e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal Of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704114 |

Secure Medical Record Management Using Blockchain Technology

Mrs. S. Bhagya Rekha, P. Varun Reddy[2], CV. Sai Phanish Reddy[3], Y. Dhilip Reddy[4]

Assistant Professor, Department of CSE, Anurag University, Telangana, India

Student, Department of CSE, Anurag University, Telangana, India

Student, Department of CSE, Anurag University, Telangana, India

Student, Department of CSE, Anurag University, Telangana, India

ABSTRACT: In today's digital landscape, the vulnerability of personal information, particularly medical data, looms large. Safeguarding medical records against unauthorized access is paramount. This project endeavors to create a robust and secure application leveraging blockchain technology for storing medical records. Through the Ethereum blockchain network, a series of smart contracts will be developed and maintained to ensure the integrity and confidentiality of medical data. The cornerstone of this application lies in its meticulous registration process for hospitals, granting authorized access to input and retrieve medical details. By restricting entry solely to registered hospitals, the system fortifies the security of medical records. This approach ensures that only authorized entities can interact with sensitive medical data, thereby minimizing the risk of unauthorized access or data breaches. Through the implementation of smart contracts, a suite of operations will be orchestrated to safeguard medical records on the internet. Encryption techniques will be employed to shield data from prying eyes, while the immutable nature of blockchain technology will uphold the integrity of records.

KEYWORDS: Smart contracts, Blockchain, Ethereum, Solidity programming, Meta Mask, Ganache, NFT, De-centralized application, Ethereum Virtual Machine, Ether, Remix IDE, Gas fee, Web3.

I. INTRODUCTION

In contemporary times, the significance of information security cannot be overstated across various domains. With data misuse capable of inciting chaos and profound disruptions, safeguarding information is imperative. Data holds immense value to individuals and society alike, making its protection a top priority. Threat actors, such as hackers and intruders, constantly probe databases and servers of social media platforms and other applications, seeking to exploit vulnerabilities for personal gain. Thus, robust security measures are indispensable to thwart unauthorized access and prevent data exploitation.

Information security encompasses more than just barring unauthorized users; it extends to ensuring data integrity, accessibility, and confidentiality. Health data, in particular, holds immense significance in an individual's life, often containing personal details, diagnosis, and treatment information. The confidentiality and integrity of such data are paramount, as individuals are hesitant to disclose sensitive health information to others. However, traditional methods of storing and accessing medical data in hospitals are prone to security breaches, posing significant risks to data integrity and confidentiality.

Despite advancements in technology, including cloud services offering expansive storage and management capabilities, concerns regarding security persist. While cloud technology provides scalability and convenience, relying on third-party services introduces inherent risks. Cloud vendors levy charges based on storage usage and service utilization, making it imperative to weigh the cost against the security implications.

Addressing these challenges necessitates innovative approaches to information security, particularly in the healthcare sector. Implementing robust encryption protocols, access controls, and auditing mechanisms can bolster data protection measures. Moreover, fostering collaboration between healthcare institutions to establish secure data-sharing frameworks can enhance interoperability while safeguarding patient privacy.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704114 |

II. LITERATURE SURVEY

Ayesha Shahnaz, Usman Qamar, and Ayesha Khalid[1] highlight the potential of blockchain technology to revolutionize electronic health record (EHR) systems. While various industries have already capitalized on blockchain's benefits, they argue that the healthcare sector stands to gain significantly from its implementation, particularly in terms of security, privacy, and decentralization. In their article, they acknowledge the existing challenges faced by EHR systems, including issues related to data security, integrity, and governance. They propose leveraging blockchain technology to address these challenges and offer a solution in the form of a comprehensive framework for implementing blockchain in EHR healthcare. The primary objective of their framework is two-fold: firstly, to integrate blockchain technology into EHR systems, and secondly, to ensure secure storage of electronic records. They emphasize the importance of defining precise access rules for users within the framework to maintain data security and integrity. Furthermore, the authors tackle scalability concerns inherent in blockchain technologies by incorporating off-chain storage of records into their framework. This approach aims to provide EHR systems with the benefits of scalability, security, and comprehensiveness offered by blockchain-based solutions. Overall, their proposed framework presents a promising approach to transforming EHR systems by harnessing the potential of blockchain technology while addressing critical issues related to data security, integrity, and scalability.

William J. Gordon and Christian Catalini delve into the shifting landscape of interoperability within healthcare, moving from a traditional focus on data exchange between commercial entities to a more patient-centric approach. They highlight the emergence of patient-centric interoperability, which redefines data exchange around the patient's needs and preferences. This shift brings forth a new set of challenges and requirements across security, privacy, technology, incentives, and governance that must be addressed for successful data sharing on a large scale. The authors propose that blockchain technology can serve as a catalyst for this transformation through five key mechanisms: (1) digital access rules, (2) data aggregation, (3) data mobility, (4) identity of the patient, and (5) immutability of the data. However, the authors acknowledge several barriers to achieving patient-centric interoperability through blockchain technology, including concerns related to clinical data transaction volume, privacy and security, patient engagement, and incentivization. Despite these challenges, they emphasize the promising trend of patient-centric data sharing in healthcare. They argue that blockchain technology holds significant potential to facilitate the transition from institution-centric to patient-centric data sharing, promising a future where patients have greater control over their healthcare data and its exchange.

Gulara Muradova and Mehran Hematyar This paper explains about the delve into the burgeoning utilization of technology within the healthcare industry, propelled by the rapid digitization sweeping across global healthcare domains. They spotlight blockchain as a prominent technology trend renowned for enhancing data security and fortifying defenses against digital thefts and cyberattacks. The authors elucidate the concept of blockchain, deriving its name from the amalgamation of "block" and "chain," signifying a sequential chain of interconnected blocks. Blockchain, as expounded, operates as a decentralized information and reporting system wherein any form of information can be entered and recorded within blocks. Highlighting the intrinsic value of healthcare data, encompassing electronic-based medical records, patient registries, and histories, Muradova and Hematyar- underscore the potential for extracting valuable insights through data mining techniques. They emphasize the significance of accessing and analyzing healthcare data to identify correlations among patients, behaviors, medical conditions, and demographic factors, facilitating early warning triggers for preventive care management. Within the blockchain framework, information is securely stored within blocks and shared among network participants, rendering it nearly impossible to delete or manipulate recorded information due to encryption protocols. They illustrate the immutability of blockchain through a hypothetical scenario wherein each block represents a clinic recording patient names and records. Any attempt to alter patient information within a block would result in a change in the block's hash, subsequently invalidating subsequent blocks—a fundamental characteristic underscoring the security and integrity of blockchain technology. In essence, Muradova and Hematyar's paper serves as a comprehensive exploration of the potential of blockchain technology in revolutionizing healthcare data management, emphasizing its role in enhancing security, transparency, and data integrity across healthcare systems worldwide.

Zhijie Sun, Dezhi Han, Dun Li, Xiangsheng Wang, Chin-Chen Chang, and Zhongdai Wu emphasize the critical importance of safeguarding the privacy and security of medical data within the public sector. They highlight that medical information often contains sensitive personal and diagnostic data of patients, making it imperative to adopt

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704114 |

robust security measures. In light of recent technological advancements, the healthcare sector is undergoing a transformation in how medical information is managed and stored. The authors advocate for the application of blockchain technology in medical information management, citing its decentralized nature and secure storage capabilities facilitated by distributed consensus and authentication mechanisms. They argue that blockchain technology has the potential to enhance various aspects of the healthcare sector, including security and user experience. Before the advent of modern technology, healthcare institutions relied on inefficient and insecure paper-based systems for storing medical records. By contrast, blockchain technology offers a decentralized approach that distributes information and enables shared ownership of data. Transactions on blockchains are securely hashed and managed by a peer-to-peer network, providing enhanced security measures. Overall, the authors underscore the potential of blockchain technology to revolutionize medical information management, offering a secure, decentralized solution that empowers patients and enhances data security within the healthcare sector.

III. PROBLEM STATEMENT

The medical record maintenance application leveraging blockchain technology aims to enhance data security and transparency by restricting certain users from modifying data and adding blocks to the existing blockchain network. This core objective ensures that only authorized users have access to the system, preserving the authenticity of the data. Another key objective of the application is to uphold transparency in the medical data entered into the network. By utilizing blockchain technology, the application ensures that all transactions are recorded in a transparent and immutable manner, providing a clear audit trail of data entries and modifications. An analysis of the existing system reveals several disadvantages, prompting the development of the proposed system. Blockchain technology enables the maintenance of transaction ledgers across the network, promoting transparency by allowing all users to access transaction history. Additionally, this property of the application eliminates data redundancy by ensuring that each patient's medical data is stored securely on the blockchain without duplication. Overall, the proposed system leverages blockchain technology to overcome the limitations of the existing system, providing enhanced security, transparency, and efficiency in medical record maintenance while offering a user-friendly experience for authorized users.

3.1 Existing System

In the medical field, a vast amount of data accumulates daily, encompassing various patient details such as personal information, diagnoses, and treatment records. Historically, this data has been stored either on hard disks/drives or on third-party servers. However, traditional storage systems, relying on general servers and personal computers, are highly susceptible to security attacks and breaches. Hospitals often rely on third-party servers for medical data maintenance, yet these systems typically lack robust security measures. Authentication is often minimal, with weak or absent password protocols. Consequently, such systems offer inadequate security assurances, leaving data vulnerable to breaches and unauthorized access. The existing system thus suffers from significant disadvantages in terms of data security and integrity. In summary, the current reliance on traditional storage methods and third-party servers for medical data management poses considerable security risks and shortcomings.

3.2 Proposed System

Considering the drawbacks of the current system, it's evident that blockchain technology offers numerous advantages. Blockchain is inherently resistant to many cyberattacks and can efficiently handle large-scale data management. In this context, a web application serves as the interface for users to interact with the blockchain network, where all generated data is stored in blocks. The primary users of this application are doctors and patients. Patient details are securely stored within blocks on the blockchain network, with new blocks continually added as new data is generated. Only doctors have the authority to modify the data within the network, and they are solely responsible for adding patient details. Additionally, the application integrates smart contracts to facilitate backend transactions. Smart contracts authenticate users on the blockchain network, verifying their ownership and granting access to make necessary data changes. These contracts utilize unique IDs or hash values to validate users' actions within the network. In essence, this proposed system offers enhanced security and advantages compared to the existing medical record maintenance system

IV. SPECIFICATIONS

The medical record maintenance application is designed to manage the daily influx of patient data in the healthcare sector. As individuals seek treatment at various hospitals, doctors diagnose and treat them, leading to the accumulation

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704114 |

of extensive medical records. Traditionally, such data is stored on hard disks or third-party servers, which pose inefficiencies and vulnerabilities to cyberattacks. In response to these challenges, the primary objective of the application is to ensure the security of patients' medical data and personal information. This goal is achieved through the utilization of blockchain technology, renowned for its decentralized and ledger-based architecture. By leveraging blockchain, the application enhances data security, as information becomes immutable and resistant to tampering once entered into the network.

Ultimately, the main aim of the medical record maintenance application is to provide a secure platform for storing and accessing sensitive medical data. Through the implementation of blockchain technology and smart contracts, the application achieves this objective while also ensuring that all users within the network are authenticated and authorized to access the data. This innovative approach has the potential to revolutionize the healthcare industry, enhancing patient care by offering increased accessibility and security of medical data

Software Specifications
Backend:
• Solidity Programming (Smart Contracts)
• Meta Mask (Account)
• Ethereum Blockchain Network (Ganache)
UI:
• HTML
• CSS
• JavaScript
• Bootstrap

V. SYSTEM DESIGN AND ANALYSIS

The Medical Record Maintenance Application is a web-based platform designed to centralize patient, doctor, and hospital details using blockchain technology, ensuring data security and accessibility. The application facilitates registration for hospitals, doctors, and patients, each receiving a unique identifier (ID) upon registration. This unique ID is crucial for authentication and access control, ensuring that only authorized users can interact with specific data.

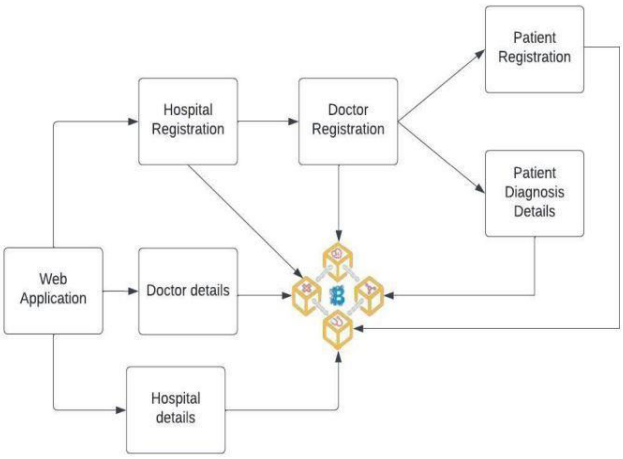
The registration process begins with hospitals registering themselves by providing necessary details, generating a unique ID that serves as their ownership record. Subsequently, hospitals can register doctors, assigning them unique IDs for identification within the network. Doctors, once verified, gain access to add patient details, including personal information, diagnosis, and treatment records. Only doctors have the authority to add or modify patient data, enhancing data integrity and security.

Patients are granted limited access, enabling them to view their own medical records using their unique ID. They cannot access or modify data belonging to other patients, maintaining privacy and confidentiality. Similarly, consultant doctors can access and modify patient data within their network, ensuring continuity of care.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704114 |



Blockchain technology underpins the application, storing all transactions in distributed ledgers accessible to all network participants. Each transaction, represented as a block, is added to the blockchain using hash values, ensuring data integrity and transparency. This distributed ledger system eliminates the need for a centralized backend, as copies of ledgers are maintained by all network peers, ensuring data redundancy and resilience.

The use of unique IDs enhances security and access control, ensuring that each user can only access their specific data. This approach prevents unauthorized access to sensitive medical information and simplifies data retrieval for users. Overall, the application leverages blockchain technology and unique IDs to provide a secure, transparent, and efficient medical record management system, improving data security and accessibility for all stakeholders.

VI. IMPLEMENTATION

6.1 Modules

Hospital Module:

The Hospital module is a fundamental component of the medical record maintenance application, responsible for managing the essential details of registered hospitals. This module facilitates the registration process by collecting pertinent information about each hospital. Key details gathered during registration include the hospital's name, contact number, address, and other relevant information

Doctor Module:

In the doctor module of the medical record maintenance system, hospitals can register doctors by entering their basic details such as name, age, experience, specialization, qualifications, and contact information. Hospitals have exclusive access to verify and modify the doctor's details. While doctors and other users can view the doctor's information, they are unable to make any changes. Additionally, the system verifies the hospital's ownership to ensure authorized modifications to the doctor's details.

Patient Module:

In the patient module of the medical record maintenance application, only doctors can add or modify patient details stored in the blockchain network. Patients can only view their own details and are restricted from accessing information about other patients. Doctors, authenticated with patient IDs, have the authority to view and update patient information, ensuring privacy and data integrity.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704114 |

6.2 Introduction to the technologies used:

Solidity programming:

Solidity is a statically typed, object-oriented programming language similar to Java, tailored for Ethereum's blockchain. It facilitates the creation of smart contracts, enabling automatic execution based on predefined conditions. With features like inheritance, libraries, and complex user-defined types, Solidity empowers developers to build robust smart contracts. Utilizing Remix IDE, developers can efficiently write, test, and deploy Solidity-based smart contracts on the Ethereum blockchain, ensuring security and trust in decentralized applications.

Meta Mask:

MetaMask, a Google Chrome extension, serves as both a software cryptocurrency wallet and a tool for creating Ethereum accounts. Users can manage keys, broadcast transactions, and securely interact with decentralized applications via the extension or mobile app, facilitating seamless Ethereum-based transactions and token management.

Ethereum blockchain network:

Ethereum provides a decentralized platform for deploying immutable applications via smart contracts. Unique to Ethereum is the creation and exchange of Non-Fungible Tokens (NFTs), verifying ownership of digital assets. Ether (ETH) is Ethereum's native cryptocurrency, used for rewarding miners and paying transaction fees. The Ethereum Virtual Machine (EVM) executes Solidity programs, ensuring secure and decentralized smart contracts. Ethereum empowers developers to build decentralized applications while pioneering innovative value creation through NFTs and smart contracts.

Gas fees: Each transaction on the Ganache blockchain necessitates the payment of a gas fee by the sender account, serving as compensation for miners processing the transaction.

VII. RESULTS AND DECLARATION

Test Case ID	Test Case	Description	Input	Expected Output	Actual Output	Status
1.	Hospital Registration	Hospital registration completed via web application.	Hospital Id, Name, Address, Specification	Registration Successful	Registration Successful and Hospital details are added to the network	Passed
2.	Doctor Registration	Doctor Registration can be done only by a registered Hospital.	Id, Name, Specification Address, Phone No.	Registration Successful	Registration Successful and Doctor details are added to the network	Passed
3.	Patient Registration	Patient Registration can be done only by a registered Doctor.	Id, Name, Age, Address, Phone No., Attendant details	Registration Successful	Registration Successful and Patient details are added to the network	Passed
4.	Invalid Doctor Registration	Doctor Registration fails when done by Invalid user (Hospital).	Id, Name, Specification, Address, Phone No.	Registration Successful	Registration failed	Failed
5.	Invalid Patient	Patient Registration	Id, Name, Age, Address,	Registration Successful	Registration failed	Failed

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704114 |

	Registration	fails when done by Invalid user (Doctor).	Phone No, Attendant details			

Table 7.1 Test Cases

Fig 7.2: Home Page of Secure Medical Record Management Application

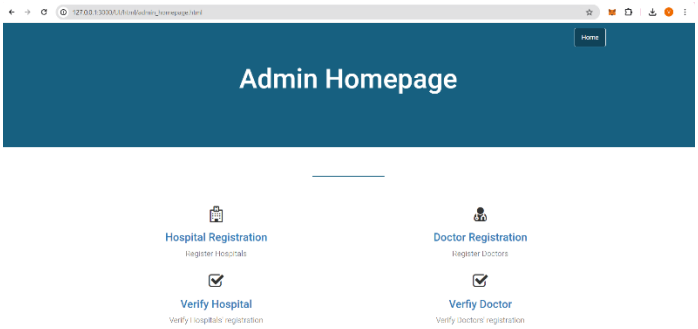


Fig 7.3: Admin Home Page

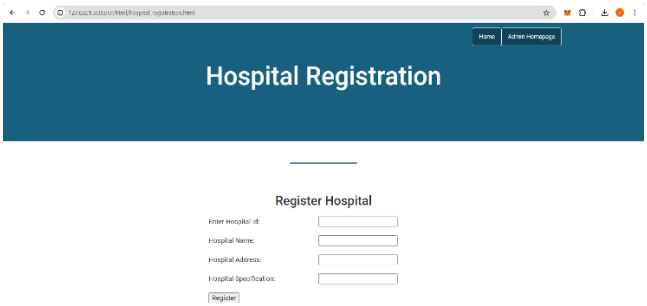


Fig 7.4: Hospital Registration

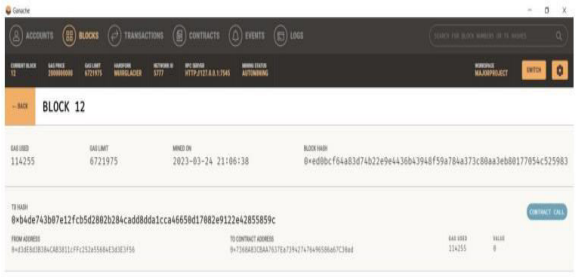


Fig 7.5: Block Added for Hospital Registered

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704114 |

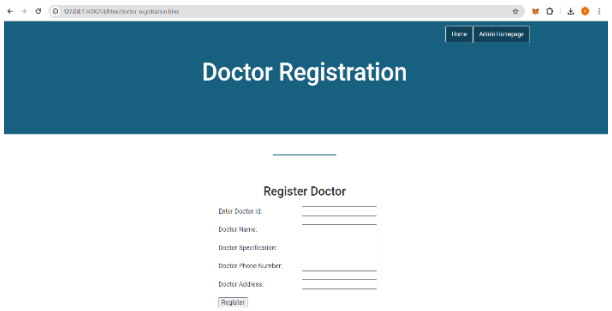


Fig 7.6: Doctor Registration Page

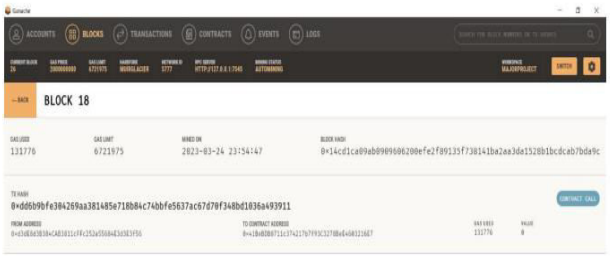


Fig 7.7: Block added for Doctor Registration

VIII. CONCLUSION

Medical record maintenance applications leverage blockchain technology and smart contracts to ensure the secure management of patient data. Deployed as web applications, they offer easy accessibility to users while utilizing smart contracts for automated data operations on test networks. Blockchain's immutable record storage, accessed via unique hashes or IDs, ensures data integrity and prevents unauthorized alterations, enhancing security significantly. Furthermore, blockchain's decentralized nature allows data to be accessible to authenticated users across hospitals while restricting unauthorized modifications.

The transparency and trustworthiness of these applications are further bolstered by blockchain's distributed ledger technology, providing a clear and auditable history of data transactions. Smart contracts play a crucial role in verifying user ownership and controlling access to various application modules, adding an extra layer of security.

By replacing traditional systems, medical record maintenance applications using blockchain offer extensive security measures and contribute significantly to healthcare efficiency and reliability. This innovative approach simplifies medical record maintenance methods while ensuring patient privacy and data integrity, ultimately benefiting society as a whole.

REFERENCES

[1] Ayesha Shahnaz , Usman Qamar, and Ayesha Khalid "Using Blockchain for Electronic Health Records " , IEEE Access ,Oct, 2019.
[2] Mohammad Mouussa Madine, (Member, IEEE), Ammar Ayman Battah ,Ibbar Yaqoob, (Senior Member, IEEE), Khaled Salah, (Senior Member, IEEE),Raja Jayaraman . Yousuf AL-Hammadi , Sasa Pesic, and Samer Ellahham "Blockchain for Giving Patients Control Over Their Medical Records" , IEEE Access ,Oct, 2020.
[3] Zhijie Sun, Dezhi Han, Dun Li, Xiangsheng Wang, Chin-Chen Chang, Zhongdai Wu, “A blockchain-based secure storage scheme for medical information”, Cornell University.
[4] Agbo, Cornelius C., Qusay H. Mahmoud, and J. Mikael Eklund, "Blockchain Technology in Healthcare: A Systematic Review", MDPI, 2019.
[5] Harshini V M, Shreevani Danai, Usha H R, Manjunath R Kounte ,"Health Record Management through Blockchain Technology" , IEEE Xplore , 2019.
[6] Gulara Muradova, Mehran Hematyar,"Protecting and securing medical records using blockchain technology", "Actual multidisciplinary scientific-practical problems of information security" V Republic Conference, November 29, 2019.
[7] Usman, M., & Qamar, U, Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology. In 2019 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI),ELSEVIER
[8] William J. Gordon, Christian Catalini "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability", Computational and Structural Biotechnology Journal, June, 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com