chain. Utilizing the proxy re-encryption technology, the model could make data sharing among doctors from different hospitals. The stored medical information is very secure and could not be easily tampered since they are stored in the block chain.
2) An improved consensus mechanism is proposed by improving the traditional delegated proof of stake. It is secure, reliable, and efficient.
3) We design a symptoms-matching mechanism for patients who register in different hospitals and have the same disease symptoms. One session key could be set between the patients after they make mutual authentication. The mechanism can help patients to communicate the disease information[3].

"Electronic Healthcare Data Record Security using Blockchain and Smart Contract" The Paper by, Sami Bourouis, Punit Gupta, Dinesh Kumar Saini, Farjana Khanam Nishi, Mahizebin Shams-E-Mofiz, Mohammad Monirujjaman Khan and Abdulmajeed Alsufyani. This paper presents a block chain-based system that helps the patient's data be managed and secured into a single record held by the patient. This system was developed using the Ethereum network using Ganache, as well as programming languages, tools, and techniques such as Solidity and web3.js. The measured approach suggested in this paper uses this platform to store patients' data and execute functions in a decentralized system using block chain smart contracts. Transactions are communicated through the smart contract once it has been launched, providing security and privacy features. Furthermore, the transaction's desired alterations can be verified and transmitted to the entire distributed network. There is also a cryptocurrency wallet (MetaMask) that holds a centrally controlled, private information system in which records can be quickly accessed and secured by authorities. Doctors and patients can access the system through the wallet. Moreover, all the data of the doctor and patient will be secured and managed through this system. This proposed system is aimed at doing things such as the following: block chain technology allows users to obtain the same data at the same time, increasing efficiency, developing credibility, and reducing barriers. It enables the secure storage of data by setting specific access for users. Additionally, this proposed system facilitates the secure transfer of patient medical records. Finally, this paper describes a health-record system and a new protocol that are quick and secure to use. It allows greater openness and ownership of sensitive data to be recorded and secured and also promotes the healthcare sector with blockchain[4].

"Electronic Health Record Monitoring System and Data Security Using Blockchain Technology" by Kazi Tamzid Akhter Md Hasib,1Ixion Chowdhury,1Saadman Sakib, Mohammad Monirujjaman Khan, Nawal Alsufyani, Abdulmajeed Alsufyani, and Sami Bourouis. The study focuses on limiting third-party engagement in medical health data and improving data security. Throughout the process, this will improve accessibility and time efficiency.

People will feel safer during the payment procedure, which is the most significant benefit. A smart contract and a peer-to-peer encrypted technology were used. The hacker will not be able to gain access to this system since this document uses an immutable ledger. They will not be able to change any of the data if they gain access to the system. If the items are found to be defective, the transaction will be halted. Transaction security will be a viable option for recasting these problems using cryptographic methodologies. We developed a website where patients and doctors will both benefit because of the use of blockchain technology to ensure the security of medical data. We have different profiles for doctors and patients. In the patient profile, they can create their own account by using a unique address, name, and age. This unique address will be created from the genesis block. The unique address is completely private to the owner, who will remain fully secure in our network. After creating an account, the patient can view the doctors' list and they can upload their medical reports such as prescriptions and X-rays. All the records uploaded by the patient will be stored on our local server (Ganache). The records are stored as hashed strings of the data. Those files will also have a unique address, and it will be shown in the patient profile. After granting access, the doctors will be able to view their records in the respective doctor's profile. For accessing the options such as uploading, viewing, or editing the data, Ethereum currency (a fee) will have to be paid in order to complete the request. On the other hand, doctors can enter their profile using their name and unique address. After logging in, they can view their name, unique address, and the list of patients that have granted access to the doctor to view their files.

III. METHEDOLOGY

A distributed electronic health record (EHR) system is a system in which patient health information is stored in a network of interconnected, distributed databases rather than in a central, authoritative database. This type of system has potential advantages over his centralized EHR system, including increased security, greater patient control over their health information, and ease of information sharing among different health care providers. To implement a decentralized EHR system, the following methodology can be followed:

1) *Define the Scope of the System:* Step one in implementing a decentralized EHR gadget is to genuinely define the scope of the gadget. This need to encompass the sorts of data as a way to be stored within the gadget, the stakeholders who could have get admission to to the device, and any legal or regulatory requirements that ought to be met.
2) *Identify and select the Appropriate Technology:* Decentralized EHR systems typically use blockchain technology to store and manage patient health information. The next step, therefore, is to identify and choose the right blockchain technology for your system. This includes conducting research, consulting with experts, and evaluating various options to determine the best technology for your system's needs.
3) *Develop the System Architecture:* Once the technology has been chosen, the next step is the development of the system architecture. This should include defining the structure of the decentralized database network, determining how information will be shared between different healthcare providers, and designing the user interfaces and other tools used to access the system and handle it.
4) *Implement and Test the System:* In the next step, the system will be implemented according to the developed architecture. This may include creating decentralized databases, developing user interfaces, and testing the system to ensure it is working properly.
5) *Train Stakeholders on the use of the System:* Once the system has been implemented and tested, the next step is to train stakeholders to use the system. This should include training on accessing and managing patient health information and the security measures that must be followed.
6) *Launch the System and Monitor its Performance:* The final step in implementing a decentralized EHR system is to launch the system and begin using it in practice. It is important to monitor the performance of the system to ensure that it is meeting the needs of stakeholders and to make any necessary adjustments as needed.

Web3 storage is a decentralized data storage service that uses the Web Assembly module to store files on the Ethereum blockchain. Web3 storage files are interoperable with any file system and through the Ethereum network, become accessible by anyone without a central server.

A. *How Does it Work?*

In Web3.Storage, content is persistently stored on Filecoin and pinned redundantly to IPFS using a network of storage providers. As a result of their combined efforts, Filecoin and IPFS provide content addressability and persistent storage for content, data, and applications. A content-addressable link is an immutable link that is based on the content itself (CIDs), preventing information from being changed, edited, or compromised without leaving a traceable record of the alteration. By ensuring persistence, this service makes sure the data is preserved and available for future use. This is supported by the solid Filecoin economic model and verifiable evidence of the reliability of the data that is stored.

More specifically, information sent to Web3.Storage is immediately pinned to a Protocol Labs-hosted IPFS cluster made up of three geographically dispersed nodes. In order to store it on the Filecoin network, it is then placed in a queue. It is then stored with at least five geographically dispersed miners after being packed with additional data in a Filecoin deal while in this queue. It is also pinned to other IPFS pinning services, such as Pinata, for added availability and redundancy.

The actions to be taken in our decentralized storage platform are as follows:

1) Upload a medical record to be stored
2) Upload: By clicking upload button content of file gets stored on IPFS and now file is decentralized i.e., on IPFS.
3) Get the unique URL.

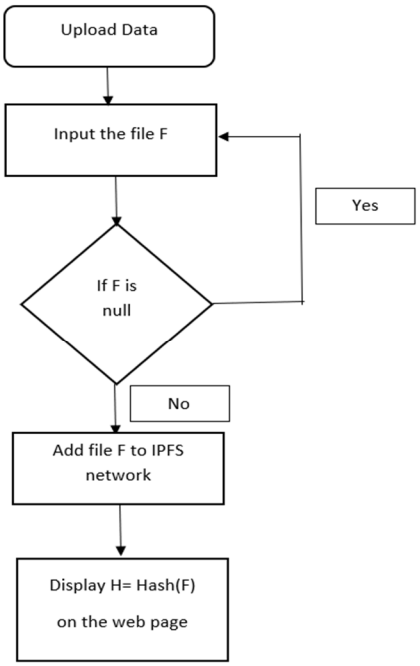


Fig. III.1 Flowchart

IV. IMPLEMENTATION

MetaMask has connected for the needed service. The authorized user/patient will upload the record and that submit the record. The record will store in IPFS and generate the unique key with an access link. IPFS objects, each of which may hold up to 256 kilobytes of data, are where files are kept. A data structure called an IPFS object has two fields: Binary data is kept in the data field, while the links field contains a list of links to all the other parts of the file, organized in an array.

A link structure consists of the following three elements:

1) *Name:* The link's name or alias.
2) *Hash:* The linked object's cryptographic hash
3) *Size:* The linked object's overall size.

a) *IPFS:* IPFS is a decentralized storage system that, like Bit Torrent, allows for the retrieval of content data. IPFS provides an environment in which any user can distribute a file via its address and anyone can request material in the peer's network from any node present using a defined distributed hash table. The goal of IPFS is to create a unified global network. In a single global network, when two users send a block of data with the same hash Data will be transferred between peers who download data from user 1 and those who download data from user 2. Connecting to the IPFS network can be accomplished using either the command-line interface (CLI) or their desktop application. When either of these services is started, the local node must perform a look-up to see which other nodes it can connect to. This lookup request is sent to any of the IPFS team's bootstrap nodes. IPFS also wants to bring back protocols used for static web pages and transfer them via HTTPS-enabled gateways. Users can also use a public gateway instead of installing IPFS Client. The IPFS page has several gateway lists. In February 2015, the alpha version of IPFS was released. IPFS nodes possess a key pair and communicate with one another directly over a peer-to-peer network. Which uses the private key to sign in to the IPNS service while the public key is used to create NodeID. In order to establish a connection, two nodes must first exchange public keys. If the NodeID does not match the public key being exchanged, the connection is broken. There are essentially three different types of nodes: client nodes, retrieval miner nodes, and storage miner nodes.

b) *Client Node:* The node exclusively stores and retrieves files via the IPFS network. It does not, however, offer its storage space to the IPFS network.

c) *Retrieval Miner Node:* This node on the IPFS network makes storage space available to store files for other nodes. However, the garbage collection function of IPFS saves and deletes the files kept on this node transiently.

d) *Storage Miner Node:* The node makes storage capacity available to the IPFS network and permits the pinning service to store files for an extended period of time.

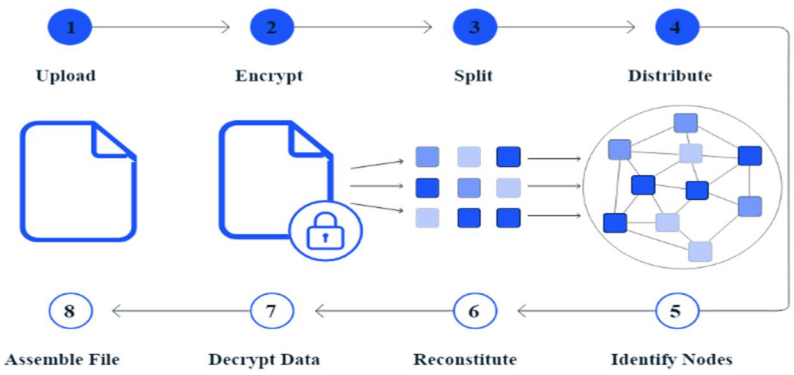


Fig. IV.1 How IPFS works

e) *WEB3 Storage:* Web3 means that the users can read, write, and own their material. This means that users can preserve, retrieve, and maintain their own content in Web3 storage. Web3 storage protocols and chains are classified as network-based storage, peer-to-peer storage, and coordination platforms. Storage on a network indicates that data is kept and maintained within storage resources, while the storage resources themselves are owned by the protocol/chains, as opposed to peer-to-peer. Clients can choose which storage resources store their data in P2P storage. Clients (peer 1), like File coin, use IPFS to store their data by selecting one or more storage nodes (peer 2). Behind the scenes, content sent to Web3.Storage is persistently stored on Filecoin and pinned redundantly on IPFS across a network of storage providers. Together, Filecoin and IPFS provide content addressability and persistence to information, data, and applications. Immutable links based on the content itself (CIDs) enable content addressability, making information impossible to change, edit, or compromise without leaving a traceable record of tampering. Persistence ensures that the data stored through this service will remain intact and accessible, backed by Filecoin's robust economic model and verifiable proofs of the stored data's integrity. Data delivered to Web3.Storage is immediately pinned to an IPFS Cluster of three geographically scattered nodes hosted by Protocol Labs. It is then queued to be stored on the Filecoin network. It is packed with other data in a Filecoin transaction while in this queue, and then stored with at least five geographically spread miners. It is also pinned to other IPFS pinning services, such as Pinata, for added redundancy and availability!

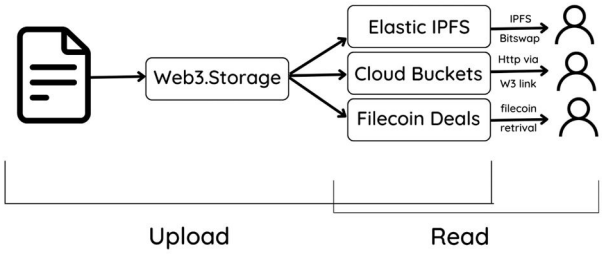
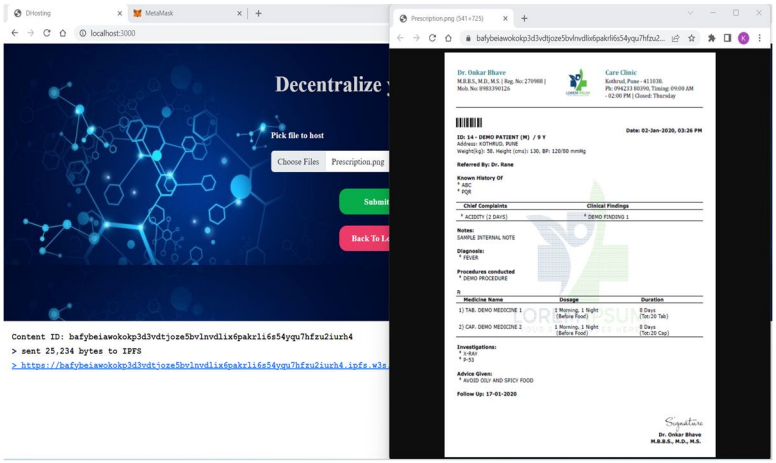


Fig IV.2 Architecture of web3. storage

V. RESULT

1) *Login Page:* The Login Page for MetaMask is displayed to help users securely access their cryptocurrency wallet and interact with the decentralized web.
2) *MetaMask Account Page:* You can find your MetaMask address under account name (in the format 0x12r45... 6HJ9) and also displays ETH you have on your wallet.
3) *Connect to Wallet using MetaMask:* After "Connect Wallet", if your MetaMask account address is found to be valid, it will connect you to metamask and the "Upload" button will be displayed.
4) *Click on Upload File:* After clicking on "Upload File", a page will be displayed asking you to decentralize your records.
5) *Decentralize Your Records:* The following page will ask you to upload a file to have greater control over your own medical records.
6) *Choose a File to Upload:* Choose a medical file from your memory you wish to decentralize.
7) *Submit File:* Click on "Submit File" to store your medical record on IPFS through web3.
8) *Unique URL Generation:* Once the medical record is submitted and gets stored on IPFS, a unique URL will be generated and displayed on the screen.
9) *View your Record:* You can view your record by clicking on the link generated in the previous step.



View your Record

VI. CONCLUSION

Blockchain can be considered the most secure and immutable way of storing any information or data with the help of Smart-Contracts. It is very hard or almost impossible to alter even a small part of data although it is a publicly distributed ledger. Blockchain is a technology which can have a huge impact in the healthcare sector. In conclusion, the decentralized file storage system using IPFS and web3storage offers several benefits over traditional centralized storage systems. It allows for secure and efficient storage of files, as well as decentralized access and control over the stored data. This system also provides enhanced privacy and censorship resistance, as well as the ability to easily integrate with other decentralized applications on the blockchain. Overall, the use of IPFS and web3storage in a decentralized file storage system is a promising solution for the future of data storage. Blockchain helps to achieve this as it provides immutability and security to data stored on network. The next development in healthcare that can improve communication between patients and doctors is the use of electronic health records (EHRs).

VII. FUTURE SCOPE

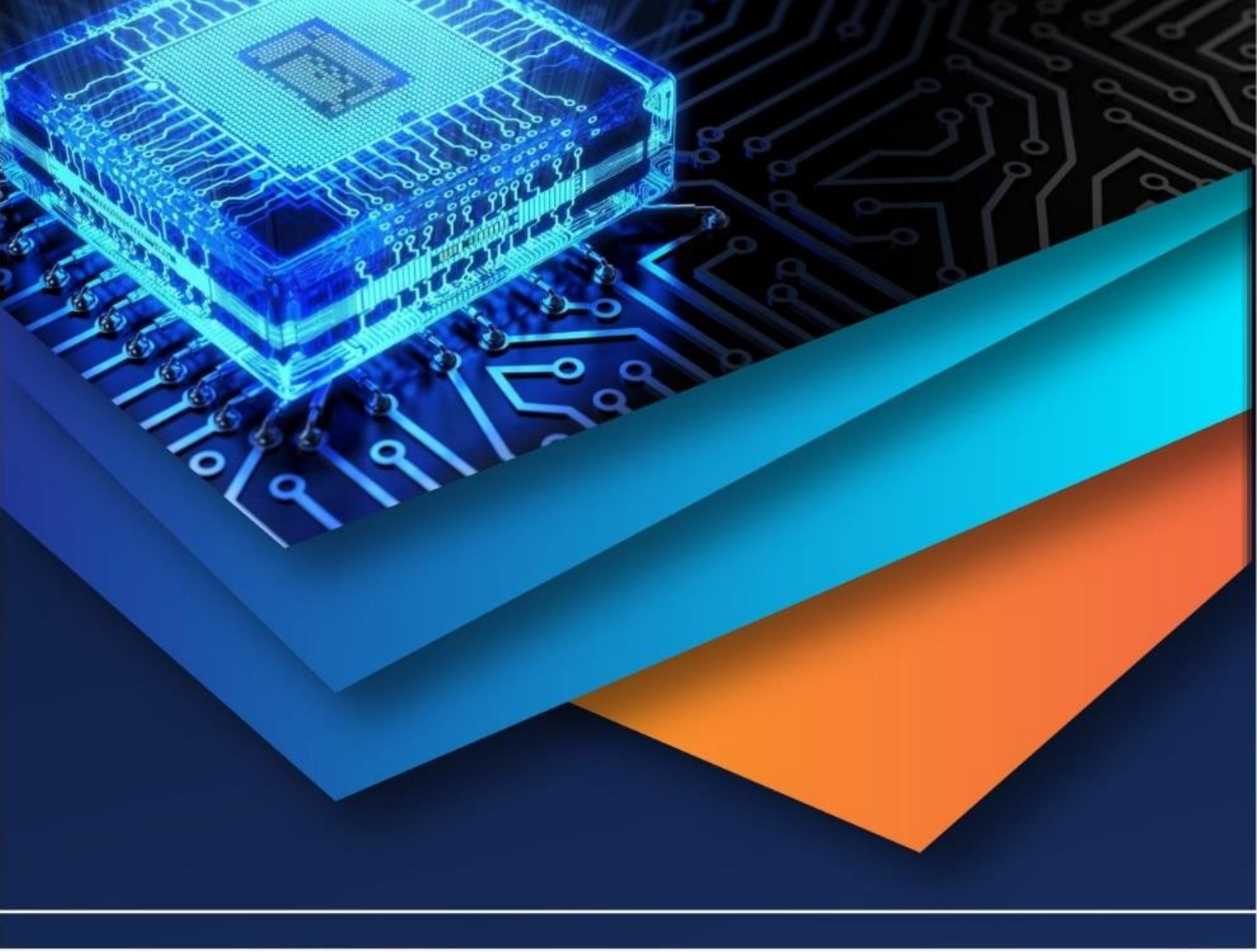
The future of decentralized electronic health record systems is bright. These systems have the potential to revolutionize the way that medical information is stored, accessed, and shared. Here are some potential future developments for decentralized electronic health record systems:

1) *Increased Interoperability:* One of the key challenges with current electronic health record systems is that they are often siloed and not easily accessible to other healthcare providers. In the future, decentralized systems could help to overcome this challenge by allowing healthcare providers to easily access and share patient information, regardless of the specific system they are using.
2) *Improved Security:* Decentralized electronic health record systems use advanced encryption and blockchain technology to protect patient data. This makes them much more secure than traditional centralized systems, which are often vulnerable to cyber-attacks. In the future, this improved security could help to prevent data breaches and protect patient privacy.
3) *Greater Patient Control:* Decentralized electronic health record systems give patients greater control over their own medical information. This means that patients can choose who has access to their data and can easily share it with healthcare providers as needed. In the future, this could help to improve communication between patients and healthcare providers and enable patients to take a more active role in their own healthcare.
4) *More Personalized Care:* Decentralized electronic health record systems can be used to store a wide range of medical information, including genetic data and other personalized health information. In the future, this data could be used to provide more personalized and tailored healthcare to patients. For example, doctors could use the data to develop personalized treatment plans that are tailored to an individual's specific health needs.

Overall, the future of decentralized electronic health record systems is promising. These systems have the potential to improve the quality, accessibility, and security of medical information, ultimately leading to better healthcare outcomes for patients.

REFERENCES

[1] Muhammad Usmana, Usman Qamar "Secure Electronic Medical Records Storage and Sharing .Using Blockchain Technology"
[2] Jin Sun, Xiaomin Yao, Shangping Wang, And Ying Wu. “Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS”
[3] Xiaoguang Liu, Ziqing Wang, Chunhua Jin, Fagen Li, Gaoping Li “Using Blockchain for Electronic Health Records”.
[4] Sami Bourouis, Punit Gupta, Dinesh Kumar Saini, Farjana Khanam Nishi, Mahizebin Shams-E-Mofiz, Mohammad Monirujjaman Khan and Abdulmajeed Alsufyani. “Electronic Healthcare Data Record Security using Blockchain and Smart Contract”
[5] “Electronic Health Record Monitoring System and Data Security Using Blockchain Technology” by Kazi Tamzid Akhter Md Hasib,1Ixion Chowdhury,1Saadman Sakib, Mohammad Monirujjaman Khan, Nawal Alsufyani, Abdulmajeed Alsufyani, and Sami Bourouis.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY