Grenze International Journal of Engineering and Technology, June Issue

MedBlock: Revolutionizing Healthcare Data Management through Blockchain and IPFS

K.V. Deshpande[1], Shubham Nagare[2], Tejas Patil[3], Abhishek Dhanke[4] and Rushikesh Sarode[5]
[1-5]JSPM'S Rajarshi Shahu College of Engineering, Pune-411033, Maharashtra, India
Email: shubhamnagare2002@gmail.com, kvdeshpande_comp@jspmrscoe.edu.in, patiltejashitendra@gmail.com, abhishekrd636@gmail.com, rushisarode2002@gmail.com

Abstract— **MedBlock is a pioneering solution designed to address the critical challenges in contemporary health record management by leveraging blockchain and InterPlanetary File System (IPFS) technologies. This decentralized health record storage system ensures data integrity, security, and user privacy through innovative encryption mechanisms. The blockchain component, based on Ethereum, establishes a tamper-resistant ledger, while IPFS provides a decentralized and distributed file storage infrastructure. Access control mechanisms guarantee that only authorized individuals can retrieve health records, ensuring stringent privacy standards. The user-friendly interface enhances the overall experience, making health record access and management seamless. Through rigorous evaluation, MedBlock demonstrates superior security measures and promising performance metrics, positioning itself as a robust solution for the future of decentralized health record storage. This paper outlines the architecture, implementation details, security measures, user interface, evaluation results, and future enhancements of MedBlock, contributing to the ongoing discourse on blockchain applications in healthcare.**

Index Terms— **MedBlock, Healthcare, Blockchain, IPFS, Decentralization, Security, MERN.**

I. Introduction

MedBlock introduces a revolutionary healthcare technology that combines blockchain and IPFS for decentralized health record storage. This innovative platform ensures secure, transparent, and patient-centric management of health records by leveraging blockchain's immutable ledger and IPFS's distributed storage. With cryptographic encryption and smart contracts, MedBlock provides unprecedented control over health data while automating secure data-sharing among healthcare providers. Its decentralized nature enhances data security, promotes interoperability, and fosters a patient-centric healthcare experience. By addressing concerns about data breaches and privacy infringements, MedBlock establishes trust and cooperation among patients, healthcare professionals, and stakeholders, paving the way for decentralized technologies to transform healthcare data management.

A. Overview

MedBlock pioneers a decentralized health record storage system, addressing challenges in centralized healthcare databases. Integrating blockchain (Ethereum) for tamper-resistant ledgers and IPFS for decentralized file storage, MedBlock ensures data integrity and security. Robust encryption and access control mechanisms enhance user privacy. The user-friendly interface optimizes health record management. Evaluation results demonstrate superior

Grenze ID: 01.GIJET.10.2.91

security measures, positioning MedBlock as a groundbreaking solution. This paper provides a comprehensive overview of MedBlock's architecture, implementation, security measures, user interface, and future enhancements, contributing to the evolving landscape of blockchain applications in healthcare.

B. Challenges

Implementing MedBlock faces challenges in balancing decentralization with scalability, ensuring compatibility with diverse healthcare systems, and addressing interoperability issues. Integrating blockchain and IPFS necessitates meticulous attention to user authentication, complex encryption methodologies, and establishing efficient consensus mechanisms. Additionally, navigating regulatory frameworks and ensuring compliance poses a substantial challenge. Overcoming these hurdles demands a multidisciplinary approach, combining expertise in blockchain technology, healthcare protocols, and cybersecurity. MedBlock's success hinges on adeptly managing these challenges to deliver a secure, decentralized, and user-friendly health record storage solution.

C. Objective

The primary objective of MedBlock is to establish a secure and decentralized health record storage system by leveraging blockchain and IPFS technologies. This involves ensuring data integrity through the immutability of blockchain, preventing unauthorized access or tampering. The system aims to provide robust security measures, including encryption and access control, to safeguard sensitive health information and prioritize user privacy. Additionally, MedBlock seeks to offer a user-friendly interface for seamless health record management. Through these objectives, MedBlock aims to contribute to the evolution of healthcare systems, providing a reliable and innovative solution to the challenges associated with centralized health record compliance.

D. Expected Outcome

The outcome of the MedBlock project is a transformative decentralized health record storage system that enhances data security, privacy, and accessibility. By successfully integrating blockchain and IPFS technologies, MedBlock ensures tamper-resistant health record ledgers and decentralized storage infrastructure. The implementation demonstrates robust encryption mechanisms, stringent access controls, and a user-friendly interface. The project yields a tangible solution to the challenges of centralized health record management, providing a secure and transparent alternative.

II. LITERATURE SURVEY

A increasing number of people are interested in employing blockchain technology to improve the security and accessibility of health information, according to a literature review on a blockchain-based decentralised health record storage system using IPFS. Previous research explores the utilization of IPFS for decentralized file storage, providing an immutable and distributed infrastructure for health data. The studies highlight the advantages of blockchain, such as data integrity and patient-centric control through smart contracts. While advancements are noted, challenges, including concerns about scalability and interoperability, are identified. In order to increase the overall effectiveness and dependability of decentralised health record systems and pave the way for more safe and patient-centered healthcare solutions, researchers are actively investigating strategies to overcome these problems.

A. A Decentralised Health Record Storage System Utilising IPFS and Blockchain

The implementation of a decentralized health record storage system using blockchain and IPFS incorporates various models and algorithms. This approach aims to enhance the security and accessibility of health records by leveraging blockchain technology and the distributed storage capabilities of IPFS. The primary objective is to ensure data integrity and patient-centric control, addressing issues such as unauthorized access and tampering. By employing these techniques, the system strives to create a secure and transparent environment for health record management, ultimately contributing to improved healthcare outcomes.

B. Healthcare record storage based on blockchain algorithm

In a comprehensive review by A. Patel et al. [2] (2021), the application of a Blockchain-Based Decentralized Health Record Storage System using IPFS is explored. The paper delves into the utilization of IPFS for secure and decentralized health data storage, coupled with blockchain for ensuring data integrity. The study highlights the effectiveness of this system in providing patient-centric control over health records and preventing unauthorized access. The research emphasizes the potential of this approach to revolutionize health record management, ensuring transparency and security in the healthcare domain.

C. Literature Review (2014- 2022)

In 2019, a study [1] analysed read and write transactions to see how well the blockchain network may support the sharing of Electronic Health Records (EHRs). File sharing worked well during testing, with few data transfer lags. Patients were able to add or remove information according to their choices through the use of smart contracts and cryptography techniques.

In 2018, another research effort [2] focused on ensuring patient ownership and accessibility of medical records. The study placed a strong emphasis on patients' complete control and the access to a single, unified picture for healthcare professionals, which encouraged a thorough comprehension of individuals' medical historiesHowever, concerns were raised about the cost of storing electronic patient record (EPR) data.

A 2019 study [3] proposed a system combining secure record storage with granular access controls using IPFS for off-chain storage. Future plans called for adding a payment module to the decentralised blockchain system that would calculate the cost of a doctor's consultation. The emphasis was on addressing data storage concerns with a focus on confidentiality, authentication, and integrity.

In 2020, a study [4] presented a patient information management method utilizing RSA and Diffie Hellman encryption techniques with SHA256 acting as an integrity check. The study acknowledged the need for improvements to increase security while simplifying the system for user-friendliness. Despite its security measures, the system was deemed not cost-effective and lacked integrity assurance.

Another 2020 article [5] proposed a blockchain-based off-chain solution framework maintaining system compatibility features. It incorporated authentication keys for user data access control, emphasizing user empowerment over data access. The framework utilized IPFS for off-chain solutions while allowing users to control who accesses records and for how long.

In 2019, a research effort [6] highlighted the necessity to address scalability, interoperability, and regulatory compliance issues in healthcare. Enhancing the blockchain-based EHR systems' scalability, interoperability, and regulatory compliance was the goal of the suggested approach. The study investigated digital signatures and public-key cryptography as safe methods of transferring data between authorised parties.

A 2020 article [7] discussed the benefits of blockchain for patient access to medical records, emphasizing autonomy, privacy, security, and decreased administrative load. Challenges included interoperability, regulation, and network effects. Future research suggestions included developing new solutions addressing regulatory and interoperability issues, promoting adoption, and exploring applications in other industries.

In 2022, a report [8] highlighted challenges with implementing blockchain-based EHR systems, such as interoperability and regulatory constraints. The creation of interoperability standards, performance and scalability measurement, and implementation issues were among the future study areas. The paper proposed multiple avenues for the advancement of EHR management based on blockchain technology.

Another 2022 article [9] described a proposed solution for blockchain-based EHR management, including a permissioned blockchain network, decentralized storage, smart contracts, and a patient mobile application. The authors discussed potential benefits, financial feasibility evaluation, and exploration of blockchain-based solutions in other healthcare fields.

In 2020, a study [10] proposed a solution integrating attribute-based access control and blockchain technology for medical data sharing, ensuring privacy and security. The paper suggested future research analyzing trends and patterns of blockchain adoption in healthcare and factors influencing adoption.

In 2019, a research paper [11] highlighted the crucial role of enhanced EHR systems in the progress of healthcare. Blockchain-based systems were recognized for their greater potential impact on the future of EHR systems compared to conventional systems. The survey paper suggested an update on emerging systems and an analysis of their strengths and weaknesses.

A 2021 paper [12] proposed a blockchain-based solution for secure, decentralized patient medical record management. It outlined an EHR architecture, blockchain framework, and data storage block for secure sharing. The paper suggested a survey analyzing the slow adoption of blockchain-based systems in healthcare.

In 2016, a study [13] conducted a systematic literature review on the use of Blockchain technology in Electronic Health Records (EHRs), identifying key challenges, issues, and potential benefits. The survey paper could explore strategies for improving usability and user experience in blockchain-based EHRs.

In 2017, MedRec [14] demonstrated how blockchain technology could implement decentralization principles in managing electronic medical records. The survey paper could investigate extending MedRec's use cases beyond medical data access and permission management for other healthcare applications.

D. Why should we use IPSF for data storage?

The integration of IPFS (InterPlanetary File System) for data storage holds paramount significance. IPFS offers a decentralized and peer-to-peer approach to storing and retrieving data, aligning seamlessly with the objectives of MedBlock's blockchain-based decentralized health record storage system.

Firstly, IPFS's decentralized architecture contributes to enhanced data security. Traditional centralized storage systems are vulnerable to single points of failure and are more susceptible to hacking attempts. In contrast, IPFS distributes data across a network of nodes, reducing the risk of data breaches and unauthorized access.

Secondly, IPFS facilitates efficient and reliable data accessibility. Its peer-to-peer network allows for faster retrieval of information by fetching data from multiple nodes simultaneously. This decentralized approach is particularly advantageous in the healthcare context, where timely access to accurate health records can be critical for informed decision-making and patient care.

Moreover, IPFS promotes data integrity by utilizing content addressing. Each piece of data is uniquely identified by its content, making it resistant to corruption or manipulation. This aligns with MedBlock's commitment to maintaining the integrity of health records through cryptographic measures, collectively establishing a robust system for ensuring the reliability and trustworthiness of stored data.

III. PROPOSED ARCHITECTURE

Module 1: Patient Data Addition in MedBlock

It focuses on the secure addition of patient data to the decentralized health record storage system, employing blockchain and IPFS technologies. The process begins with user authentication, ensuring the secure identification of authorized users through cryptographic methods and user credentials. A smart contract is then initialized to facilitate the addition of patient data, defining conditions to enforce data integrity and access control. Patient data is encrypted using robust encryption algorithms, with the patient's public key employed for added security. The system creates a blockchain transaction to record the addition of patient data, utilizing a consensus algorithm for validation. For decentralized off-chain storage, IPFS is integrated, generating a unique hash for data referencing. The smart contract is updated to include the IPFS hash, establishing a link between the blockchain and off-chain data. The success of the transaction and IPFS storage is confirmed, and relevant details are provided in a transaction receipt. Events are logged in the blockchain for auditing purposes, capturing essential details such as timestamps, user IDs, and transaction status. Upon successful addition of data, users are notified, including instructions on securely accessing and sharing their information.

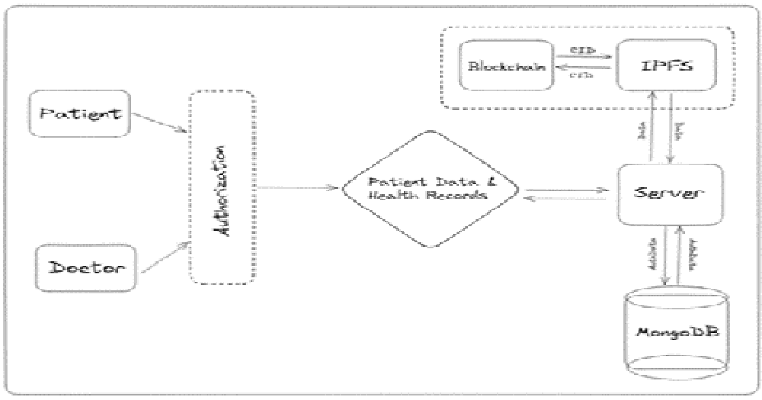


Fig. High Level Data Flow Diagram

Module 2: IPFS Integration in MedBlock

MedBlock focuses on the seamless integration of IPFS to enhance the decentralized health record storage system. The first step involves setting up IPFS nodes within the MedBlock infrastructure, configured for optimal performance and reliability. Subsequently, the module facilitates the secure upload of encrypted patient data to the IPFS network, generating unique and dynamic IPFS hashes for each health record to ensure content integrity and efficient referencing.

These IPFS hashes are then linked to the blockchain through updates to the smart contract, establishing a tamper-proof connection between on-chain transactions and off-chain data storage. Users and authorized entities can directly retrieve health records from IPFS, with the system incorporating mechanisms for efficient data retrieval within the user interface.

Monitoring tools and maintenance protocols are implemented to track the health and performance of IPFS nodes, promptly addressing any issues or node failures. The module concludes with a focus on user education and support, providing clear guidance on IPFS usage for accessing and managing health records, and offering support mechanisms for user inquiries and concerns related to IPFS integration. Through these steps, Module 2 fortifies MedBlock's capabilities, leveraging IPFS to create a robust and secure ecosystem for decentralized health record storage and management.

Module 3: Content ID Integration on Blockchain in MedBlock

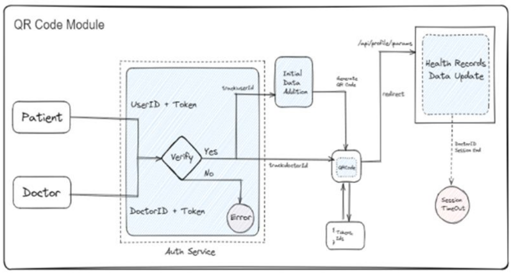
In MedBlock is dedicated to the integration of Content ID on the blockchain, a crucial step in ensuring the traceability and authenticity of health records stored on the decentralized IPFS network. The module begins with the establishment of a robust Content ID system that generates unique identifiers for each health record. These Content IDs, derived from the IPFS hashes, serve as a secure and verifiable link between the on-chain transactions and the off-chain health data. The smart contract is updated to include these Content IDs, effectively anchoring the health records on the blockchain.

Through this connectivity, users, healthcare providers, and other authorised entities can directly verify the legitimacy of health records on the blockchain, improving the system's openness and auditability. By embedding Content IDs in the blockchain, MedBlock ensures an immutable and tamper-resistant record of each transaction and associated health data. This module not only strengthens the integrity of the decentralized health record storage but also facilitates streamlined verification processes. Content IDs become the backbone of trust within the system, providing a clear and unforgeable reference for each health record.

Additionally, the Content ID integration contributes to the overall security posture of MedBlock by leveraging the blockchain's inherent security features. It establishes a seamless connection between Content IDs and the blockchain within MedBlock, reinforcing the system's commitment to data authenticity and transparency. This integration enhances the reliability and trustworthiness of health records stored on IPFS, setting the stage for a robust and secure decentralized health record storage system.

Module 4: QR Code Module

A key component of a Blockchain-based Decentralised Health Record Storage System that uses IPFS is the QR code module, which allows medical professionals—especially physicians—to securely and quickly access patient data. Patient health records are securely stored on IPFS, a decentralized file system ensuring data integrity and availability across a distributed network of nodes. The blockchain component manages access control and records transactions related to patient data, with each record and its permissions stored as transactions. When a patient desires to grant access to their health records, a QR code is generated containing pertinent information such as patient identity, specific records, and access permissions. Smart contracts on the blockchain enforce access rules, and upon scanning the QR code, the doctor triggers a transaction that verifies their identity and permissions. Access is granted if conditions are met, leading to real-time retrieval of patient data from IPFS. The entire process, including consent, access attempts, and data retrieval, is recorded as an immutable audit trail on the blockchain, ensuring transparency, accountability, and heightened security in the management of sensitive health information.



QR code Module

IV. MATHEMATICAL DESCRIPTION OF PROPOSED MODEL

1. Blockchain Consensus Model

Describe the MedBlock consensus algorithm, including Proof-of-Work (PoW) and Proof-of-Stake (PoS). If applicable, include equations describing the probability of a node successfully adding a block to the chain based on the consensus mechanism.

2. Blockchain Security Model

Detail the cryptographic algorithms employed for securing transactions and data integrity. If relevant, include mathematical representations of hashing functions, digital signatures, or other cryptographic protocols used.

3. Smart Contracts Logic

Provide an overview of the smart contracts used in MedBlock and their logic. If possible, include formalized representations of the conditions and actions specified in the smart contracts.

4. Decentralized Storage (IPFS)

Outline the mathematical aspects related to IPFS, such as data distribution, replication, and retrieval time. If applicable, include equations representing data distribution, content addressing, and data retrieval time.

5. Data Encryption Model

Explain the mathematical models governing data encryption and user privacy measures. If feasible, include representations of cryptographic algorithms ensuring data privacy.

6. User Control and Privacy Model

Discuss mathematical representations of user permissions, access control, and privacy-preserving techniques. If applicable, include mathematical expressions for user-controlled access and privacy preservation.

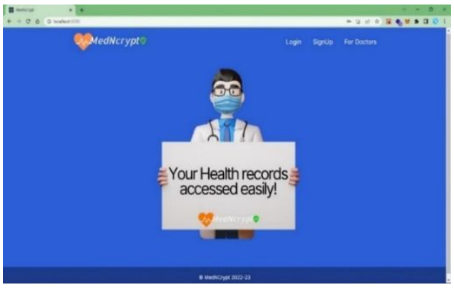
7. System Performance Metrics

Highlight mathematical models for system performance metrics, including transaction throughput and confirmation times. Include relevant equations representing the efficiency and performance of the MedBlock system.

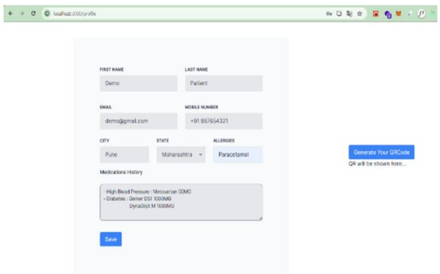
8. Interoperability Model

Describe mathematical considerations for ensuring interoperability with existing healthcare systems and standards. If applicable, provide representations of data mapping, translation, and cross-system communication.

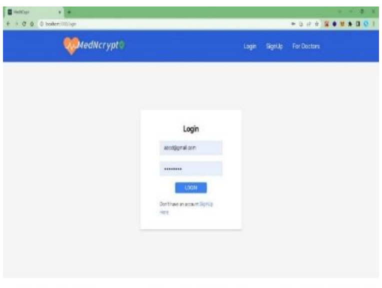
V. RESULT



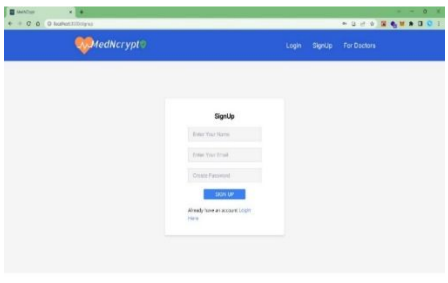
Home Page



New Patient Data Addition Form



Patient Signup



Patient Login

- *Frontend*

1. Framework/Library

React.js: React.js is a well-liked JavaScript user interface library. React is renowned for its efficient component-based architecture.

2. State Management

Redux: A reliable state container designed for JavaScript programmes. It could be used to manage the state of the frontend application, especially if there are complex data flows.

3. User Interface (UI) Design

Material-UI or Ant Design: Libraries that provide pre-designed components following the principles of Material Design or Ant Design, offering a consistent and visually appealing UI.

4. Data Visualization

D3.js: If there is a need for complex data visualization, D3.js is a powerful JavaScript library for creating interactive and dynamic data visualizations.

5. Web3 Integration (Blockchain Interaction)

Web3.js: A JavaScript library that allows interaction with the Ethereum blockchain. It could be used for integrating blockchain functionality into the frontend.

• *Backend*

1. Server-Side Technology

Node.js: A server-side JavaScript runtime that is commonly used for building scalable and fast network applications.

2. Web Framework

Express.js: A basic and versatile Node.js web application framework that delivers a rich set of functionality for web and mobile applications.

3. Blockchain Integration

Ethereum Smart Contracts: If MedBlock is built on the Ethereum blockchain, the backend might interact with Ethereum smart contracts to manage health record transactions.

4. Decentralized Storage Integration (IPFS)

IPFS.js: A JavaScript implementation of the IPFS protocol that enables interaction with the InterPlanetary File System. This could be used for storing and retrieving health records.

5. Database

MongoDB: A NoSQL database that is schema-less and can handle large amounts of data, for the authorization of patients and doctors.

6. Authentication and Authorization

JSON Web Tokens (JWT): A standard for securely transmitting information between parties, often used for authentication purposes.

A. IPFS used

In MedBlock, integrating IPFS (Inter Planetary File System) is crucial for secure medical record preservation. IPFS, a decentralized storage system, complements blockchain transparency and immutability. Each record is uniquely identified through content addressing via cryptographic hashing. This hash serves as the record's address on the IPFS network. IPFS tackles challenges in healthcare record management by decentralizing storage, eliminating single points of failure, and enhancing resilience. Health records are distributed across nodes, reducing data loss and unauthorized access risks.

IPFS's peer-to-peer architecture enables efficient data retrieval, promoting accessibility and user control. It ensures data integrity by making records tamper-resistant through content addressing. Any alteration to data changes its unique hash, immediately signalling compromise. This aligns with MedBlock's security goals, maintaining trust and accuracy. IPFS supports MedBlock's decentralized ethos by empowering users with control over their health data. Overall, IPFS integration in MedBlock enhances data security, accessibility, and integrity, reinforcing its effectiveness in healthcare record management.

B. Software used

MedBlock revolutionizes healthcare record management through a blend of cutting-edge software components. Blockchain technology, including Ethereum and Hyperledger Fabric, forms its core, ensuring immutable ledgers and controlled access to patient data. Complementing this, MedBlock utilizes IPFS for decentralized storage, enhancing data security and accessibility across distributed networks. IPFS's content-based addressing boosts data retrieval efficiency while mitigating centralized storage risks. Encryption methods like SHA-256, AES, and RSA fortify patient record security, guaranteeing end-to-end confidentiality.

Beyond blockchain and IPFS, MedBlock features a user-friendly interface developed with modern web technologies. This interface facilitates seamless interaction for patients and healthcare providers, enabling record access, appointment scheduling, telemedicine consultations, and potential AI-driven diagnostics. MedBlock stands as a paradigm of secure and efficient healthcare data management, leveraging state-of-the-art technologies to meet evolving industry demands.

VI. CONCLUSION

In conclusion, MedBlock represents a significant leap forward in healthcare technology, presenting a robust and secure solution for health record management. By harnessing the power of blockchain and integrating seamlessly with IPFS, MedBlock addresses critical challenges in data security, transparency, and accessibility within the healthcare ecosystem.

The utilization of blockchain ensures the immutability and transparency of health records, safeguarding against unauthorized access and tampering. Complementing this, the decentralized architecture of IPFS provides a reliable and efficient storage mechanism, granting users control over their health data and promoting accessibility from anywhere.

MedBlock's emphasis on cryptographic encryption not only guarantees data integrity but also prioritizes user privacy. The implementation of smart contracts streamlines data-sharing processes, facilitating secure collaboration among healthcare providers while upholding the confidentiality of patient information.

By fostering interoperability and decentralization, MedBlock stands as a beacon of innovation, offering a trust-centric environment that enhances collaboration between patients and healthcare stakeholders. The platform not only addresses current concerns regarding data breaches but also sets the stage for a future

In essence, MedBlock paves the way for a transformative shift in healthcare information systems, where the integration of blockchain and IPFS creates a resilient and patient-friendly ecosystem. As we move towards an era of digital healthcare, MedBlock stands at the forefront, embodying the principles of security, transparency, and accessibility in health record storage and management.

REFERENCES

[1] Jack Huang, Yuan wei Qi, Muhammad Rizwan Asghar, Andrew Meads, and Yu-Cheng ,New Zealand2019 18th IEEE International Conference on Trust, Security and Privacy.

[2] Sofia Alexaki, George Alexandris, Vasilis Katos, Nikolaos E. PetrouLakis “Blockchain Based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions”.2018 IEEE Workshop on Computer Aided Modelling and Design of communication Links and Network.

[3] AYESHA SHAHNAZ, USMAN QAMAR, AND AYESHA KHALID, (Member, IEEE). “Using Blockchain for Electronic Health Records” 2019 IEEE Access

[4] Kavga Yapa Abeywardena, Buddhima Attanayaka, Kabilashan Periyasamy, et. al. “Blockchain based Patients' detail management System” 2020 2nd International Conference on Advancements in Computing (ICAC). Piran. “A Blockchain-Based Credibility Scoring Framework for Electronic Medical Records” 2020 IEEE Globecom Workshops (GC Wkshps)

[5] Siva Rama Krishnan S, Manoj M.K, Thippa Reddy Gadekallu, Neeraj Kumar, Praveen Kumar Reddy Maddikunta, S. Bhattacharya, D. Y. Suh, and M. J. Piran. “A Blockchain-Based Credibility Scoring Framework for Electronic Medical Records” 2020 IEEE Globecom Workshops (GC Wkshps)

[6] Mathis Steichen, Fiz Beltran, Norvill Robert, Shabir Wazen And Radu Sedan “Blockchain Based Decentralised Access Control For Ipfs” 2018 Ieee Confs On Internet Of Things, Green Computing, Cyber, Social Computing And Physical, Smart Data, Blockchain, Information Technology And Computer.

[7] Ammar Battah, Mohammad Madine (Ieee Member), Ibrar Yaqoob, Raja Jayaraman, (Senior Ieee Member), Khaled Salah, (Senior Ieee Member), Yousof Al-Hammadi, Samer Ellahham And Sasa Pesic, “Blockchain For Giving Patients Control Over Their Medical Records” Receive On September 27, 2020, Accept On October 15, 2020, Publication Date October 20, 2020, Date Of Latest Version November, 2020.

[8] Abdullah Al Mamun, Sami Azam, (Member, Ieee), And Clementine, “Electronic health records management using blockchain a thorough review and future research directions”

[9] Alixandra Taylor, Austin Kugler, Praneeth Babu Marella, And Gaby G. Dagher ,Coeur D’alene, “A Blockchain-Based Method for the Healthcare Supply Chain Using Decentralized Storage Systems and Smart Contracts”

[10] Zhijie Sun, Dezhi Han , Dun Li, Xiangsheng Wang, Chin-Chen Chang. "A Blockchain-based Secure Storage Scheme for Medical Information".

[11] R. Shanthapriya, V. Vaithianathan, Seitz, Juergen, Rifi, Nabil, Alla, Sujatha, Liu, Jingwei. "An Extensive Survey on Blockchain-Based Electronic Health Record Systems" Receive On September 22, 2020, Accept On October 10, 2020, Publication Date October 26, 2020.
[12] Prof. Rohini Hanchate, Samriddhi Garudik, Shruti Chavan, Naisargi Bajpai. "Blockchain for giving patients control over their healthcare records".
[13] Yue X, Wang H, Jin D, et al. “Electronic health records in a Blockchain: A systematic review J Med Syst “ 2016; 40(10): 218.
[14] Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman, Media Lab, “MedRec: Using Blockchain for Medical Data Access and Permission Management”