iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XI **Month of publication:** November 2024

DOI: https://doi.org/10.22214/ijraset.2024.65641

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 12 Issue XI Nov 2024- Available at www.ijraset.com

HealthLink: A Decentralized Health Data Management System using Merkle Tree-Based Approach

Sarthak Madhikar[1], Ranjana Jadhav[2], Sushrut Patil[3], Tejas Gambhir[4], Aman Manakshe[5], Sahil Jagtap.[6]
Department of Information Technology, Vishwakarma Institute of Technology, Pune, India

Abstract: ***Challenges with health data management in the healthcare industry include security, privacy, and interoperability. Most traditional centralized systems tend to be insecure, inefficient, and deprive the patient of considerable control over their personal health record. HealthLink introduces a decentralized approach to the management of health data employing a Merkle tree-based recovery of these issues. With the application of blockchain technology, HealthLink provides the immutability and security of data while allowing for its integrity. The Merkle tree-based architecture is used for health record verification in a way that is both efficient and secure without exhausting the dataset's content. This system makes it possible to have seamless interoperability among different healthcare providers, thus making health information exchange between them both secure and efficient. By allowing the patients control over their health data, access permissions are provided on demand, thus incorporating enhanced privacy and trust. This would thus place the HealthLink method at the forefront of health data management, providing a robust, secure, and user-centric solution that might be tailored to meet the needs of the healthcare sector as a means of improving patient care and also reducing the efficiency in managing data.***

Keywords: Electronic Health Record (EHR), Blockchain, Merkle Tree, Smart Contract.

I. INTRODUCTION

Blockchain and smart contracts enhance the security and sharing of patients' data within EHR. With the integration of blockchain into healthcare infrastructure, performance is going to be significantly improved. EHR systems continue to gain popularity as a transfer method of medical data among many healthcare organizations. The main difficulty with accessing crucial patient records from various EHRs is that the majority of existing databases are connected to only one specific health provider or otherwise confined to one or more specific geographical locations. The additional advantages of using blockchain for data storage and access might help patients through remote monitoring and cost reductions as well as through better care beyond traditional healthcare settings. In the modern healthcare environment, it is patient confidentiality now. The rapid growth in usage of IoT devices raises a great number of privacy and security challenges. Blockchain technology will provide safety for e-health records through a decentralized peer-to-peer network. It will serve as a secure mechanism to process and exchange medical data for improving healthcare efficiency.

This paper discusses the approach toward managing health data through a decentralized system using a Merkle tree-based structure. The system uses blockchain to provide immutability, integrity, and security guarantees for the health records. The Merkle tree structure specially makes it convenient and safe to verify data without needing to access the entire set of data and maintains privacy while reducing computational overhead.

Thus, it aims to bridge the gap between the multiple kinds of healthcare providers by establishing interoperability in secure data exchange. It makes patients who have control over their own health data: permission is granted or access given when needed, hence building trust and improving privacy. Moreover, this decentralized system enables remote monitoring as well as care delivery, which may decrease healthcare costs and improve patients' results compared to that with traditional clinical settings.

II. RELATED WORK

[1] In the research proposal, the methodology to conceptualize, execute, and evaluate the proposed blockchain-driven EHR management system as designed by healthcare providers is presented. The four fundamental frameworks in the integration part of this system include the Immutable Log Creation Model, the Patient-Provider Permission Model, the Data Sharing Model, and the Viewership Model.

To maintain the integrity of someone's health records throughout the lifecycle, the system is to be designed with immutable logs to avoid any shred of insider threats and ensure proper transparency, security, and privacy of sensitive health information. **[2]** In this paper, an electronic medical record management system built on the Hyperledger platform is introduced, maintaining privacy, security, and convenient accessibility of the medical records. It employed permissioned blockchain technology, where the node in the system will function under the Hyperledger framework, as all nodes receive certificates from the Member Service Provider (MSP). Each user in the network has a unique username-password pair that allows them to get an Enrollment Certificate (Ecert). Transaction certificates or TCert issued by the Transaction Certificate Authority to Ecert holders allow them to conduct secure transactions within the network. **[3]** The system, through Hyperledger's permissioned blockchain technology, ensures efficient storage and sharing of EMRs, thus greatly enhancing the security and privacy of data. It can store and disseminate the sensitive medical information in a secure manner, thereby mitigating the risks posed by the dangers of exposure and interference with data. This paper identifies a blockchain-based approach focused on securing medical data in cloud computing environments and evaluates and implements several blockchain methodologies for that purpose. **[4]** In the first place, collected data is encrypted and sent to fog nodes. During this phase, in these fog nodes, data accumulated will undergo verification before storing it in CSPs storage, with indexing included as well. To further strengthen security against potential vulnerabilities, an access log and metadata for all incoming encrypted data from the users are created and stored in a distributed private blockchain. Five main components, namely IoT Node, Cloud Storage and Private Blockchain, Medical User, Fog Node, are involved in the system model design. **[5]** A framework for EHR based on blockchain has been proposed by the authors. Their framework is designed to meet the requirements defined by various national and international standards on EHRs, such as HIPAA and HL7. Their framework facilitates secure health information exchange with immutability properties, security, and user-controlled access to stored records without centralized storage. They elucidate how blockchain technology can facilitate the enhancement of the security, privacy, and user autonomy ascribed to EHRs to ensure seamless data sharing and communication between diverse healthcare providers. **[6]** The paper presents a system architecture and an access control policy algorithm to enhance accessibility and privacy of data along with security at both ends-the patients' and healthcare providers. It deals with the performance of the proposed system in terms of latency, throughput, resource utilization, and network traffic. **[7]** A comparative study has been undertaken with related existing systems to check its effectiveness. This is a proposed EHR system that is based on blockchain. Smart contracts, chain code, and access control policies are used in efficient and secure management and exchange of EHR across different healthcare providers. **[8]** In this paper, they present a clear overview of how blockchain networks are organized. The special features of decentralized consensus in these networks and provide a detailed review of the latest consensus protocols. Our focus is on two key areas: how to design a distributed consensus system and how to create effective incentive mechanisms. **[9]** In the paper, the authors propose the RSP consensus algorithm, which incorporates three balance states—R, S, and P—based on the concept of the Rock-Scissors-Paper game. This game is commonly used for reaching consensus in everyday situations, aiming to achieve smooth agreement among multiple participants. To address issues in existing consensus algorithms, the authors apply the RSP game concept for consensus in a distributed blockchain network. **[10]** This prototype serves as a proof, showing how decentralized systems and blockchain technology can enhance the security and interoperability of electronic health record (EHR) systems. By using Ethereum smart contracts, it coordinates a content-access system across different storage and provider locations. It manages access to medical records, while giving patients full access to their records, the ability to audit their care, and control over data sharing.

III. METHODOLOGY

The methodology for developing a Blockchain based EHR Management System involves several key steps. Initially, the project begins with a thorough requirement analysis to identify the need for secure, decentralized medical record management and to define the core functionalities, such as creating and retrieving medical records. The chosen technology stack includes HTML, CSS, and JavaScript for the frontend, Solidity for the smart contract on the Ethereum blockchain, the Web3.js library for blockchain interactions, and MetaMask as the Ethereum wallet extension.

The development phase involves writing the smart contract (Medical Record) in Solidity, defining a Record struct, and implementing functions to create and retrieve records. After deploying the contract on the Ethereum network using tools Remix, the frontend is developed with forms for input and a table to display records. Web3.js is integrated to connect the frontend with the Ethereum network, enabling interactions with the smart contract through MetaMask. Rigorous integration and testing ensure that all functionalities work correctly, including error handling and edge cases. Once tested, the system is deployed on the Ethereum testnet. Comprehensive documentation is created to guide users through setup, deployment, and usage, culminating in a secure, user-friendly application that leverages blockchain technology for managing medical records.

A. *Smart Contracts*

Smart contracts are a decentralized way to manage transactions on a blockchain. They act as tools that allow participants in a network to carry out transactions automatically, based on set rules, terms, and conditions.

Each contract has **a** unique address on the blockchain that helps track its status and ownership. Smart contracts also handle interactions like sending and receiving requests. For example, in a system, a registration contract might be used to create digital health records.

1) *Contract for Patient Registration*

In the system, the registration contract controls the creation of patient medical records and their storage inappropriate blocks. Hash b locks are instantly stored in a special database. When a patient seeks medical treatment at a hospital, their health and personal details are recorded in the Electronic Health Record (EHR) database, integrated into a blockchain system. Each patient possesses unique attributes like name, age, and gender, identified by a Patient-ID. Post consultation, all medical interactions, test results, prescriptions, and comprehensive records are logged for future reference under the patient's profile.

In the system, the registration contract controls the creation of patient medical records and their storage in special blocks. These encrypted blocks are quickly stored in special storage facilities. When patients go to the hospital for treatment, their health and personal information is added to the electronic health record (EHR) blockchain system. Each patient has unique details such as name, age, and gender, which are identified by the patient ID. After the consultation, all medical consultations, test results, prescriptions, and all information are stored in the patient's profile for future reference.

2) *Contract for Patient Data Retrieval*

As patients, doctors, and medical professionals become part of the blockchain network, patients have access to their medical information for personalized treatment and early treatment. However, patients need authorization to view their full medical history. Doctors have special permissions to manage their patients' accounts, allowing them to change monitoring settings or adjust medications. A viewership contract is also set up, enabling patients to access their records through the blockchain system.

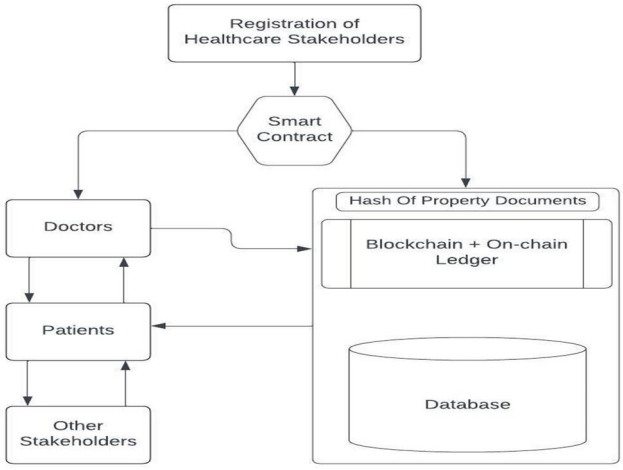


Figure 1: System Architecture of the system

B. *Merkle Tree Structure*

A Merkle Tree, which is also called a hash tree, is a type of data structure used in blockchain and cryptography. It is a binary tree in which each page contains the hash value of a block of data and each non-page node holds the encrypted hash value of its child node. In this system, each patient's medical information (such as medical records, test reports, or prescriptions) is first hashed to create a unique value for that information. These hashes form the leaves of the Merkle tree, with each leaf representing the patient's electronic health record (EHR). The leaves are then combined and merged together to form the next level of the tree. This process continues until a hash value is created at the top (called the Merkle base). The Merkle root is a unique hash value that records all the data in the tree and stores it in the blockchain block header as a fingerprint for all patient data in that block.

When a new health record is added for a patient, it is hashed and included as a new leaf node in the Merkle Tree, which is then recalculated to update the Merkle root. When a patient or doctor requests a health record, the system provides it along with a Merkle proof, which includes the necessary hashes to verify the record against the Merkle root stored in the blockchain. The system can also perform periodic integrity checks by recalculating the Merkle Tree and comparing the Merkle root to the one on the blockchain, ensuring no data has been tampered with.

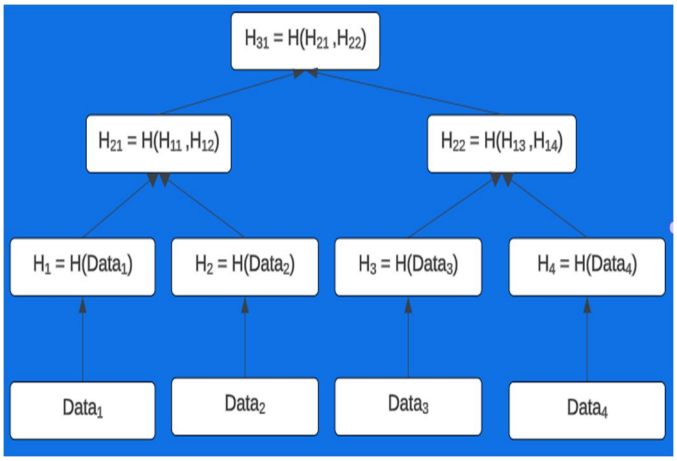


Figure 2: Merkle Tree Structure

C. Structure of Blockchain

The structure of a blockchain for an Electronic Health Record (EHR) management system is designed to securely store, verify, and manage patients' health data. Figure 3 shows the structure of the Merkle tree used with blockchain to ensure data security and integrity. Each piece of data (Data1, Data2, Data3, Data4) is individually hashed. The hashes of the data items are paired and hashed together to form intermediate nodes (Hash21 and Hash22). The intermediate nodes in the Merkle tree are hashed together to create the Merkle root (Hash31), which summarizes all the data in a block. The Merkle root, along with other important details like the Block ID, Previous Hash, Timestamp, Nonce, and Hash Target, is stored in the block header. The Merkle root guarantees the integrity of the data in the block because any change in the data will affect its hash, which then changes the Merkle root. Merkle trees make it easy to verify individual pieces of data since only a small part of the tree is needed to check if a specific piece of data is part of the block. The "Previous Hash" connects blocks securely, making the blockchain difficult to tamper with or change.

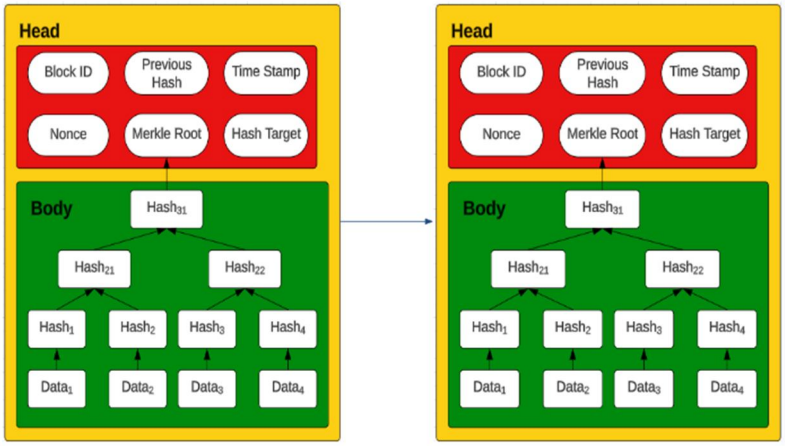


Figure 3: Structure of blockchain

IV. RESULTS AND DISCUSSION

The patient record is created in the blockchain after the doctor adds the specified information about the patient in the prescription. Then the patient registration contract is called in the process which stores the data into an account which is created for that patient. MetaMask records this transaction and shows it on the Ganache blockchain simulator. The blockchain simulator is used for doing all the transactions.

A new address is designated to every new transaction that is created. After that a key is generated for that record which is used in the decentralization process. That key can be used by other doctors or hospitals to retrieve the data of the patient without needing to go through the process all over again. Figure 4 shows how a key is used to get the data of a given patient. All the details such as prescription, future follow ups and any medical documents can be retrieved through this process.

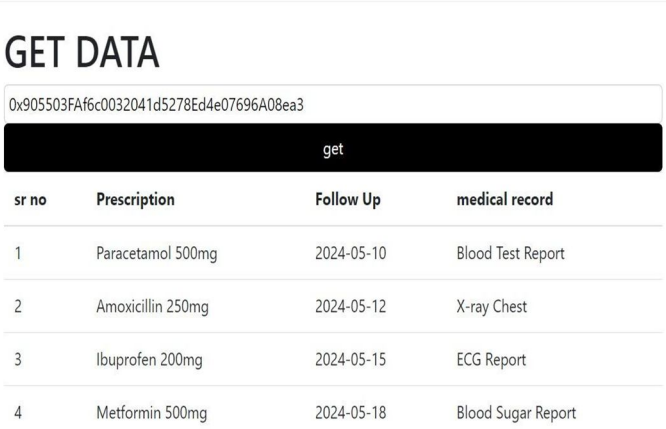


Figure 4: getData contract for data retrieval

As shown in Figure 4, the system uses a unique identifier (hash code) which is the transaction hash or address on the blockchain. The system queries the blockchain with this key to retrieve patient records securely. In healthcare, this ensures the authenticity and immutability of data. The prescription column reflects the medication prescribed to the patient, along with its dosage, i.e. Paracetamol 500 mg and along with the date when the patient will be followed up in the follow-up column. All the documents regarding treatment of the patient, such as test reports and diagnostic images, are reflected in the medical record column. Every prescription is accompanied by a corresponding medical report and date of follow-up, and an unbreakable bond is ensured between a patient's medicines history and clinical document. The blockchain-based retrieval assures that every medical data is tamper-proof, decentralized, and saved in safety. Every link of prescription, follow-up date, and every single piece of medical report is safely encrypted and linked to the blockchain data of the patient in such a way that access or alterations by non-authorized parties can't take place. Probably, it denotes the unique ID of the patient in the blockchain. It will then allow the application to fetch the medical data of the patient securely and privately.

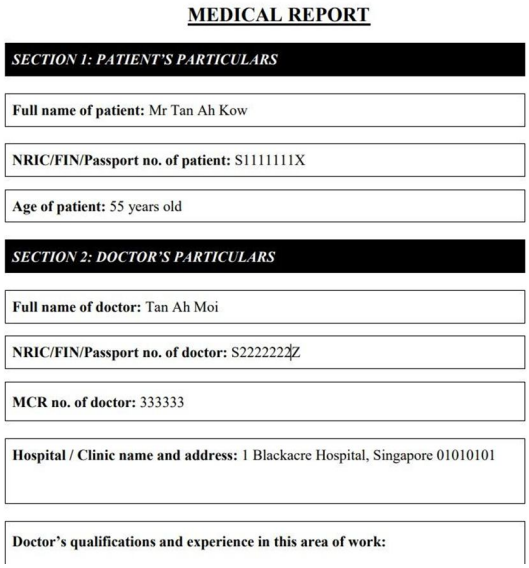


Figure 5: Medical report/documents attached with the respective record.

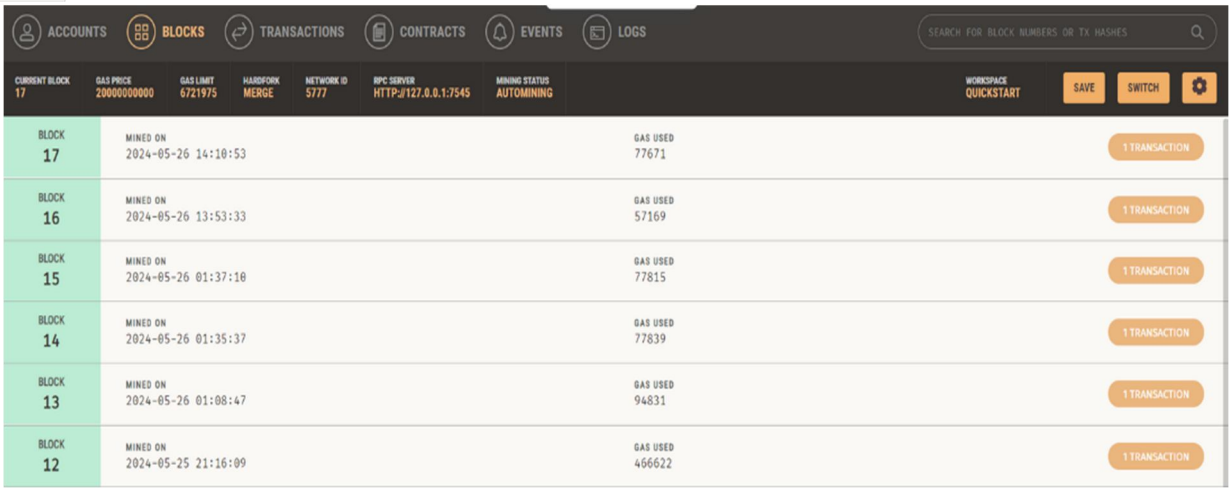


Figure 6: Display of Blocks of Blockchain

In figure 6, Ganache shows all the blocks that are created in the blockchain with their keys or addresses. Since blockchain ensures that all transactions are immutable, every block mined will contain a record of interactions with patient data. Once recorded, these transactions cannot be altered, ensuring the integrity and security of the patient's medical information. The gas used for each transaction reflects the cost of processing the data request on the blockchain. Proper use of gas is key to ensuring that the system is optimal due to the fact that, within healthcare applications, large parts of data are potentially processed. Each block here represents a transaction that most likely interacts with patient health records, such as queries for prescriptions or updating of medical records. That there is only one transaction per block suggests that the system is modular since each transaction is likely to be on a different aspect of the patient data. It also tends to give clarity and traceability to information. Timestamp information is important since it helps the system to keep track of when some particular medical information was accessed or changed, so that the entire history of patient interactions is clear and may be audited.

V. CONCLUSION

In conclusion, the decentralized electronic health data management system utilizing a Merkle tree-based approach offers a robust and secure solution for handling sensitive health records. By using blockchain technology, this system ensures data integrity, transparency, and immutability, addressing many of the prevalent concerns in traditional centralized health data systems. The use of Merkle trees facilitates efficient and secure verification of data, allowing for scalable and trustworthy management of electronic health records. This innovative approach not only enhances the privacy and security of patient data but also fosters better interoperability and accessibility for patients, healthcare providers, and administrators. Consequently, it represents a significant advancement in the realm of digital health management, promising improved patient outcomes and streamlined healthcare operations.

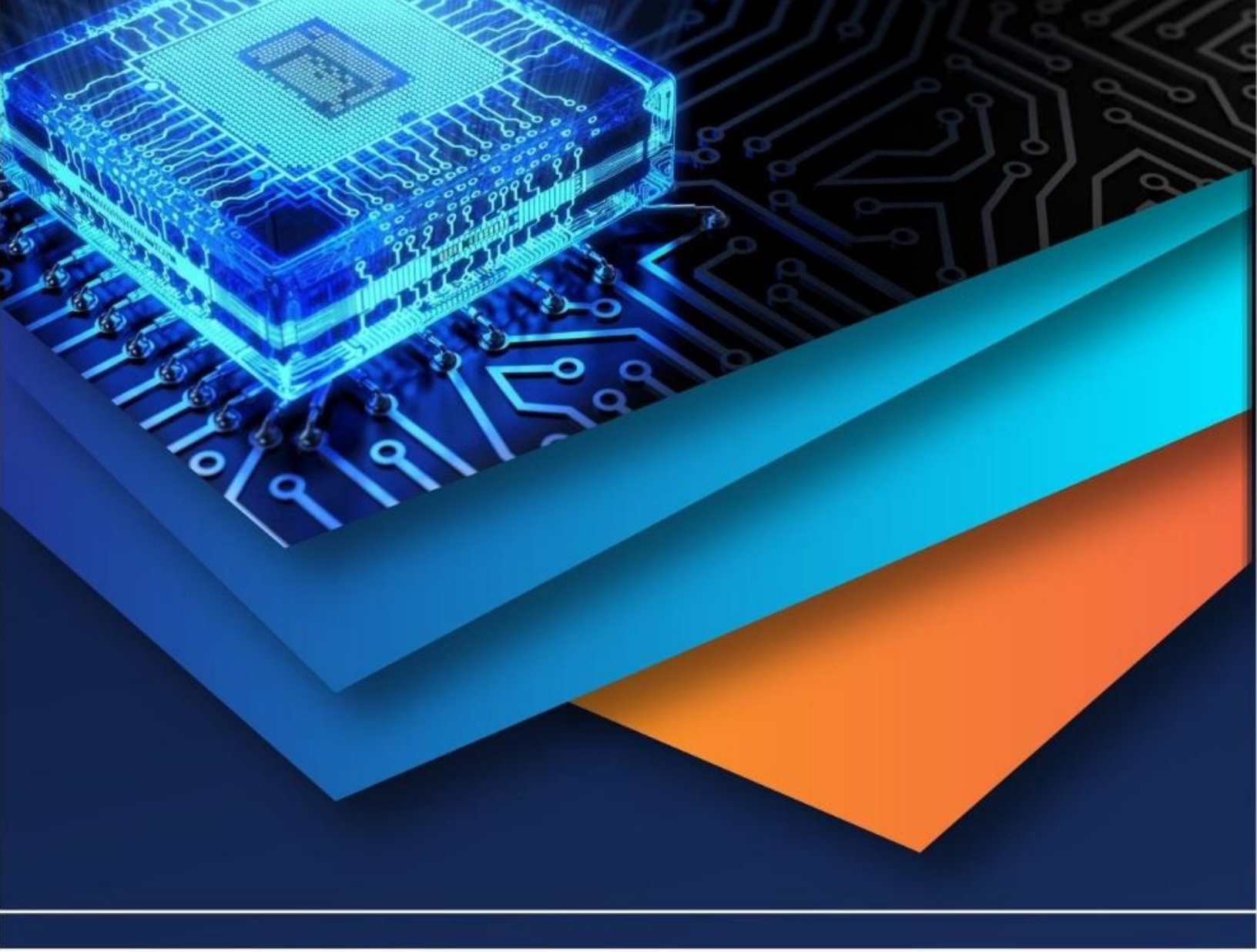
REFERENCES

[1] Chelladurai, U. and Pandian, S., 2022. A novel blockchain based electronic health record automation system for healthcare. Journal of Ambient Intelligence and Humanized Computing, pp.1-11.
[2] Usman, Muhammad, and Usman Qamar. "Secure electronic medical records storage and sharing using blockchain technology." Procedia Computer Science 174 (2020): 321-327.
[3] Mahajan HB, Rashid AS, Junnarkar AA, Uke N, Deshpande SD, Futane PR, Alkhayyat A, Alhayani B. Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. Appl Nanosci. 2023;13(3):2329-2342. doi: 10.1007/s13204-021-02164-0. Epub 2022 Feb 4. PMID: 35136707; PMCID: PMC8813573.
[4] Reegu, F.A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A.A., Jabbari, A., Sonkamble, R.G. and Dziyauddin, R.A., 2023. Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. Sustainability, 15(8), p.6337.
[5] Tanwar, Sudeep, Karan Parekh, and Richard Evans. "Blockchain-based electronic healthcare record system for healthcare 4.0 applications." Journal of Information Security and Applications 50 (2020): 102407.
[6] Khan, A.U.; Shahid, A.; Tariq, F.; Ghaffar, A.; Jamal, A.; Abbas, S.; Javaid, N. Enhanced Decentralized Management of Patient-Driven Interoperability Based on Blockchain; Springer International Publishing: New York, NY, USA, 2020; Volume 97, ISBN 9783030335069.
[7] Kuo, T.-T.; Kim, H.-E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inform. Assoc. 2017, 24, 1211–1220.

[8] Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access 2019, 7, 22328–22370.

[9] Kim, D.H.; Ullah, R.; Kim, B.S. RSP Consensus Algorithm for Blockchain. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019; pp. 1–4.

[10] Ekblaw, Ariel, et al. "A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data." Proceedings of IEEE open & big data conference. Vol. 13. 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY