iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59289

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 III Mar 2024- Available at www.ijraset.com

Leveraging Blockchain and IPFS for Secure and Privacy-Preserving Patient Medical Record Management: A Government-Controlled Approach

Jyotiraditya Gandhi[1], Krishnakumar Maurya[2], Viveksingh Panwar[3], Utpalkumar Patel[4], Sujaya Bhattacharjee[5], Meetkumar Patel[6]

[1, 2, 3]*4th Year BTech CSE, Parul University, Vadodara, Gujarat*

[4, 5, 6]*Assistant Professor, Computer Science & Engineering, Parul Institute of Technology, Parul University, Vadodara, Gujarat, India*

Abstract: ***In recent years, the integration of blockchain technology with healthcare systems has garnered considerable attention due to its potential to enhance security, privacy, and interoperability in managing patient medical records. This paper proposes a novel approach to patient medical record management by leveraging Ethereum blockchain and InterPlanetary File System (IPFS) for storage, within a government-controlled framework. The system ensures secure and immutable storage of patients' medical records, accessible only by verified medical professionals, thus facilitating informed diagnosis and treatment. Additionally, the platform provides mechanisms for patient recourse in case of inaccuracies, as well as potential integration with insurance agencies. Furthermore, the proposed system envisages a future extension to facilitate anonymized data sharing with the scientific community, thereby contributing to advancements in medical research. This paper provides a comprehensive academic description of the proposed approach, discussing its technical architecture, security measures, regulatory framework, and potential impact on healthcare delivery and research.***

Keywords: Blockchain technology, Healthcare systems, Patient medical records, Ethereum blockchain, InterPlanetary File System (IPFS), Security, Privacy, Interoperability, Government-controlled framework, Immutable storage, Verified medical professionals, Patient recourse, Integration with insurance agencies, Anonymized data sharing, Medical research,

I. INTRODUCTION

In the digital age, the management of patient medical records poses significant challenges, including issues related to security, privacy, interoperability, and accessibility. Traditional centralized systems often suffer from vulnerabilities such as data breaches, unauthorized access, and lack of transparency. Blockchain technology has emerged as a promising solution to address these challenges by providing a decentralized and immutable ledger for storing sensitive data. This paper presents a novel approach to patient medical record management, utilizing the [27] Ethereum blockchain and [26] IPFS for secure and privacy-preserving storage, within a government-controlled framework.

II. RELATED WORK

In [1] Dwivedi, S. K., et al., the authors propose an innovative approach to Electronic Medical Records (EMRs) management, utilizing blockchain technology, smart contracts, and a tailored consensus algorithm within a cloud environment. The system addresses key challenges in traditional EMR systems, including security, data integrity, interoperability, and accessibility. Blockchain technology is employed to establish a decentralized and immutable ledger for EMR storage, ensuring data integrity and security without relying on a central authority. Smart contracts automate agreements between various healthcare ecosystem participants, facilitating processes such as access control and consent management. A custom consensus algorithm ensures transaction validity and block ordering consensus among network nodes, maintaining data consistency. Deployment in a cloud environment enhances scalability, reliability, and accessibility. Advantages of the approach include enhanced security, data integrity, automation, interoperability, and scalability. However, limitations such as scalability challenges, regulatory compliance concerns, implementation complexity, and adoption hurdles are also noted.

In [2] Uddin, M. A., et al. introduce a patient agent system utilizing blockchain technology for secure remote patient data management. The system targets enhanced data integrity, security, and privacy in remote monitoring setups.

The proposed architecture includes the patient agent, blockchain network, and healthcare provider system. The patient agent, installed on the patient's device, securely collects and stores health data, while the blockchain network ensures data immutability and integrity. Healthcare providers access patient data through the patient agent's interface, enabling timely interventions. Implementation details cover blockchain platform selection, smart contract development, and integration with existing healthcare IT. Advantages include enhanced security, data transparency, patient empowerment, and interoperability. Limitations encompass scalability issues, regulatory compliance challenges, data privacy concerns, and technical complexity.

In [3] Saha, A., et al. present a review on "Blockchain technology based medical healthcare system with privacy issues" published in Security and Privacy in 2019. The paper underscores the growing importance of blockchain technology in diverse sectors, particularly in healthcare, and addresses privacy concerns associated with medical data management. It explores the fundamental concepts of blockchain, emphasizing its decentralized nature, immutability, and transparency. The authors analyze the applicability of blockchain in healthcare, focusing on its potential to secure patients' medical records and enable efficient data sharing among stakeholders. They highlight use cases such as electronic health records (EHRs) management, medical supply chain tracking, and clinical trials administration. Moreover, the paper scrutinizes the challenges inherent in implementing blockchain-based healthcare systems, including scalability issues, interoperability concerns, regulatory compliance, and the necessity for standardization. The approach's advantages encompass enhanced security through cryptographic encryption and decentralized storage, improved privacy via transparency and encryption, efficient data management, and fostering trust and transparency. However, limitations include scalability challenges, interoperability issues, regulatory compliance complexities, and the need for standardized protocols and frameworks.

In [4] Liu, P. T. S. presents a medical record system aiming to tackle security, accessibility, and privacy challenges in healthcare data management, in Information and Communications Security, ICICS 2016. The system integrates blockchain, big data analytics, and tokenization to address issues like data breaches, lack of interoperability, and centralized control. Blockchain technology ensures a distributed and tamper-resistant ledger for storing medical records, enhancing security and integrity through cryptographic measures. Big data analytics extracts insights from vast medical data, improving decision-making and treatment plans. Tokenization controls data access, empowering patients to manage their information and incentivizing data sharing. The system offers benefits in security, transparency, privacy, data analytics, and interoperability, but faces challenges in scalability, adoption, regulatory compliance, data ownership, and technical complexity.

In [5], Zhang, J., Xue, N., & Huang, X. propose a secure system for pervasive social network-based healthcare, as detailed in their paper published in IEEE Access. The system aims to integrate social networking aspects into healthcare management, ensuring security and privacy. Employing cryptographic techniques, it facilitates secure communication and data sharing among patients and healthcare providers. The system employs access control mechanisms to regulate data access, ensuring that only authorized users can view sensitive medical information. Additionally, it incorporates encryption methods to protect data during transmission and storage, safeguarding patient confidentiality. Through this system, users can securely share health-related information within their social network, fostering collaboration and support while maintaining privacy.

In [6], Xia, Q., et al. introduce BBDS, a blockchain-based data sharing system for electronic medical records in cloud environments. Their approach utilizes blockchain technology to enhance security and privacy in sharing medical records, aiming to mitigate risks associated with centralized storage. By leveraging smart contracts, BBDS ensures secure and transparent access control, allowing patients to retain ownership and control over their data. However, while the use of blockchain enhances data integrity, the reliance on cloud environments may introduce vulnerabilities if not adequately addressed in terms of security measures. Nevertheless, the proposed system presents a promising direction for improving data sharing in healthcare, emphasizing patient-centric control and privacy preservation within cloud infrastructures.

In [7] Al Omar et al. present "Medibchain," a blockchain-based platform designed for privacy-preserving healthcare data management. The system utilizes blockchain technology to ensure the security and integrity of patient data while preserving privacy. Through smart contracts, Medibchain enables controlled access to medical records by authorized parties only. However, the paper lacks detailed discussion on scalability and performance issues that might arise with blockchain-based systems in healthcare, such as transaction throughput and latency.

In [8], Bocek et al. introduce a use-case scenario for blockchain implementation in the pharmaceutical supply chain, presented at the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management. The paper explores the potential of blockchain technology to enhance transparency and efficiency in pharmaceutical supply chains. It suggests leveraging blockchain to track the flow of pharmaceutical products from manufacturers to consumers, aiming to mitigate issues like counterfeit drugs and supply chain inefficiencies.

The proposed system employs blockchain's decentralized ledger to record transactions and ensure data integrity across the supply chain network. However, it does not provide empirical evidence or case studies to validate the effectiveness of blockchain technology in addressing the stated issues within the pharmaceutical supply chain.

In [9], Ding, Conti, and Solanas present a smart health application addressing privacy concerns. The application aims to enhance health monitoring and management through smart devices. However, their system lacks comprehensive consideration of privacy issues, potentially exposing sensitive health data to unauthorized access. While the paper discusses the benefits of the smart health application, it fails to provide detailed mechanisms for ensuring robust privacy protection. Moreover, there's a lack of discussion on encryption techniques, access control mechanisms, and data anonymization methods, leaving the system vulnerable to privacy breaches.

In [10], Novikov, S. P., et al. propose a decentralized health infrastructure utilizing blockchain and smart contracts. Their system aims to enhance security and transparency in healthcare data management. By leveraging blockchain technology, medical records are securely stored and managed, ensuring immutability and accessibility. Smart contracts facilitate automated execution of predefined agreements, streamlining processes such as patient consent management and insurance claims processing. However, the paper lacks in-depth discussion on scalability issues inherent in blockchain systems, particularly in the context of healthcare where large volumes of data are generated.

In [11], Azaria et al. introduce MedRec, a blockchain-based system for medical data access and permission management. The system utilizes blockchain technology to provide secure and auditable access to medical records, enhancing patient privacy and data integrity. Through smart contracts, MedRec enables patients to control access to their medical data while ensuring transparency and accountability in data sharing among healthcare providers.

In [12], Vidhya Ramani et al. propose a system for secure and efficient data accessibility in blockchain-based healthcare systems. Their approach integrates blockchain technology to ensure secure and immutable storage of patient medical records, with a focus on enhancing privacy and interoperability. By utilizing Ethereum blockchain and the InterPlanetary File System (IPFS) for storage, the system enables access to patient records only by verified medical professionals within a government-controlled framework. However, the paper lacks detailed discussion on mechanisms for patient recourse in case of inaccuracies, as well as potential integration with insurance agencies. Additionally, while the proposed system envisions future extension for anonymized data sharing with the scientific community, specifics on the implementation and safeguards for preserving patient privacy in such data sharing are not thoroughly addressed.

In [13] Jian Li introduces a novel blockchain-based system for transferring electronic medical records (EMRs) with an emphasis on data privacy. The proposed system utilizes blockchain technology to securely transfer EMRs between healthcare providers while ensuring patient data privacy. Li's system employs encryption techniques to safeguard sensitive medical information during transmission. However, the paper lacks a detailed discussion on the scalability of the proposed solution and potential challenges in integrating with existing healthcare IT infrastructures. Despite these shortcomings, the paper presents a promising framework for enhancing EMR transfer efficiency and privacy protection through blockchain technology.

In [14], B.L. Radhakrishnan et al. propose a system for securing blockchain-based electronic health records (EHR) through multilevel authentication. The approach aims to enhance security in managing EHR by incorporating multiple levels of authentication. However, the paper lacks detailed discussion on the specific authentication mechanisms employed, such as biometric, two-factor, or multi-factor authentication. Additionally, the paper does not sufficiently address the potential vulnerabilities and threats inherent in blockchain-based EHR systems, such as the risk of unauthorized access, data breaches, or tampering. While multilevel authentication is proposed as a security measure, the effectiveness and resilience of this approach against sophisticated attacks are not thoroughly explored.

In [15], Gordon and Catalini propose a blockchain-based solution for healthcare, aiming to empower patient-driven interoperability. Their system leverages blockchain technology to facilitate secure and transparent sharing of medical data among various stakeholders. By utilizing smart contracts and decentralized storage, the platform ensures data integrity and privacy. However, while emphasizing patient control, the paper lacks a detailed discussion on the regulatory challenges and legal frameworks surrounding healthcare data sharing. Additionally, it doesn't address potential scalability issues that might arise with blockchain implementation in large-scale healthcare systems.

In [16], Xu et al. propose "Healthchain," a blockchain-based privacy-preserving scheme tailored for large-scale health data management. Their approach utilizes blockchain technology to enhance security and privacy in handling sensitive medical information. By employing cryptographic techniques, such as encryption and hashing, Healthchain ensures data integrity and confidentiality while enabling efficient access control mechanisms.

However, the paper lacks detailed discussion on the scalability and performance aspects of their proposed scheme, particularly in the context of managing large volumes of health data. Additionally, while emphasizing privacy preservation, it overlooks potential vulnerabilities in the blockchain network, such as the risk of data leakage through metadata analysis or deanonymization attacks.

In [17] da Conceição et al. propose a system for electronic health records (EHR) utilizing blockchain technology. Their approach integrates blockchain for secure and immutable storage of EHR, aiming to enhance privacy and interoperability in healthcare systems. However, the paper lacks detailed discussion on the specific blockchain platform employed and how it addresses scalability and privacy concerns inherent in healthcare data management. Additionally, the absence of a thorough analysis of regulatory compliance and governance frameworks for handling sensitive medical information is notable. While the paper emphasizes the potential benefits of blockchain in healthcare, such as facilitating patient-controlled access to medical records and enabling secure data sharing, it falls short in providing concrete implementation strategies and addressing real-world challenges like integration with existing healthcare infrastructure and interoperability with legacy systems.

In [18], Yang and Li propose a blockchain-based architecture for securing electronic health record (EHR) systems, presented at the IEEE International Conference on Cloud Computing Technology and Science (CloudCom) in 2018. The authors introduce a system leveraging blockchain technology to enhance the security and integrity of EHRs. Their approach utilizes blockchain's decentralized and immutable ledger to store patient health data, aiming to mitigate risks associated with centralized storage and potential data tampering. However, the paper lacks detailed insights into the specific mechanisms employed for ensuring data privacy and confidentiality within the blockchain framework. Additionally, there is limited discussion on scalability challenges inherent in blockchain implementations for healthcare systems, particularly regarding transaction throughput and storage requirements. Furthermore, the paper does not address regulatory compliance considerations essential for healthcare data management, such as GDPR or HIPAA requirements.

In [19], Kushch et al. introduce a novel concept termed "Blockchain tree for ehealth" presented at the IEEE Global Conference on Internet of Things (GCIoT), 2019. Their approach integrates blockchain technology into eHealth systems, aiming to enhance data security and integrity. The system employs a hierarchical structure resembling a tree, wherein each node represents a healthcare entity or participant, facilitating secure data sharing and access control. However, the paper lacks detailed insights into the specific cryptographic techniques or consensus mechanisms utilized within the blockchain framework. Moreover, there is a deficiency in discussing potential scalability challenges inherent in blockchain-based systems, especially concerning the management of large volumes of medical data. Additionally, the paper does not address the regulatory and compliance aspects crucial for deploying such systems in healthcare settings. Despite these limitations, the proposed Blockchain tree for ehealth concept presents a promising direction for leveraging blockchain in eHealth applications, but further research and refinement are necessary to address the identified shortcomings and ensure practical implementation in real-world healthcare environments.

In [20], Zhang and Lin propose a scheme for secure and privacy-preserving data sharing in e-health systems utilizing consortium blockchain. Their approach aims to enhance security and privacy in sharing sensitive medical data among multiple parties. By leveraging consortium blockchain, they establish a decentralized network where participating entities maintain control over the shared data. However, the paper lacks detailed discussion on the specific consensus mechanism employed in the consortium blockchain, which is crucial for ensuring the integrity and reliability of the shared data. Additionally, while the authors emphasize privacy preservation, there is a lack of thorough analysis on the potential vulnerabilities or attacks targeting the proposed system, such as privacy leaks or data breaches. Moreover, the scalability and efficiency of the system in handling large volumes of medical data are not adequately addressed. Despite these limitations, the paper provides valuable insights into leveraging blockchain for secure data sharing in e-health systems, highlighting the importance of further research to address the identified shortcomings.

In [21], Kuo, Kim, and Ohno-Machado introduce blockchain distributed ledger technologies for biomedical and healthcare applications. The paper outlines the potential of blockchain in enhancing data security, interoperability, and privacy within healthcare systems. Specifically, the authors discuss the utilization of blockchain to manage medical records, facilitate secure data sharing among healthcare providers, and ensure patient consent and control over their data. While the paper highlights the benefits of blockchain in healthcare, it lacks in-depth discussion on the technical implementation challenges, scalability issues, and regulatory hurdles associated with integrating blockchain into existing healthcare infrastructures. Additionally, there is limited exploration of potential drawbacks such as energy consumption and computational overhead inherent to blockchain systems. Further research and practical insights are needed to address these shortcomings and realize the full potential of blockchain in healthcare.

In [22], M.B. Hoy introduces the blockchain technology and its potential implications for libraries and medicine. The paper provides an overview of blockchain fundamentals, emphasizing its decentralized and immutable nature, and discusses its applications in healthcare, including medical record management, supply chain integrity, and research data sharing.

However, the paper lacks detailed technical insights into how blockchain integration can address specific challenges in healthcare systems, such as interoperability issues or patient privacy concerns. Additionally, while it touches upon the potential benefits for libraries, such as enhancing authentication and preserving digital content, it lacks concrete examples or case studies to illustrate practical implementations. Overall, while the paper serves as a general introduction to blockchain's potential in healthcare and library settings, it could benefit from deeper analysis and real-world examples to substantiate its claims and provide actionable insights for practitioners in these fields.

In [23], Angraal, Krumholz, and Schulz explore the applications of blockchain technology in healthcare, focusing on its potential benefits and challenges. They discuss the promise of blockchain in enhancing security, privacy, and interoperability in managing patient medical records. However, the paper lacks specific technical details on the implementation of blockchain in healthcare systems and fails to address potential scalability issues that may arise when storing large volumes of medical data on a blockchain network. Moreover, the authors do not delve into the regulatory framework necessary for the adoption of blockchain technology in healthcare, nor do they provide insights into how patient recourse mechanisms could be integrated into their proposed system. Additionally, while the paper mentions potential benefits for medical research, such as anonymized data sharing, it lacks a detailed discussion on how this could be achieved while ensuring patient privacy and data integrity. Therefore, while the paper highlights the promise of blockchain in healthcare, it falls short in providing a comprehensive analysis of its technical implementation, regulatory considerations, and potential limitations.

In [24], Mettler discusses the potential of blockchain technology in healthcare, emphasizing its revolutionary impact. The paper explores how blockchain can address issues of data security, integrity, and interoperability within healthcare systems. Mettler highlights the ability of blockchain to provide a decentralized and tamper-proof ledger for patient records, enhancing trust and transparency in medical data management. However, the paper lacks specific technical details on how blockchain integration would occur in healthcare systems, including the scalability challenges inherent in blockchain technology. Moreover, there's limited discussion on the regulatory and privacy concerns surrounding the implementation of blockchain in healthcare. Despite acknowledging the transformative potential, Mettler falls short in providing a comprehensive analysis of the practical implications and potential limitations of blockchain technology in healthcare.

In [25], Yue et al. introduce Healthcare Data Gateways, a system aimed at enhancing healthcare intelligence using blockchain while addressing privacy concerns. The system employs blockchain technology to securely store and manage healthcare data, ensuring immutability and transparency. However, the paper lacks detailed discussion on the specific blockchain architecture and mechanisms employed, limiting the clarity on how privacy risks are effectively mitigated. While emphasizing privacy control, the paper falls short in providing comprehensive insights into the specific techniques utilized for ensuring privacy protection. Additionally, there is a need for more explicit elaboration on the mechanisms for data access control and patient consent management within the proposed framework. Despite its contributions to leveraging blockchain for healthcare data management, the paper could benefit from a more in-depth discussion on the practical implementation challenges and scalability considerations associated with deploying such a system in real-world healthcare environments.

III. PROPOSED SCHEME

A. Technical Architecture

The proposed system consists of three main components: the Ethereum blockchain, IPFS, and a user interface for patient and medical professional interaction. Each patient is assigned a unique identifier (ID) linked to their medical records stored on the Ethereum blockchain. Medical data, including past diagnoses, ailment history, prescriptions, and reports, are encrypted and stored on IPFS, with the corresponding hash values recorded on the blockchain for reference. Access to patient data is restricted to verified medical professionals, who undergo stringent verification processes to ensure authenticity and trustworthiness.

B. Security and Privacy Measures

The security and privacy of patient medical records are paramount in the proposed system. By leveraging blockchain technology, data integrity and immutability are ensured, mitigating the risk of tampering or unauthorized modifications. Encryption techniques are employed to protect sensitive medical information stored on IPFS, with access controls implemented to restrict data access to authorized personnel only. Additionally, mechanisms for patient recourse are provided, allowing individuals to challenge inaccuracies in their medical records through established regulatory channels.

C. Regulatory Framework

The proposed system operates within a government-controlled framework, with regulatory oversight to ensure compliance with data protection laws and medical standards. Medical professionals are required to undergo verification processes, including validation of their practitioner licenses against government records. Moreover, patients have the right to control access to their medical records and can choose to share data with insurance agencies, subject to their consent. Regulatory authorities oversee the verification process, handle disputes, and enforce penalties for non-compliance or malpractice.

IV. POTENTIAL IMPACT AND FUTURE DIRECTIONS

The proposed approach has the potential to revolutionize patient medical record management by providing a secure, transparent, and privacy-preserving platform for storing and accessing sensitive healthcare data. Future extensions to the system include integration with insurance agencies, enabling seamless data sharing for claims processing and risk assessment. Furthermore, plans to facilitate anonymized data sharing with the scientific community hold promise for accelerating medical research and innovation.

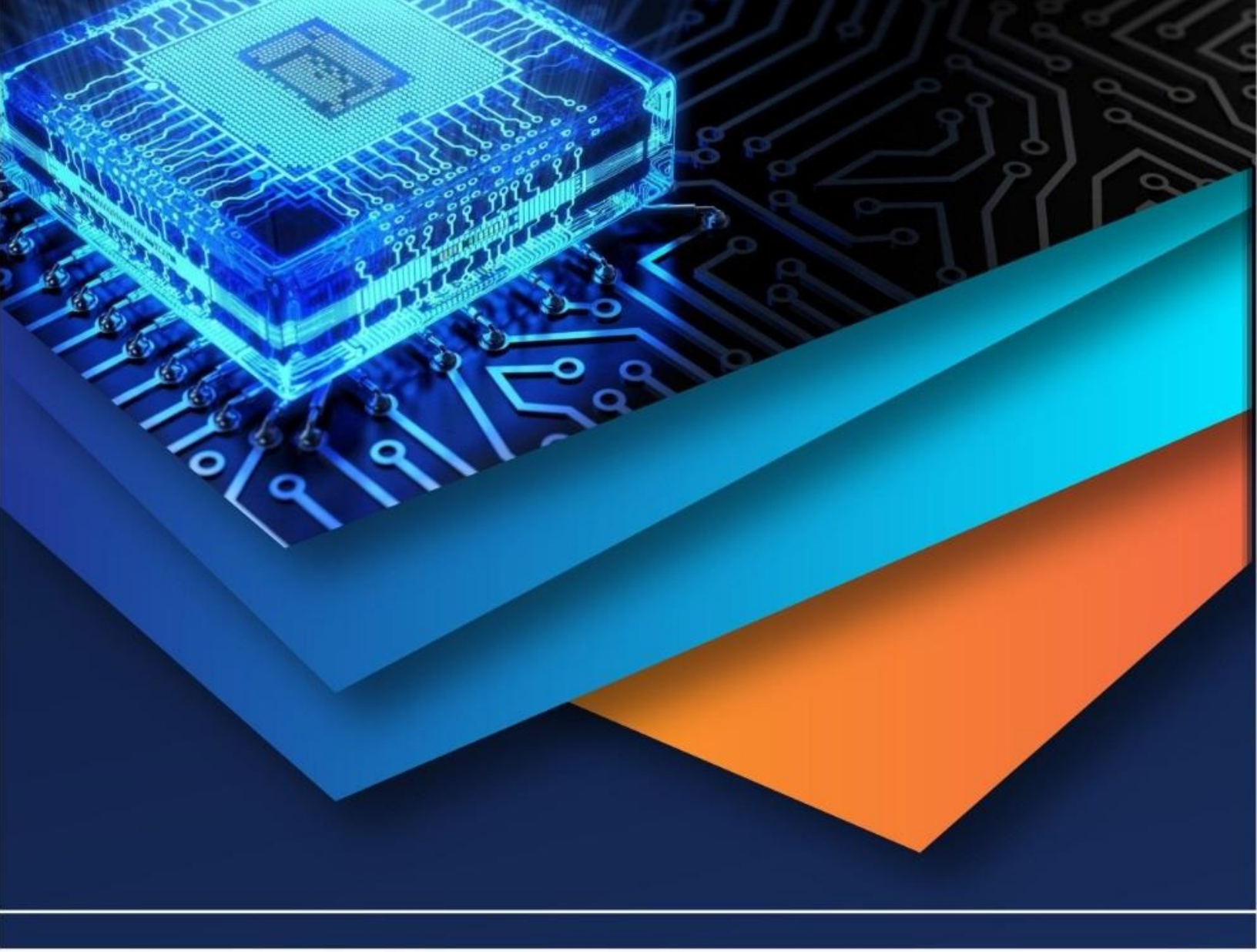
V. CONCLUSION

In conclusion, the proposed approach to patient medical record management represents a significant advancement in leveraging blockchain and IPFS technologies within a government-controlled framework. By ensuring security, privacy, and regulatory compliance, the system addresses critical challenges in healthcare data management while fostering trust and transparency among stakeholders. Continued research and development efforts are warranted to realize the full potential of this innovative solution in improving healthcare delivery and advancing medical science.

REFERENCES

[1] S. K. Dwivedi, et al., "Blockchain-Based Electronic Medical Records System with Smart Contract and Consensus Algorithm in Cloud Environment," Publishing Date: 15 September 2022.
[2] M. A. Uddin, et al., "A patient Agent to manage blockchains for remote patient monitoring," in Studies in Health Technology and Informatics, vol. 254, pp. 105–115, 2018.
[3] A. Saha, et al., "Review on 'Blockchain technology based medical healthcare system with privacy issues'," in Security and Privacy, vol. 2, no. 5, p. e83, 2019.
[4] P. T. S. Liu, "Medical Record System Using Blockchain, Big Data and Tokenization," in Information and Communications Security. ICICS 2016, K. Y. Lam, C. H. Chi, and S. Qing (Eds.), Springer, Berlin, Germany, pp. 254–261, 2016.
[5] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," in IEEE Access, vol. 4, pp. 9239–9250, 2016.
[6] Q. Xia, et al., "BBDS: blockchain-based data sharing for electronic medical records in cloud environments," in Information, vol. 8, no. 2, 2017, pp. 44.
[7] A. Al Omar, et al., "Medibchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data," in Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2017. Lecture Notes in Computer Science, G. Wang, M. Atiquzzaman, Z. Yan, and K. K. Choo (Eds.), Springer, Berlin, Germany, pp. 534–543, 2017.
[8] T. Bocek, et al., "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain," in Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), May 2017.
[9] D. Ding, M. Conti, and A. Solanas, "A smart health application and its related privacy issues," in Proceedings of the 2016 Smart City Security and Privacy Workshop (SCSP-W), April 2016.
[10] S. P. Novikov, et al., "Blockchain and smart contracts in a decentralized health infrastructure," in Proceedings of the 2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS), September 2018.
[11] A. Azaria, et al., "MedRec: Using Blockchain for Medical Data Access and Permission Management," in IEEE, Aug. 2016, pp. 25–30.
[12] Vidhya Ramani, et al., "Secure and Efficient Data Accessibility in Blockchain based Healthcare Systems."
[13] J. Li, "A New Blockchain-based Electronic Medical Record Transferring System with Data Privacy."
[14] B. L. Radhakrishnan, et al., "Securing Blockchain based Electronic Health Record using Multilevel Authentication."
[15] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient driven interoperability," in Comput. Struct.
[16] J. Xu, et al., "Healthchain: a blockchain-based privacy preserving scheme for large-scale health data," in IEEE Internet Things J., vol. 6, no. 5, 2019, pp. 8770–8781.
[17] A. F. da Conceição, et al., "Electronic health records using blockchain technology," arXiv:1804.10078, 2018.
[18] G. Yang and C. Li, "A design of blockchain-based architecture for the security of electronic health record (EHR) systems," in IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2018, pp. 261–265.
[19] S. Kushch, et al., "Blockchain tree for ehealth," in IEEE Global Conference on Internet of Things (GCIoT), 2019, pp. 1–5.
[20] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," in J. Med. Syst., vol. 42, 1–18, 2018.
[21] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," in Journal of the American Medical Informatics Association, vol. 24, no. 6, pp. 1211-1220.
[22] M. B. Hoy, "An Introduction to the Blockchain and Its Implications for Libraries and Medicine," in Medical reference services quarterly, vol. 36, no. 3, pp. 273-279.

[23] S. Angraal, H. M. Krumholz, and W. L. Schulz, "Blockchain technology: applications in health care," in Circulation: Cardiovascular Quality and Outcomes, vol. 10, no. 9, p. e003800.
[24] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on. IEEE, 2016.
[25] X. Yue, et al., "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," in Journal of medical systems, vol. 40, no. 10, 2016, pp. 218.
[26] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," arXiv:1407.3561 [cs.NI], Jul. 2014. [Online]. Available: https://doi.org/10.48550/arXiv.1407.3561.
[27] G. Wood et al., "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, vol. 151, no. 2014, pp. 1-32, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY