International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Protecting Data Privacy in Cloud Using Ethereum Blockchain Technology for the Case of Patients Electronic Health Record (EHR)

Komala R[1], Arun Kumar B. R[2,] Pavan Kalyan S[3], Prem Raj S[4], Pratik B Patil [5,] Shreyas A[6]

Submitted: 25/01/2024 **Revised**: 03/03/2024 **Accepted**: 11/03/2024

Abstract: This research work introduces a decentralized framework designed to empower individual patients in securely managing and controlling sharing of their medical health records. The work is built on the foundation of the Interplanetary File System (IPFS) for robust and secure data storage with Ethereum blockchain for transparent transaction recording. The framework offers a versatile solution to address privacy concerns inherent in traditional healthcare data management systems. A distinguishing feature of the framework is its user-centric approach, granting patients complete autonomy to grant or revoke access permissions to their medical records for insurance companies or any l agencies, third-party providers, or hospitals. By placing control firmly in the hands of patients, the framework enables individuals to make informed decisions regarding the sharing of their sensitive medical information, thereby enhancing privacy and confidentiality. Through an intuitive and adaptable interface, patients can effortlessly manage access permissions, ensuring data security while facilitating collaborative healthcare efforts. This paper represents a significant step forward in decentralized healthcare solutions, promoting patient empowerment and privacy within the digital healthcare landscape.

Keywords: Electronic Health Record, Interplanetary File system, Blockchain, Privacy and Security

Introduction

In recent years, the healthcare sector has witnessed an alarming increase in data breaches, posing significant challenges to the security and privacy of patient information. Incidents such as the cardiovascular consultants breach impacts 484k, healthcare suffers data breach 112k, and delta dental of California moveit Hack Impacts 7M Individuals underscore the urgent need for a paradigm shift in how medical records are safeguarded [1]. Conventional centralized cloud storage solutions have proven inadequate in protecting highly sensitive healthcare data, leading to widespread vulnerabilities and breaches with far-reaching consequences [2].

Addressing these critical challenges requires a comprehensive and innovative approach to healthcare data privacy and security. In response, our paper proposes the development of an advanced application leveraging cutting-edge technologies such as blockchain with the Interplanetary File System (IPFS) as backbone to establish a secure, transparent, and decentralized framework for managing medical records.

The work follows a comprehensive approach that includes the design and analysis of algorithms. Initially, a dataset of annotated medical images is collected and pre-processed to ensure consistent quality and format. The annotated images serve as ground truth, providing pixel-level labels for training and evaluation purposes.

[1]*Research Scholar, Department of MCA, BMSIT &M, Bengaluru Assistant Professor, Department of MCA, Ramaiah Institute of Technology, Bengaluru-560064*
Email: komal.uday@gmail.com
ORCID ID: 0000-0002-4565-8696
[2] *Research Supervisor, Department of MCA & Professor, Department of Computer Science and Engineering B M S Institute of Technology and Management Bengaluru-560064*
Email:arunkumarbr@bmsit.in
ORCID ID: 0000-0002-8659-6102
[3]*UG Scholar, Department of CSE, B M S Institute of Technology and Management Bengaluru-560064*
Email:pk20180708248@gmail.com
[4]*UG Scholar , Department of CSE, B M S Institute of Technology and Management Bengaluru-560064*
Email:pratikpatil6362@gmail.com
[5]*UG Scholar , Department of CSE B M S Institute of Technology and Management Bengaluru-560064*
Email:premraj4044@gmail.com
[6]*UG Scholar , Department of CSE,Sai Vidya Institute of Technology Bengaluru-560064 shreyasa.23cs@saividyacin*

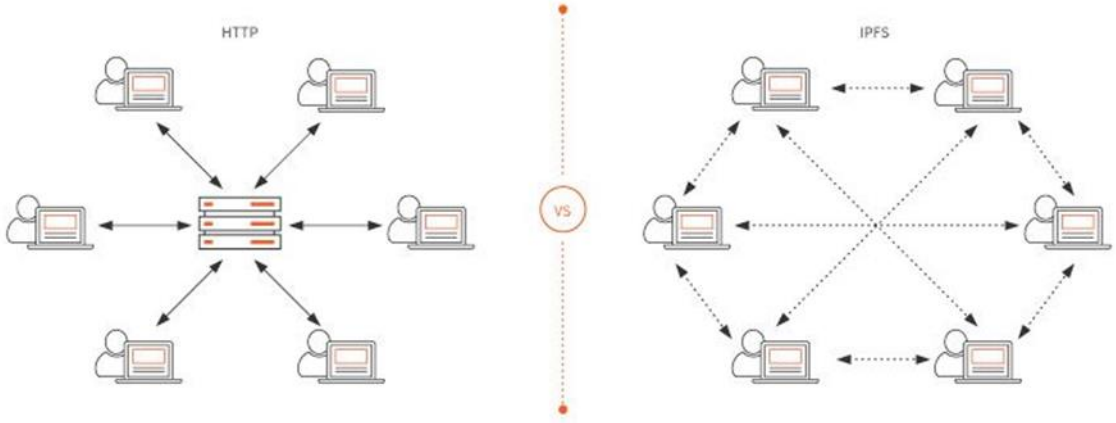

Fig 1.1 HTTP vs IPFS (courtesy [22])

Figure 1.1 shows a high-level architecture of HTTP (Hypertext Transfer Protocol) and IPFS (Interplanetary File System). HTTP and IPFS differ significantly in their approach to data sharing. HTTP follows a centralized client-server model, relying on live servers for data retrieval. In contrast, IPFS is a decentralized and persistent data storage across multiple nodes. IPFS uses cryptographic hashes for data retrieval, making it more efficient and bandwidth-friendly. While HTTP is an industry standard, IPFS offers a promising alternative for distributed computing, especially as its adoption continues to grow.

1. Motivation:

The motivation behind the work stems from the critical need to address the escalating crisis of data breaches within the healthcare sector. Recent incidents such as the cardiovascular consultants breach impacts 484k, healthec suffers data breach 112k, and Delta Dental of California moveit Hack Impacts 7M Individuals highlight the vulnerabilities inherent in the current security infrastructure governing medical records.

Traditional centralized cloud storage solutions, upon which healthcare organizations heavily rely, have proven deficient in safeguarding the highly sensitive and confidential nature of patient information [7]. This inadequacy exposes patient data to significant risks, including unauthorized access, cyber-attacks, and regulatory non-compliance.

The consequences of these breaches extend far beyond individual privacy concerns, impacting trust in healthcare institutions, compromising patient care, and resulting in legal and financial repercussions. In light of these challenges, there is an urgent need for a paradigm shift in the safeguarding of medical records.

1.1 Existing System:

The existing system for storing and managing medical records in the healthcare sector predominantly relies on centralized cloud storage solutions. These systems typically involve storing patient data in databases hosted on centralized servers managed by healthcare organizations or third-party service providers.

In the traditional centralized system:

i. Centralized Cloud Storage: Patient medical records, including personal information, diagnoses, treatment histories, and test results, are stored in centralized databases hosted on cloud servers. These databases are often managed by healthcare organizations or contracted third-party vendors (2).

ii. Access Controls: Access to patient records is typically managed through role-based access controls (RBAC) implemented within the centralized system. Healthcare professionals are granted varying levels of access based on their roles and responsibilities within the organization. However, granular access controls may be limited, leading to potential security vulnerabilities.

iii. Security Measures: Security measures such as firewalls, encryption, and access controls are implemented to safeguard patient data. However, the centralized nature of these systems poses inherent security risks, including single points of failure and increased vulnerability to cyber-attacks.

iv. Data Sharing: Sharing patient records between healthcare providers, insurance companies, and other authorized entities often involves manual processes or electronic health record (EHR) systems that may lack interoperability. Data exchange may occur through secure channels or electronic data interchange (EDI) protocols, but challenges related to data standardization and compatibility can hinder seamless information sharing

v. Regulatory Compliance: Healthcare organizations must adhere to strict regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, to ensure the privacy and security of patient information. Compliance efforts typically involve implementing security policies, conducting risk assessments, and implementing technical safeguards within the centralized system [10].

2.2 Limitations of Existing System:

Despite these measures, the existing centralized system has several limitations and vulnerabilities:

i. Single Point of Failure: Centralized cloud storage creates a single point of failure, where a breach or outage in the central database can result in widespread data loss or unauthorized access to patient records.

ii. Data Breach Risks: Centralized systems are susceptible to data breaches, insider threats, and cyber-attacks, posing significant risks to patient privacy and confidentiality.

iii. Limited Transparency: Centralized systems may lack transparency and auditability, making it challenging to trace data access and modifications, which can hinder accountability and compliance efforts [9].

iv. Interoperability Challenges: Lack of interoperability between different healthcare systems and databases can impede data exchange and care coordination, leading to fragmented patient care and inefficiencies in healthcare delivery [10].

In summary, while the existing centralized system provides a means for storing and managing medical records, it faces significant challenges related to security, privacy, transparency, and interoperability. These shortcomings underscore the need for alternative approaches, such as decentralized blockchain-based solutions, to address the evolving demands and vulnerabilities in healthcare data management.

2.3 Analysis of related literature work

The current investigation focuses on preserving patient's EHR while ensuring security and privacy. The work in [7] presents a systematic approach for implementing blockchain based approach for privacy. The need for security for health record is highlighted in [8] and proposes a frame work based on hyper-ledger smart contracts that further uses proof of stake (PoS) mechanism developed on hyper-ledger.

As per the reports of the several research works carried out [1]-[21], it is recommended to adopt Blockchain technology to protect EHR with privacy. However, it is found that very less no. of papers has highlighted authority or autonomy to patients to control their data. Novelty of this work is that it extending privacy control to individual patients by participating during the data sharing session. Further, the model adopts IPFS based distributed EHR storage and sharing. This work also analyses the cost for executing the smart contract and performance of IPFS for the considered record sizes.

As per the analysis of the papers, blockchain technology offers promising solutions for protecting patient data privacy. However, it is essential to consider the potential challenges and limitations of implementing such technology in healthcare settings [3].

2.4 The Contribution of this paper includes.

This paper proposes the development of a novel block chain-based system tailored specifically for securing medical records. Leveraging the inherent features of block chain technology including decentralization, immutability, and cryptographic security, the proposed solution aims to address the shortcomings of traditional centralized storage systems. By utilizing block chain, the system ensures tamper-proof and transparent record-keeping, reducing the risk of unauthorized access and data breaches.

Key features of the proposed system include decentralized data storage, encryption for data privacy, access control mechanisms, and immutable audit trails. Through the implementation of smart contracts, patients can retain ownership and control over their medical records, granting or revoking access to healthcare providers as needed. Additionally, the system facilitates secure and seamless data sharing between authorized parties, improving interoperability while maintaining data confidentiality and integrity.

2. Methodology adopted and DApp architecture

The research work has adopted the following seven steps:

I. Authentication via MetaMask: Users log in to the web application using MetaMask, ensuring secure and decentralized authentication. MetaMask provides a seamless integration with blockchain technology, enabling users to access their accounts securely.

II. Data Classification and Upload: Upon login, users can upload two types of data: crucial data requiring high security and daily use data with lower privacy concerns. To optimize costs, only crucial data is uploaded to the application. Users can classify the data during the upload process, ensuring that sensitive information is securely stored on the distributed blockchain network.

III. Integration with Pinata API: The application utilizes Pinata API to transfer data from the application to the Interplanetary File System (IPFS). Once the data is uploaded to IPFS, a unique hash is generated, serving as a reference to access the stored information.

IV. Transaction Triggering via Smart Contracts: Upon successful upload to IPFS, a smart contract is triggered, initiating a transaction on the blockchain. Users are prompted to accept the transaction and pay the estimated gas fees to complete the uploading process securely.

V. Access Control Mechanism: Users, acting as patients, have full control over granting access to their data. They can log in to the application and specify the address of the third party, such as an insurance company or hospital, to whom they want to grant access.

VI. Granting Access via Smart Contracts: When the patient clicks on the "Grant Access" button, a smart contract is triggered, adding access permissions for the specified third party. This action initiates a transaction on the blockchain, ensuring transparency and accountability in data sharing.

VII. Revoking Access: Patients also have the option to revoke access to their data at any time. By accessing the application and selecting the option to revoke access, the patient triggers a smart contract that removes the specified third party's access permissions. A transaction is then executed on the blockchain to reflect the change in access rights.

In line with the methodology adopted, the decentralized application architecture can be viewed as one adopted in [23].

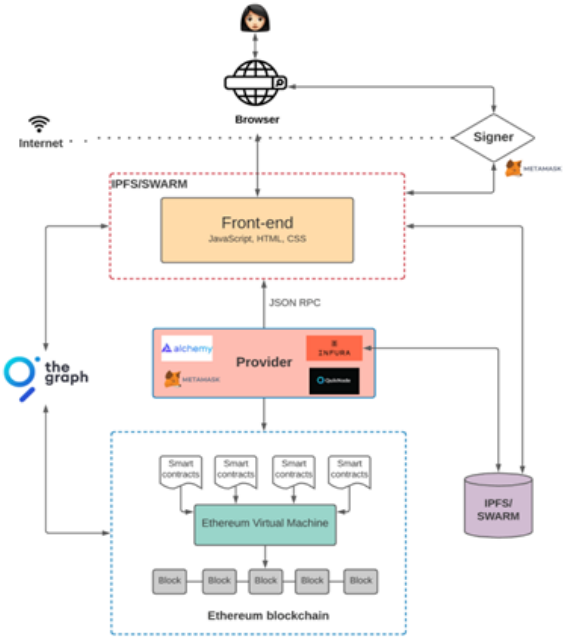

Fig 3.1.1 Application architecture (courtesy [23])

The architecture of the proposed system integrates cutting-edge technologies to establish a robust framework for managing medical records securely and efficiently. At its core, the architecture leverages React frontend for user interaction, providing a seamless interface for data upload and access control. The decentralized storage infrastructure is powered by Interplanetary File System (IPFS), ensuring data resilience and availability across distributed networks. Ethereum Virtual Machine (EVM) serves as the execution environment for smart contracts, written in Solidity, enabling trustless interactions and enforcing access control policies. MetaMask integration facilitates secure authentication and transaction signing, while Pinata API streamlines data transfer between the application and IPFS. This architecture not only enhances data security and privacy but also empowers users with greater control over their medical information, laying the foundation for a more transparent and patient-centric healthcare ecosystem

The working details of the application are further described with the help of a flow chart (Figure 3.1.2)

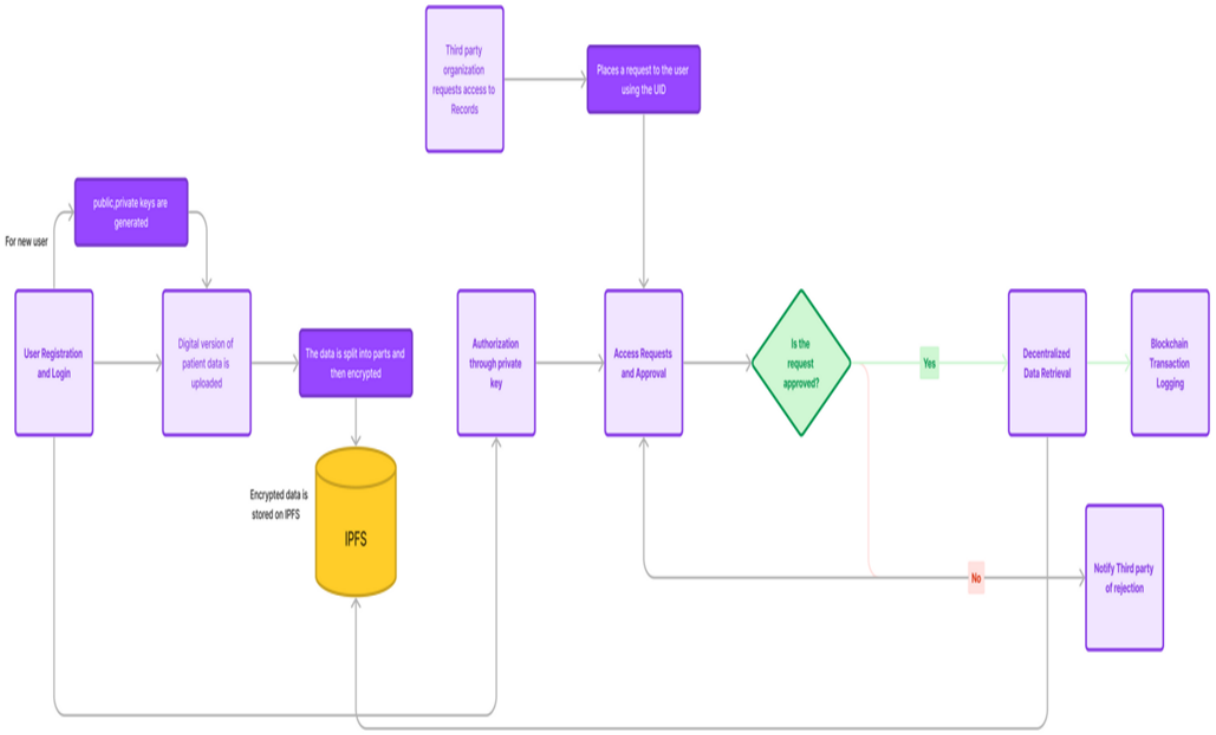

Fig 3.2.1 Set up of the experiment

3.2 Screenshots of the results

Before proceeding, it is essential to verify that the user has set up a MetaMask account and funded it with Ether. The application mandates compatibility with the MetaMask extension. Begin the process by logging into the application using your MetaMask credentials. This initial step establishes the foundation for seamless interaction with the platform's functionalities.

Fig 3.2.1 User trying to access data associated

The Figure 3.2.1 shows the screenshot of where user tries to access data associated with the address.

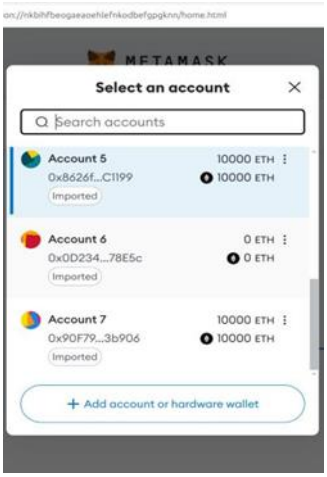

Fig 3.2.2 User can switch among different Accounts

To enhance privacy safeguards, utilize MetaMask's ability to seamlessly switch between different accounts within your wallet as shown in Figure 3.2.2. This feature enables users to manage multiple accounts effortlessly, thereby improving security by compartmentalizing sensitive information across various identities.

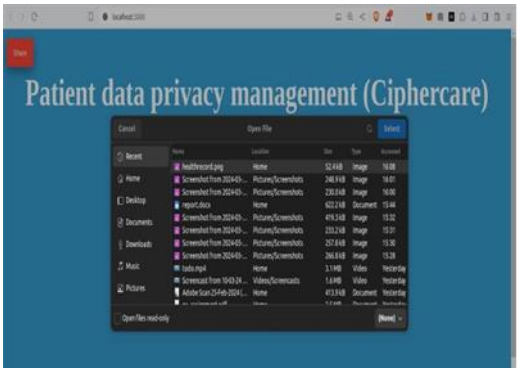

Fig 3.2.3 User uploads Health record to the application

Upon clicking "Get Data," the application initiates the retrieval process for files uploaded by the user. In cases where there are no files to display, the application prompts the message "No data to display" (Figure 3.2.3). This functionality is facilitated by querying the data stored on IPFS through the specific node associated with the application.

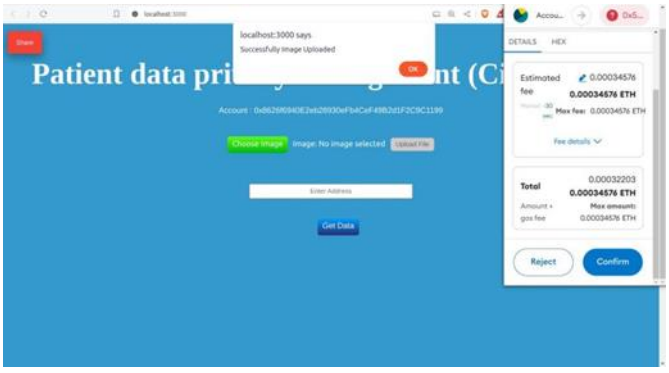

Fig 3.2.4 User approves the transaction

Upon successfully uploading a file to IPFS through the Pinata API, the application will display a notification confirming the successful upload (Figure 3.2.4). Subsequently, a transaction will be triggered on MetaMask, requiring user confirmation to authorize the transaction.

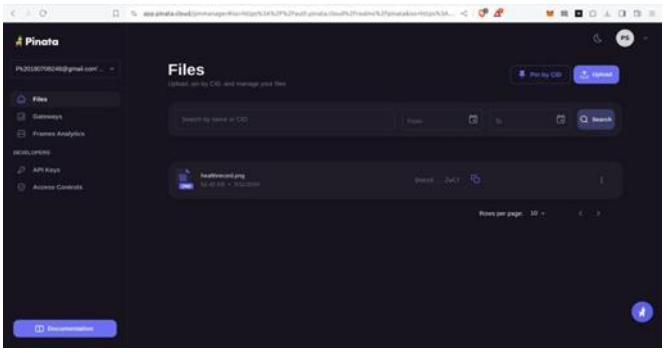

Fig 3.2.5 Pinata dashboard shows uploaded files

As observed in the IPFS storage, and shown in Figure 3.2.5 the file "healthcare.png" uploaded is visible.

Fig 3.2.6 Authorized third party accessing data

Upon entering the address and clicking on "Get Data," you'll receive a comprehensive list of all files uploaded by the associated account (Figure 3.2.6). The user can conveniently access each file by clicking on the respective link, which will open the file in a new browser tab for easy viewing Assuming the other address belongs to an insurance company or a hospital, proceed by copying the address from MetaMask and pasting it into the designated field. Then, click "Share Access." This action will initiate a transaction on MetaMask. Once the insurance company or hospital accepts the access request, access will be successfully granted to their account

4.0 Performance Evaluation:

The evaluation of our proposed framework's performance hinges on two pivotal metrics: deployment cost of smart contracts creation of transactions on each operation performed in the DApp, the processing time for user requests (upload, share access, access files).

Cost of deploying a smart contract

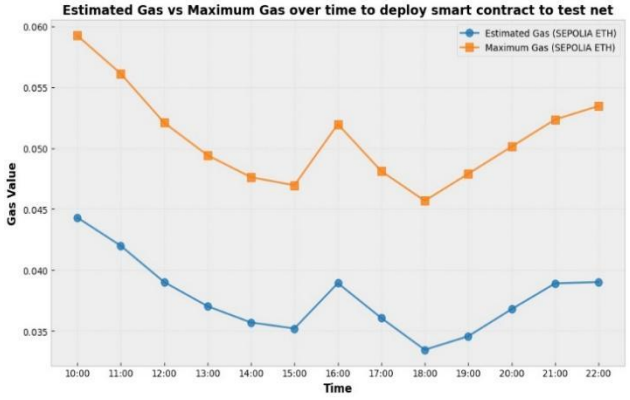

Fig 4.1.1 Estimated Gas vs Maximum Gas on Sepolia Test network

In our comprehensive assessment spanning 12 hours from 10 am to 10 pm, we meticulously analyzed the gas consumption for deploying smart contracts on our blockchain infrastructure. Notably, our findings showcase a remarkable similarity to conditions observed on the

Ethereum mainnet, affirming the reliability and scalability of our system for real-world deployment scenarios. The observed gas values, ranging from 0.03520519 to 0.04430964 SepoliaETH for estimated gas and 0.04694878 to 0.05923979 SepoliaETH for maximum gas, provide valuable insights into computational resource utilization. Furthermore, a comparative analysis with mainnet data reveals consistency in gas consumption patterns, validating the robustness of our infrastructure.

Additionally, efficiency metrics such as gas per transaction and scalability assessments underscore the cost-effectiveness and performance scalability of our system. This analysis extends to evaluating resource utilization efficiency over time, ensuring optimal performance and reliability. Ultimately, these findings bolster confidence in the readiness of our blockchain infrastructure for real-world deployment, emphasizing its efficiency and viability in comparison to the Ethereum mainnet.

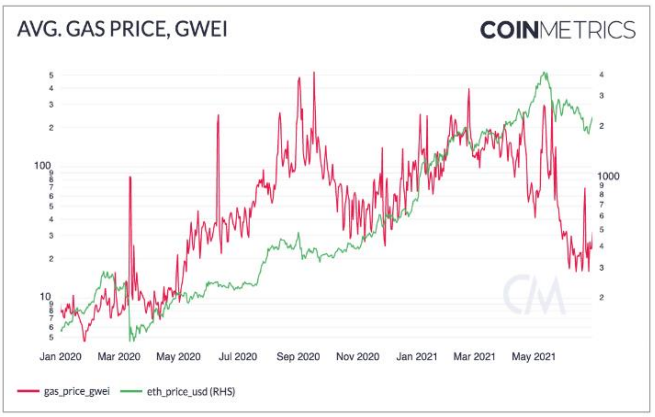

Fig 4.1.2 Gas dynamics Courtesy of COINMETRICS

Another critical consideration for our application is the fluctuating transaction fees, particularly concerning gas prices on the Ethereum main network. While we haven't directly tested our application on the main chain, it's crucial to acknowledge the potential impact of gas prices, especially given their dynamic nature. Gas prices can vary significantly depending on the current transactions being executed on the network. As depicted in the data graph, the volatility in gas prices can directly influence the cost of executing transactions within our application. Therefore, it's imperative to monitor and assess gas prices carefully, as they can affect the feasibility and affordability of using our application, particularly for users sensitive to transaction costs.

Investigating IPFS Performance and Potential: Results and Insights.

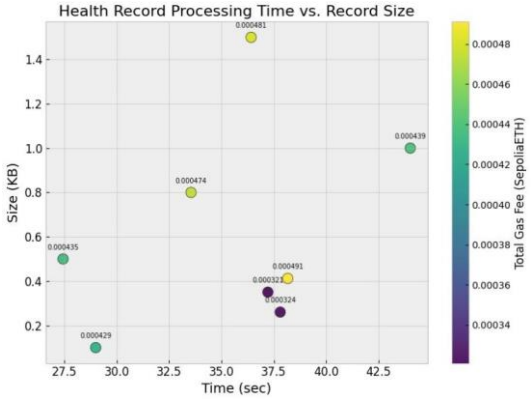

Fig 4.1.3 demonstrates the impact of file size on processing time during uploads, guiding optimization efforts. The graphical representation offers a nuanced exploration of the intricate dynamics governing file uploads within the Dapp and the time taken to upload files to IPFS. Through meticulous analysis, it unveils a compelling correlation between the size of uploaded files, transaction completion time, and associated gas fees. Notably, the graph reveals a trend where smaller files, typically below 1 KB, exhibit swifter transaction completion times, suggesting efficient processing mechanisms for lighter payloads. However, it is noteworthy that some files, despite their larger size, surprisingly take less time for transaction completion. This intriguing observation suggests that factors beyond file size alone, such as file complexity or network conditions, may influence transaction processing times. Nonetheless, as file sizes escalate beyond a certain threshold, there is a consistent increase in transaction completion time, indicating the escalating computational demands associated with larger uploads. This observation underscores the critical importance of optimizing transaction parameters and resource allocation strategies to streamline the upload process, thereby ensuring optimal performance and resource utilization across a spectrum of file sizes.

Furthermore, the graph's depiction of fluctuating gas fees across different file sizes underscores the multifaceted nature of cost considerations within the Dapp ecosystem. Such insights are invaluable for informing strategic decision-making and fine-tuning system parameters to strike a delicate balance between performance optimization and cost-effectiveness. Ultimately, this detailed analysis contributes significantly to the broader understanding of system dynamics and serves as a cornerstone for driving impact optimizations in Dapp development and deployment scenarios.

5.0 Future Enhancements:

In the road-map for future development, several enhancements are proposed to elevate the application's usability, security, and functionality. Firstly, a Django-based API will be implemented to segregate non-critical data and integrate it with a PostgreSQL database and this information which is non crucial can be stored in the cloud, ensuring that only crucial information is stored on IPFS.

Additionally, the dependency on Pinata API will be removed to prioritize data security as the application evolves into a patient-eccentric product. Furthermore, a peer-to-peer messaging service will be integrated to facilitate seamless communication between patients and third-party organizations, fostering collaboration and efficient data sharing. Lastly, an address book feature will be introduced, allowing users to assign and manage names for addresses, streamlining the process of sharing access and communicating with others. These enhancements collectively aim to bolster the application's robustness, user-friendliness, and data security, ultimately enhancing its capability to meet the diverse needs of patients and third-party organizations.

6. Conclusions

In conclusion, the proposed Blockchain based solution offers a promising approach to addressing the pressing security challenges facing the healthcare sector. By leveraging block chain technology, the project aims to enhance data protection, strengthen patient privacy, and restore trust in the secure handling of medical records

References

[1] kiania, K., Jameii, S.M. & Rahmani, A.M. Blockchain-based privacy and security preserving in electronic health: a systematic review. Multimed Tools Appl 82, 28493–28519 (2023). https://doi.org/10.1007/s11042-023-14488-w

[2] Liang Huang and Hyung-Hyo Lee, A Medical Data Privacy Protection Scheme Based on Blockchain and Cloud Computing, https://www.hindawi.com/journals/wcmc/2020/8859961/

[3] Alamri, B., Javed, I.T., Margaria, T. (2020). Preserving Patients' Privacy in Medical IoT Using Blockchain. In: Katangur, A., Lin, SC., Wei, J., Yang, S., Zhang, LJ. (eds) Edge Computing – EDGE 2020. EDGE 2020. Lecture Notes in Computer Science (), vol 12407. Springer, Cham. https://doi.org/10.1007/978-3-030-59824-2_9.

[4] Andrew J, Deva Priya Isravel, K. Martin Sagayam, Bharat Bhushan, Yuichi Sei, Jennifer Eunice, Blockchain for healthcare systems: Architecture, security challenges, trends and future directions, Journal of Network and Computer Applications, Volume 215,2023,103633, ISSN 1084-8045,

[5] https://doi.org/10.1016/j.jnca.2023.103633.

[6] Zhang, Y., Wang, D. Integrating blockchain technology and cloud services in healthcare: a security and privacy perspective. Proc.Indian Natl. Sci. Acad. 89, 837–850 (2023). https://doi.org/10.1007/s43538-023-00202-9

[7] Dong Y, Mun SK, Wang Y. A blockchain-enabled sharing platform for personal health records. Heliyon. 2023 Jul 8;9(7):e18061. doi: 10.1016/j.heliyon.2023.e18061. PMID: 37496910; PMCID: PMC10366433.

[8] Kiania K, Jameii SM, Rahmani AM. Blockchain-based privacy and security preserving in electronic health: a systematic review. Multimed Tools Appl. 2023 Feb 17:1-27. doi: 10.1007/s11042-023-14488-w. Epub ahead of print. PMID: 36811000; PMCID: PMC9936121.

[9] Amanat A, Rizwan M, Maple C, Zikria YB, Almadhor AS, Kim SW. Blockchain and cloud computing-based secure electronic healthcare records storage and sharing. Front Public Health. 2022 Jul 19; 10:938707. doi: 10.3389/fpubh.2022.938707. PMID: 35928494; PMCID: PMC9343689.

[10] M. S. Elsayed and M. A. Azer, "Health Records Privacy Issues in Cloud Computing," 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2018, pp. 1-6, doi: 10.1109/CAIS.2018.8441974.

[11] Raghavendra Ganiga, Radhika M. Pai, Manohara Pai M. M., Rajesh Kumar Sinha, Security framework for cloud based Electronic Health Record (EHR) system International Journal of Electrical and Computer Engineering (IJECE) ρ 455 Vol. 10, No. 1, February 2020, pp. 455~466

[12] J. Vora et al., "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," 2018 IEEE Globecom Workshops (GC

Wkshps), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6, doi: 10.1109/GLOCOMW.2018.8644088.

[13] Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[14] Han Y, Zhang Y, Vermund SH. Blockchain Technology for Electronic Health Records. Int J Environ Res Public Health. 2022 Nov 24;19(23):15577. doi: 10.3390/ijerph192315577.

[15] Muhammad Usman, Usman Qamar, Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology, Procedia Computer Science, Volume 174,2020, Pages, 321-327, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.06.093.

[16] V. Santhana Marichamy, V. Natarajan, Blockchain based Securing Medical Records in Big Data Analytics, Data & Knowledge Engineering, Volume 144,2023,102122, ISSN 0169-023X, https://doi.org/10.1016/j.datak.2022.102122.

[17] Rghioui, Anass. (2020). Managing Patient Medical Record using Blockchain in Developing Countries: Challenges and Security Issues. 1-6. 10.1109/Morgeo49228.2020.9121901.

[18] Pandey, P., & Litoriya, R. (2020). Securing and authenticating healthcare records through blockchain technology. Cryptologia, 44(4), 341–356. https://doi.org/10.1080/01611194.2019.1706060.

[19] M. T. Quasim, A. A. E. Radwan, G. M. M. Alshmrani and M. Meraj, "A Blockchain Framework for Secure Electronic Health Records in Healthcare Industry," 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, India, 2020, pp. 605-609, doi: 10.1109/ICSTCEE49637.2020.9277193.

[20] S D, Ashwini & Patil, Annapurna & Shetty, Savita. (2021). Moving Towards Blockchain-Based Solution for Ensuring Secure Storage of Medical Images. 1-5. 10.1109/INDICON52576.2021.9691516.

[21] Daraghmi, Eman & Daraghmi, Yousef-Awwad & Yuan, Shyan-Ming. (2019). Med Chain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2952942.

[22] Christo, Mary Subaja, Jesi, V. Elizabeth, Priyadarsini, Uma, Anbarasu Venugopal, Hridya, Karuppiah, Marimuthu Ensuring Improved Security in Medical Data Using ECC and Blockchain Technology with Edge Devices, https://doi.org/10.1155/2021/6966206.

[23] Rohit Sharma, article: Distributed File System: IPFS,

[24] https://medium.com/@rohit.sharma_7010/distributed-file-system-ipfs-e65aff6ad97d.

[25] Preethi Kasireddy, article: The Architecture of a Web 3.0 application, https://www.preethikasireddy.com/post/the-architecture-of-a-web-3-0-application.