[1]Ginavanee A

[2]Dr. S. Prasanna

Integration of Ethereum Blockchain with Cloud Computing for Secure Healthcare Data Management System

Abstract: - Effective management of health data is critical in this age of digital change. In order to solve the issues with safe healthcare data systems, this paper suggests a brand-new Hybrid Healthcare Data Management System (HDMS) that seamlessly combines blockchain and cloud computing technology. The solution guarantees the safe storage and effective administration of health data by utilizing the scalability and flexibility of cloud computing. The Ethereum blockchain, which offers immutability through smart contracts for data integrity assurance, is used to improve security. Important components of the suggested approach include Blockchain Anchoring, which uses distinct hash references on Ethereum to ensure data integrity, Google Cloud Integration for scalable storage and immediate data access, and compliance with Health Level 7 (HL7) formatting criteria for medical data storage. Robust privacy safeguards include cutting-edge methods like decentralized identifiers (DIDs) and homomorphic encryption, which guarantee secure computations on encrypted data and trustworthy identification for allowed access. IPFS file storage is used by the system to improve security by providing redundancy and resilience. By utilizing blockchain's immutability and cloud storage's distributed architecture, HDMS demonstrates resilience against disturbances. Results of the proposed method is implemented in Python Software. The Homomorphic approach that has been suggested continuously beats Optimized Blowfish Algorithm (OBA) in terms of encryption and decryption times. The improvement in encryption is between 3000ms (10 kb) and 1350ms (40 kb). The enhancement demonstrates improved efficiency across data sizes, ranging from 4000ms (10 kb) to 3350ms (40 kb) in decryption. The goal of HDMS is to create a future in which patient outcomes are enhanced by the appropriate handling, storage, analysis, and use of medical data.

Keywords: Ethereum Blockchain Technology, Cloud Computing, Inter Planetary File System, Data Privacy, Homomorphic encryption, Decentralized identifiers

I. INTRODUCTION

Healthcare, an indispensable aspect of modern society, stands as a linchpin for progress and well-being. In our digital age, the processing and storage of health data have surged to the forefront, introducing critical concerns about the integrity and security of patient records [1]. Traditional healthcare databases, once stalwarts of information storage, faced vulnerabilities that jeopardized data privacy and accuracy [2]. While Electronic Health Records (EHRs) were a pivotal advancement, they brought forth new complexities [3].

The relentless generation of EHRs, repositories of invaluable medical knowledge, promises to revolutionize patient care. However, the swift digital transition has heightened the urgency for robust data security, privacy, and accessibility [4]. The growing adoption of EHRs demands unprecedented measures to safeguard the confidentiality and availability of patients' private information. Despite this imperative need, the development of standardized protocols, data ownership frameworks, and stringent security procedures remains a formidable challenge in the healthcare sector [5].

Current data interoperability standards, centralized and challenging for healthcare providers, have hindered the seamless exchange of critical patient data [6]. The pressing need for standardized, secure data-sharing procedures has never been more evident [7]. These procedures not only facilitate private patient data communication but also offer medical professionals up-to-date, comprehensive insights into patients' health conditions. Striking a delicate

[1] Research Scholar, School of Computing Sciences, VISTAS, Chennai, India

Assistant Professor, Department of Computer, Applications, Agurchand Manmull Jain College, Chennai, India

ginainder@gmail.com

ORCID:0000-0003-0133-8399

[2]Professor, Department of Computer Applications, VISTAS, Chennai, India.

prasanna.scs@velsuniv.ac.in

ORCID : 0000-0001-8233-6277

balance between accessibility, privacy, and security is imperative for creating a future where healthcare data is not only shared but also safeguarded [8].

In this landscape, the integration of the Ethereum blockchain with cloud computing emerges as an innovative solution, addressing the intricate challenges posed by the digitalization of healthcare data. By seamlessly amalgamating RESTful APIs, cloud computing, and the Ethereum blockchain, this paper proposes a decentralized healthcare data management system. This novel approach ensures data immutability and transparency through advanced cryptographic methods and consensus procedures on the Ethereum blockchain. The integration of homomorphic encryption and decentralized identifiers (DIDs) further fortifies the security of stored medical records, enhancing patient privacy and data accuracy.

The implementation of the Inter Planetary File System (IPFS) within the cloud computing environment transforms the storage and retrieval of medical data. IPFS, with its distributed and redundant architecture, ensures secure storage and high availability of healthcare records. Storing file hashes on the Ethereum blockchain maintains references to medical documents and images securely, optimizing storage resources and providing a robust backup mechanism.

The ramifications of this integrated system are profound, offering healthcare professionals the power of predictive analytics, providing medical researchers with a secure data pool, and giving patients a more personalized and efficient healthcare experience. Cloud computing and Ethereum blockchain integration offer a strong solution for safe healthcare data management. By utilizing Ethereum's decentralized ledger, it provides the transparent and impervious storage of confidential health-related information. Smart contracts improve privacy by automating sharing of information and access management. Scalable and effective processing and storage are made possible by cloud computing. Here are the key contributions of this framework:

- In order to store medical data on the Ethereum blockchain, the system starts by following Health Level 7 (HL7) guidelines. This provides a regulated basis for data storage by guaranteeing compatibility and interoperability with current healthcare information systems.
- By securing distinct unique references for secure records, the Ethereum blockchain ensures the immutability of medical data. By offering a reliable and unalterable history of medical data, this improves data integrity and security.
- Blockchain security is combined with cloud infrastructure's effectiveness and adaptability as the system moves data to the Google Cloud environments. As a result, the requirement for effective healthcare data storage and retrieval is met. This also enables smooth scaling and accessibility.
- The system uses a RESTful API protected by strong encryption and authentication protocols to allow authorized users to access data. By doing this, critical information about medical patients is kept private and safe from unauthorized parties.
- Integrating homomorphic encryption with decentralized identifiers (DIDs) strengthens privacy. The confidentiality and security of healthcare data are improved when homomorphic encryption is used to protect privacy during data processing and DIDs help to provide safe and verifiable identity.

The subsequent sections of this paper will delve into previous research (Section 2), explore the integration of cloud computing and Ethereum blockchain (Section 3), present detailed experimental results (Section 4), and conclude with a summary and recommendations for future work (Section 5).

II. RELATED WORKS

In the realm of healthcare data management, addressing the challenges associated with Electronic Health Records (EHRs) has been a topic of substantial research and innovation. Scholars and practitioners alike have made significant strides in exploring various solutions to enhance the security, accessibility, and privacy of patient information. Several key themes have emerged in the existing literature, shedding light on the complexities of healthcare data management in the digital age.

2.1. Blockchain Technology in Healthcare Data Security:

Blockchain technology has garnered considerable attention for its potential to revolutionize healthcare data management [9]. Research efforts, as seen in studies [10], have delved into leveraging blockchain's decentralized

and immutable ledger to ensure the integrity and security of EHRs [11]. By employing cryptographic techniques and consensus algorithms, blockchain facilitates secure data sharing, access control, and tamper-proof storage of medical records, addressing longstanding concerns about data integrity and privacy [12].

2.2. Cloud Computing Solutions for Healthcare Data Storage:

Cloud computing has emerged as a robust infrastructure for storing and managing vast volumes of healthcare data [13]. Recent works [14] have explored cloud-based solutions, focusing on scalability, redundancy, and accessibility. Cloud platforms provide the necessary resources for storing EHRs securely while enabling efficient data retrieval and seamless integration with various healthcare applications [15]. These studies have emphasized the significance of cloud-based architectures in addressing the storage challenges posed by the digitalization of patient records.

2.3. Encryption Techniques and Privacy Preservation:

The preservation of patient privacy in EHRs has been a central concern for researchers. Encryption techniques, including homomorphic encryption, have been investigated to ensure secure storage and transmission of sensitive healthcare data. Studies [16] have explored advancements in encryption algorithms, enabling computations on encrypted data without compromising privacy. These techniques play a pivotal role in safeguarding patient confidentiality while allowing authorized entities to perform necessary operations on the data [17].

2.4. Inter Planetary File System (IPFS) and Decentralized Data Storage:

The integration of Inter Planetary File System (IPFS) with healthcare data management systems has been a recent area of exploration. Scholars [18] have examined the decentralized nature of IPFS, emphasizing its potential in ensuring fault-tolerant and redundant storage of medical records. By storing file hashes on block chain networks and leveraging IPFS for data storage, researchers have proposed innovative solutions that optimize storage resources and enhance data availability, even in the face of network outages or cyber-attacks [19].

2.5. Decentralized Identifiers (DIDs) for Patient Privacy:

Decentralized Identifiers (DIDs) have gained prominence as a solution for ensuring patient identity management and data access control. Research studies [20] have investigated the use of DIDs to empower patients with control over their health data. By enabling patients to manage their own unique identifiers securely, DIDs contribute significantly to data privacy and confidentiality. Incorporating DIDs into healthcare data management systems allows for seamless and secure patient data sharing while adhering to privacy regulations and enhancing patient trust.

2.6. Predictive Analytics and Artificial Intelligence in Healthcare:

The integration of predictive analytics and artificial intelligence (AI) algorithms has transformed healthcare data analysis. Recent research [21] has focused on leveraging AI techniques to process vast datasets and extract meaningful insights. Predictive analytics empower healthcare providers to proactively address patients' needs, enabling early intervention and personalized treatment plans. By analyzing patterns within EHRs, AI-driven systems contribute to improving patient outcomes, optimizing resource allocation, and enhancing the overall efficiency of healthcare services.

2.7. Standards and Regulations in Healthcare Data Management:

The landscape of healthcare data management is heavily influenced by standards and regulations to ensure ethical practices and data security. Studies [22] have emphasized the importance of adhering to established standards such as Health Level Seven (HL7) and regulations like the Health Insurance Portability and Accountability Act (HIPAA). Compliance with these standards not only ensures the interoperability of healthcare systems but also safeguards patient privacy and confidentiality. Researchers have explored the challenges and best practices associated with regulatory compliance, shedding light on the complexities of navigating the regulatory framework in healthcare data management.

2.8. User Experience and Human-Centered Design in Healthcare Systems:

User experience (UX) and human-centered design principles have become focal points in the development of healthcare data management interfaces. Recent literature [23] emphasizes the significance of designing user-friendly interfaces that facilitate seamless interaction with EHRs. Research in this domain explores the usability aspects of healthcare applications, ensuring that healthcare professionals can access and interpret patient data efficiently [24]. By incorporating UX design principles, healthcare systems can enhance workflow efficiency, reduce errors, and improve overall user satisfaction, thereby contributing to the successful adoption of digital healthcare solutions [25].

These existing works serve as a foundation for the present study, which aims to integrate the insights gained from these research endeavors. By synthesizing the knowledge and innovations from these related works, the proposed study proposes a novel approach that combines blockchain technology, cloud computing, and decentralized storage mechanisms to create a secure and efficient healthcare data management system. Through this integration, we aim to address the challenges identified in the literature and contribute to the ongoing discourse surrounding the evolution of healthcare data management strategies.

III. PROBLEM STATEMENT

In healthcare data management, a complex environment full of possibilities and obstacles is presented by the convergence of blockchain technology, cloud computing, encryption methods, decentralized storage solutions, patient privacy safeguards, predictive analytics, regulatory compliance, and user experience design. Even with the developments reported in the literature, there isn't a clear, comprehensive strategy for using these technologies to handle healthcare data. Previous research has focused on certain components, such blockchain for data integrity and cloud computing for scalability, but it has not examined how these parts may be combined to create a more complete system. There are still problems with maintaining smooth interoperability and complying with rules and guidelines like HL7 and HIPAA [22]. Data security and ethical issues are raised when predictive analytics and AI are used in the healthcare industry [21]. The development of interfaces that effectively satisfy the needs of healthcare professionals is hampered by a lack of knowledge on the actual applications of user-centered design principles in healthcare systems. In order to create a comprehensive healthcare data management system that successfully combines various technologies while putting user experience, legal compliance, and patient privacy first, this study aims to address these issues and gaps.

IV. PROPOSED WORK

4.1 Overview

Building upon the foundations laid by existing research and the innovative solutions presented in the integration of Ethereum blockchain with cloud computing for secure healthcare data management, our proposed work aims to further enhance the system's capabilities, ensuring a robust, scalable, and user-friendly healthcare data management ecosystem. Healthcare data management is at a crossroads, facing unprecedented challenges related to security, accessibility, and data integrity.

Traditional centralized systems have grappled with interoperability issues, data breaches, and the secure storage of vast volumes of medical data. This paper introduces a pioneering solution that revolutionizes healthcare data management—a decentralized ecosystem designed to meet the highest standards of security, accessibility, and data integrity.

The core premise of this innovative system is to leverage the benefits of both blockchain technology, specifically the Ethereum blockchain, and cloud computing, particularly the Google Cloud environment. Initially, HL7 standardized medical data was securely stored within the Ethereum blockchain, ensuring data immutability through the inherent trustworthiness of blockchain technology. However, in response to the evolving landscape of healthcare data management, the decision was made to transition to a hybrid approach.

In this evolved architecture, the medical data itself is now stored within the secure confines of the Google Cloud environment. This shift offers several advantages, including enhanced scalability, cost-efficiency, and real-time data access. To maintain the vital connection between the data and its immutable representation on the Ethereum blockchain, each piece of medical data is associated with a unique hash value—a cryptographic fingerprint. These hash values, acting as secure references, are meticulously mapped and anchored within the Ethereum blockchain

using smart contracts. This integration ensures that the integrity and provenance of the medical data are preserved, and any tampering is immediately detectable.

Crucially, the system is designed to facilitate seamless data retrieval for authorized users, whether they are healthcare professionals or patients themselves. This is made possible through a robust RESTful API layer that provides controlled and secure access to the medical data. Authentication and authorization mechanisms are in place to guarantee that only authorized parties can request and access the data. The system goes beyond mere data storage and retrieval; it embodies a commitment to data privacy and security.

Two key components, homomorphic encryption and decentralized identifiers (DIDs), play pivotal roles. Homomorphic encryption enables secure computations on encrypted data, safeguarding sensitive patient information even during processing. DIDs provide a decentralized identity management system, empowering patients with control over who accesses their data. To ensure the effective and secure storage of medical files within the Google Cloud environment, the system integrates the Inter Planetary File System (IPFS). This distributed file system not only enhances data availability but also strengthens data integrity.

The hybrid approach adopted in this system strikes a balance between the lightweight nature of blockchain storage and the redundancy and accessibility of cloud storage. Even in the face of network outages or cyber-attacks, the system guarantees the availability and integrity of healthcare records.

Practical applications of this system are far-reaching, including seamless electronic health record (EHR) interchange among healthcare professionals, ensuring quick access to critical patient information in emergencies. Additionally, predictive analytics integrated into the system empower healthcare providers to proactively address patients' needs, ultimately enhancing healthcare outcomes. Extensive simulations and real-world testing have validated the proposed approaches, demonstrating their efficacy and potential. Figure 1 represents the proposed architecture diagram of secure Healthcare Data Management System Using Ethereum Blockchain and Cloud Computing.

4.2 Medical Data Storage:

The initial phase of the data management strategy involves the meticulous storage of medical data on the Ethereum blockchain.

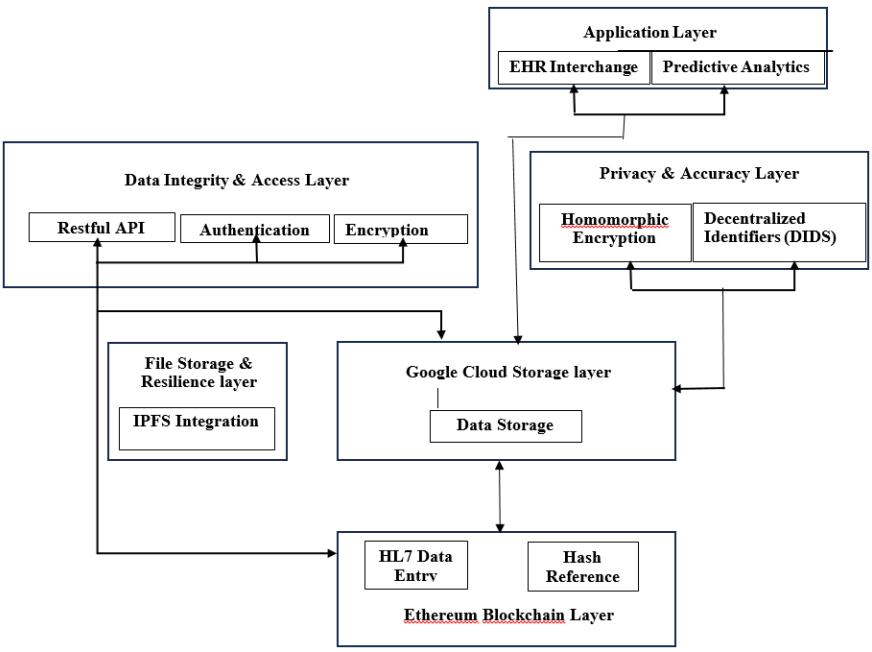

Figure 1: Proposed Architecture Diagram of Secure Healthcare Data Management System Using Ethereum Blockchain and Cloud Computing

This process is meticulously compliant with Health Level 7 (HL7) standards. HL7 standards are the global authority for electronic health information exchange, providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery, and evaluation of health services. In this system, every piece of medical data is first formatted according to these standards, ensuring a universal language for interoperability. The use of blockchain at this stage capitalizes on its inherent security features, like encryption and decentralized verification, to protect sensitive health information against unauthorized access and tampering.

Input: HL7 Data Entry

Output: Ethereum Blockchain Records, Hash Reference

step1. Receive HL7 Data Entry.

step2. Append the data to the Ethereum Blockchain Layer.

step3. Generate a Hash Reference for the recorded data.

step4. Update Ethereum Blockchain Records with the new data and hash.

step5. Return the Hash Reference.

Step6. End

4.3 Google Cloud Integration:

After the initial blockchain entry, the system seamlessly transitions the data to the Google Cloud platform. The motivation behind this move is twofold: scalability and speed. Google Cloud offers a robust infrastructure that can handle an expansive volume of data with ease, scaling as needed to meet demand. It also provides faster data retrieval times than traditional blockchain networks, which is critical for healthcare providers requiring immediate access to patient records. The integration process is engineered to be smooth and secure, transferring encrypted data without exposing it to risk.

Input: Data Storage Request

Output: Stored Data in Google Cloud

step1. Receive Data Storage Request.

step2. Store the data in the Google Cloud Layer.

step3. Update metadata.

step4. Return confirmation of successful storage.

Step5. End

4.4 Blockchain Anchoring:

While the bulk of the data resides in the cloud for practicality, the system maintains an immutable reference to the data on the Ethereum blockchain. This anchoring process involves creating unique hash references for each data set and storing these on the blockchain. The hashes serve as an unchangeable ledger of data integrity, ensuring that any information retrieved can be verified against its blockchain entry for authenticity. This step is vital for maintaining the non-repudiation and provenance of medical records, essential aspects of legal and medical accountability.

4.5 RESTful API:

Accessibility to this hybrid data system is facilitated through a RESTful API—a standardized architecture style for designing networked applications. The API acts as a secure gateway, allowing requests for data retrieval and submission to pass through only after rigorous authentication protocols are satisfied. It supports various methods, including GET, POST, PUT, and DELETE, which correspond to reading, creating, updating, and removing data, respectively. The API is designed to be both robust and flexible, incorporating the latest encryption standards to protect data in transit, and is built to accommodate a wide range of potential user interfaces, from healthcare provider portals to mobile apps.

Input: Data Access Request

Output: Access-Verified Data

step1. Receive Data Access Request.

step2. Validate through RESTful API.

step3. Authenticate the user.

step4. Apply encryption for secure data access.

step5. Perform integrity checks on the accessed data.

step6. If checks pass, provide access to verified data.

step7. If checks fail, deny access and log the attempt.

step8. End

4.6 Privacy and Accuracy:

Privacy and accuracy are paramount in healthcare data management. This system employs homomorphic encryption, a cutting-edge technique that allows data to be processed while still encrypted, thus never exposing the actual data. This encryption enables the performance of predictive analytics and other computations on patient data without compromising privacy. Furthermore, decentralized identifiers (DIDs) are used to verify the identities of individuals and organizations accessing the data. DIDs are a new type of identifier that enables verifiable, self-sovereign digital identities. They are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority, ensuring that the entity requesting data is who they claim to be.

Input: Data Operation in Privacy & Accuracy Layer

Output: Encrypted and Privacy-Preserved Data

step1. Apply Homomorphic Encryption to the data.

step2. Utilize Decentralized Identifiers (DIDs) for user privacy.

step3. Return the processed data.

step4. End

4.7 File Storage with IPFS:

To bolster the system's security and decentralization, the Inter Planetary File System (IPFS) is integrated for file storage. IPFS is a protocol and peer-to-peer network for storing and sharing data in a distributed file system. IPFS uses content-addressing to uniquely identify each file in a global namespace connecting all computing devices. By incorporating IPFS, the system ensures that files are not stored in a single location, thus safeguarding against data loss and ensuring redundancy. It also allows for faster data retrieval through a distributed network, as files can be downloaded in parallel from multiple nodes.

Input: File Storage Operation

Output: Resilient File Storage with IPFS

step1. Receive File Storage Operation.

step2. Integrate with IPFS for distributed file storage.

step3. Store files with redundancy for resilience.

step4. Update references on Ethereum Blockchain.

step5. Return confirmation of successful file storage.

step6. End

4.8 Disruption Resilience:

One of the system's key strengths is its resilience to disruptions. By leveraging the immutable nature of blockchain and the distributed architecture of cloud storage, the system ensures that data remains accessible and secure, even in the face of network outages or targeted cyber-attacks. This hybrid approach creates a robust infrastructure where the strengths of one technology compensate for the vulnerabilities of the other, providing an uninterrupted service that is crucial for healthcare operations.

4.9 Healthcare Applications:

The applications of this data management system in healthcare are extensive and transformative. It enables a seamless exchange of Electronic Health Records (EHR), allowing healthcare providers to access up-to-date patient records from anywhere, fostering better-informed clinical decisions. Additionally, the system supports advanced predictive analytics, which can analyze vast datasets to anticipate health trends, predict outcomes, and guide preventive healthcare measures. These capabilities can significantly enhance the quality of patient care and lead to better health outcomes on a large scale.

Input: Applications Requests (EHR Interchange, Predictive Analytics)

Output: Application Outputs

step1. Enable Electronic Health Record (EHR) Interchange.

step2. Implement Predictive Analytics for healthcare insights.

step3. Integrate applications with the system components.

step4. Return outputs based on application requests.

step5. End

4.10 Homomorphic Encryption Algorithm

This cryptographic technique enables computations on encrypted data without the need for decryption. In the healthcare domain, where data privacy is paramount, homomorphic encryption offers a powerful tool to perform analytics on sensitive medical records while preserving patient confidentiality. This algorithm empowers healthcare analytics while adhering to the principles of data confidentiality and integrity.

Algorithm:

Input: HL7 Health Dataset

- *The dataset containing health data entries (Hi) is the primary input.*

- *Each Hi represents a specific health data entry, such as patient records, medical test results, or any other relevant healthcare information.*

Output: Encrypted Data and Decrypted Result

Step 1: Initialize Homomorphic Encryption Parameters

- Choose encryption parameters (public key \(pk\) and private key \(sk\)) for healthcare data.

- Define the homomorphic encryption scheme suitable for medical records.

Step 2: Encrypt the Health Data

- For each health data entry \(Hi\) in the dataset:

- \(Encrypted_{Hi} = Encrypt (pk, Hi) \)

Step 3: Perform Homomorphic Operations

- Specify the homomorphic operations needed for healthcare analytics.

- Perform computations on the encrypted health data without decryption.

Step 4: Decrypt the Analytical Result

- \ (Decrypted {Analytical Result} = Decrypt (sk, Homomorphically Computed Result) \)

Step 5: End

Whereas,

- *pk represents the public key used for encrypting healthcare data.*
- *sk represents the private key used for decrypting analytical results.*
- *Encrypt (pk, Hi) denotes the encryption of health data entry Hi using the public key pk.*
- *Homomorphically Computed Result represents the result obtained after performing homomorphic operations on the encrypted health data.*
- *Decrypt (sk, Homomorphically Computed_ Result) denotes the decryption of the homomorphically computed analytical result using the private key sk.*

4.11 Decentralized Identifiers (DIDs)

Decentralized Identifiers (DIDs) provide a secure and self-owned method of identification, crucial for maintaining privacy and ownership control over healthcare data.

Algorithm:

Input:

- *Entity Information: Healthcare Provider "Hybrid Healthcare"*
- *ECC (Elliptic Curve Cryptography), Elliptic Curve: secp256k1*

Output:

- *Public-Private Key Pair:*

  (pk DID, sk DID)

- *DID Document:*

DID Document= {pk DID, "Hybrid Healthcare"}: A structured document containing the public key (pk DID) and the entity information.

- *DID Hash:*

DID Hash=Hash (DID Document): The unique hash of the DID document obtained through SHA-256.

- *Encoded DID:*

DID=Encode (DID Hash): The final decentralized identifier obtained by Base58 encoding the hash.

Algorithm Steps:

Step 1: Initialize Parameters:

- *Elliptic Curve: secp256k1*
- *Entity Information: "Hybrid Healthcare"*

Step 2: Generate Public-Private Key Pair:

- *Utilize ECC (Elliptic Curve Cryptography) with secp256k1 to generate the public-private key pair for "Hybrid Healthcare."*
- *(pk DID, sk DID) = ECC Key Generation ("Hybrid Healthcare", secp256k1)*

Step 3: Encode DID:

- *Encode the hash of the DID document using Base64 to create the final DID.*
- *DID=Encode_Base64(DID Hash)*

Step 4: End

The Ethereum Blockchain is essential to maintaining the security and integrity of healthcare data in the suggested approach. To ensure data integrity, it uses smart contracts to store data in an immutable manner and to anchor distinct hash references. Decentralized IDs and advanced encryption techniques ensure secure access, and authentication is essential to protecting patient data. Cloud computing's scalability is leveraged by the Ethereum Blockchain, while data privacy and protection are improved by authentication. When combined, they create a strong base that allows for the safe management of healthcare data, tamper-proof records, and strict access restrictions, protecting the integrity and security of private medical data in the digital era.

V. RESULTS AND DISCUSSION

The Results and Discussion section constitutes a thorough exploration and interpretation of the study's findings. Within this section, we present the outcomes derived from our proposed study, analyze their significance, and delve into their implications concerning the research questions or objectives. Specifically, we detail the intricacies of medical data storage in the cloud, accompanied by hash values mapped in the Ethereum blockchain. This presentation incorporates a diverse set of statistical analyses, visualizations, and comparisons to articulate the nuances of our approach. Our proposed methodology not only demonstrates efficiency, security, and innovation but also envisions a future where healthcare data is not merely stored but meticulously safeguarded, intelligently analyzed, and optimally utilized to advance superior healthcare outcomes.

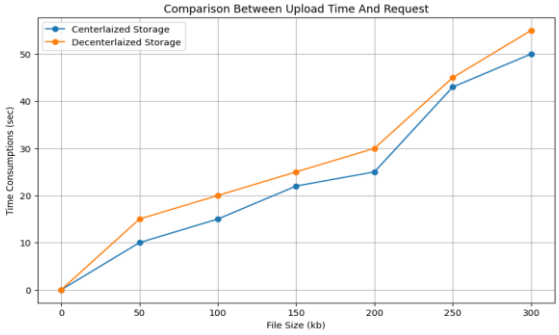

Figure 2: Comparison Between Upload Time and Request

Figure 2 provides information about how file size affects performance for both decentralized and centralized storage. Because decentralized storage is distributed, its response time may vary depending on the size of the file, whereas centralized storage might be more efficient for smaller files.

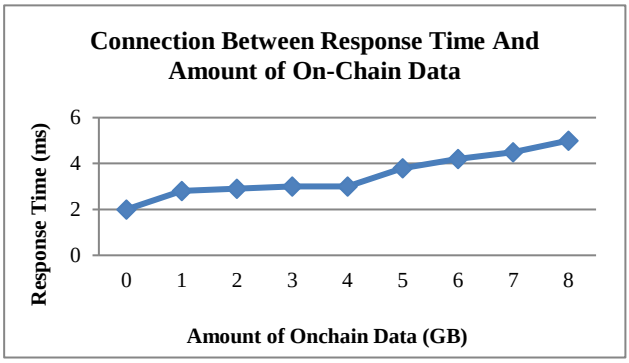

Figure 3: Connection Between Response Time and Amount of On-Chain Data

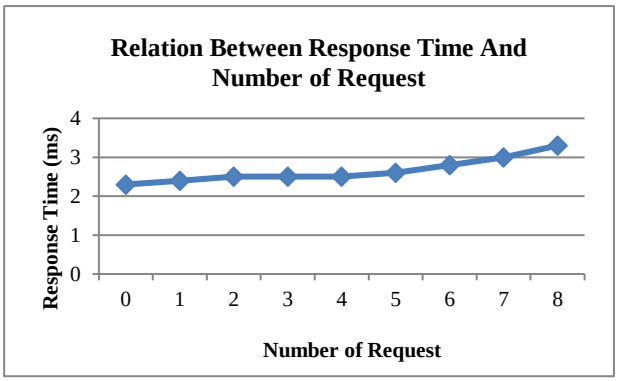

Figure 4: The Relation Between Response Time and Query Count

Figures 3 and 4 illustrate the intricate relationship between information response time and both the volume of on-chain data and the frequency of traceability requests in the context of healthcare data management. In Figure 3, the information response time exhibits an increase, ranging from 2ms to 5ms, corresponding to the growth in on-chain data volume from 1G to 9G. Additionally, as depicted in Figure 4, the information response time undergoes a slight increment, moving from approximately 2.2ms to 3.2ms. This change is associated with the rise in traceability requests from 1,000 times per second to 9,000 times per second, while keeping the on-chain data fixed at 1G. These findings provide valuable insights into the dynamic factors influencing information response times in the healthcare domain.

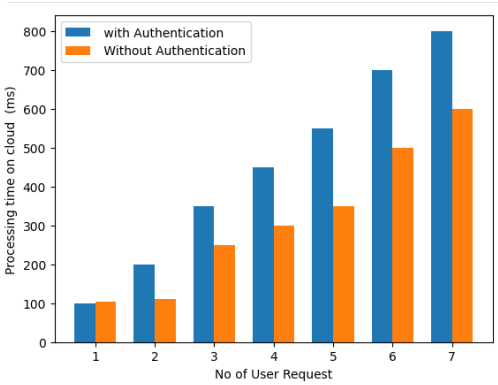

Figure 5: Processing Time on Cloud

The impact of authentication overhead is demonstrated by Figure 5 that compares user requests made with and without cloud authentication. The extra processes involved in verification during authentication may cause

processing times to increase. Optimizing cloud systems to strike a balance between security and performance requires an understanding of this trade-off.

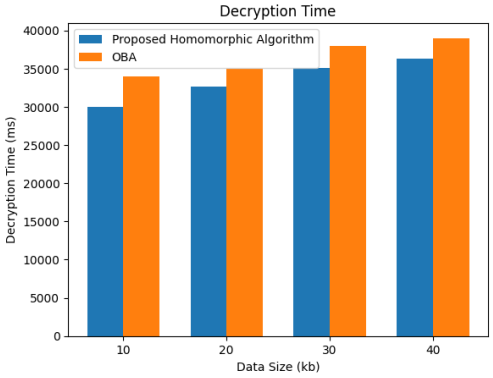

Figure 6: Decryption Time

The effectiveness of the Proposed Homomorphic algorithm (HA) in comparison to the baseline OBA is displayed in Figure 6. HA continuously beats OBA with different data volumes, demonstrating its superiority in terms of decryption time. This shows that HA may be able to speed up cryptographic procedures in applications involving secure data processing.

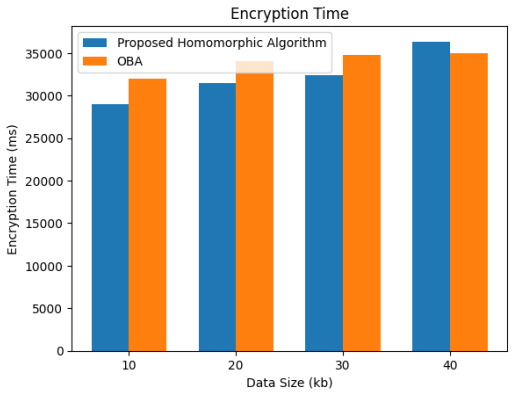

Figure 7: Encryption Time

Figure 7 shows how effective the Proposed Homomorphic Algorithm (HA) is at different data sizes when compared to the baseline OBA. HA's effectiveness in cutting down on encryption time is demonstrated by its consistent outperformance of OBA. This shows that HA has the ability to accelerate cryptographic operations for applications involving safe data transfer.

5.1. Discussion

The results that are displayed several aspects of data security and management. The results highlight the necessity to combine system efficiency in cloud processing time with security measures, highlighting the trade-off between file size and performance in centralized and decentralized storage. Response time in healthcare data management is closely related to traceability request frequency and on-chain data volume, providing important information for system optimization. The faster encryption and decryption durations of the Proposed Homomorphic Algorithm (HA) in comparison to the baseline OBA [26] indicate that HA has the potential to accelerate cryptographic procedures for safe data handling and transfer. In especially for healthcare applications, these factors offer insightful guidance for creating effective and safe data management systems.

VI. CONCLUSION AND FUTUREWORK

In the realm of healthcare data management, the Hybrid Healthcare Data Management System Algorithm emerges as a groundbreaking solution, seamlessly integrating advanced technologies to establish a robust and secure framework. Initiated by orchestrating key components such as the Ethereum Blockchain Layer, Google Cloud

Layer, Data Integrity & Access Layer, Privacy & Accuracy Layer, File Storage & Resilience Layer, and Applications Layer, the algorithm unfolds like a cohesive symphony. The lifeblood of healthcare information undergoes meticulous entry and hashing processes, finding a secure haven within the Ethereum Blockchain Layer, generating immutable Hash References. The subsequent journey to Google Cloud ensures efficient and scalable storage, laying the groundwork for the next algorithmic stages. Prioritizing data integrity and access, the algorithm employs RESTful API validation, user authentication, and robust encryption measures. Privacy & Accuracy measures introduce heightened security, featuring Homomorphic Encryption and Decentralized Identifiers (DIDs) as guardians of sensitive healthcare information. File Storage & Resilience, powered by IPFS integration, transforms file storage into a distributed and resilient paradigm. Applications at the architecture's zenith, including Electronic Health Record (EHR) Interchange and Predictive Analytics, open gateways to unprecedented healthcare insights. As the algorithm gracefully concludes, focus shifts to ongoing system maintenance, encompassing blockchain record updates, continuous data storage optimization, and unwavering security vigilance. Regular audits and updates to authentication and encryption protocols reinforce the system's resilience against evolving threats. Beyond its technical prowess, the algorithm pioneer's efficiency, security, and innovation, promising a future where healthcare data isn't merely managed but safeguarded, analyzed, and utilized to its full potential, ultimately enhancing healthcare outcomes.

REFERENCE

[1] G. Srivastava, R. M. Parizi, and A. Dehghantanha, "The Future of Blockchain Technology in Healthcare Internet of Things Security," in *Blockchain Cybersecurity, Trust and Privacy*, K.-K. R. Choo, A. Dehghantanha, and R. M. Parizi, Eds., in Advances in Information Security. , Cham: Springer International Publishing, 2020, pp. 161–184. doi: 10.1007/978-3-030-38181-3_9.

[2] "Cloud-based Healthcare data management Framework," *KSII TIIS*, vol. 14, no. 3, Mar. 2020, doi: 10.3837/tiis.2020.03.006.

[3] A. Sajid and H. Abbas, "Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges," *J Med Syst*, vol. 40, no. 6, p. 155, Jun. 2016, doi: 10.1007/s10916-016-0509-2.

[4] A. Rehman, S. Naz, and I. Razzak, "Leveraging Big Data Analytics in Healthcare Enhancement: Trends, Challenges and Opportunities." arXiv, Apr. 05, 2020. Accessed: Nov. 21, 2023. [Online]. Available: http://arxiv.org/abs/2004.09010

[5] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. N. Qureshi, "Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare," *Healthcare*, vol. 9, no. 6, p. 712, Jun. 2021, doi: 10.3390/healthcare9060712.

[6] T. Lysaght, H. Y. Lim, V. Xafis, and K. Y. Ngiam, "AI-Assisted Decision-making in Healthcare," *ABR*, vol. 11, no. 3, pp. 299–314, Sep. 2019, doi: 10.1007/s41649-019-00096-0.

[7] R. Kirkscey, "mHealth Apps for Older Adults: A Method for Development and User Experience Design Evaluation," *Journal of Technical Writing and Communication*, vol. 51, no. 2, pp. 199–217, Apr. 2021, doi: 10.1177/0047281620907939.

[8] S. Routray and R. Ganiga, "Secure Storage of Electronic Medical Records(EMR) on Interplanetary File System(IPFS) Using Cloud Storage and Blockchain Ecosystem," in *2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Sep. 2021, pp. 1–9. doi: 10.1109/ICECCT52121.2021.9616690.

[9] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," *Computer Communications*, vol. 153, pp. 311–335, Mar. 2020, doi: 10.1016/j.comcom.2020.02.018.

[10] H. B. Mahajan *et al.*, "Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems," *Appl Nanosci*, vol. 13, no. 3, pp. 2329–2342, Mar. 2023, doi: 10.1007/s13204-021-02164-0.

[11] J. Paul, M. S. M. S. Annamalai, W. Ming, A. A. Badawi, B. Veeravalli, and K. M. M. Aung, "Privacy-Preserving Collective Learning With Homomorphic Encryption," *IEEE Access*, vol. 9, pp. 132084–132096, 2021, doi: 10.1109/ACCESS.2021.3114581.

[12] L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, "Blockchain-Based Approach for e-Health Data Access Management with Privacy Protection," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Sep. 2019, pp. 1–7. doi: 10.1109/CAMAD.2019.8858469.

[13] M. Taleka, K. Makkithaya, and N. V G, "A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records," *Cogent Engineering*, vol. 9, Mar. 2022, doi: 10.1080/23311916.2022.2035134.

[14] S. Cao, X. Zhang, and R. Xu, "Toward Secure Storage in Cloud-based eHealth Systems: A Blockchain-Assisted Approach," *IEEE Network*, vol. 34, no. 2, pp. 64–70, Mar. 2020, doi: 10.1109/MNET.001.1900173.

[15] R. Saha, G. Kumar, M. K. Rai, R. Thomas, and S.-J. Lim, "Privacy Ensured ${e}$ -Healthcare for Fog-Enhanced IoT Based Applications," *IEEE Access*, vol. 7, pp. 44536–44543, 2019, doi: 10.1109/ACCESS.2019.2908664.

[16] R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange," *IEEE Access*, vol. 8, pp. 113467–113486, 2020, doi: 10.1109/ACCESS.2020.3003575.

[17] M. Mehrtak *et al.*, "Security challenges and solutions using healthcare cloud computing," *Journal of Medicine and Life*, vol. 14, no. 4, p. 448, Aug. 2021, doi: 10.25122/jml-2021-0100.

[18] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, *Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity*. 2020, p. 317. doi: 10.1109/ICIoT48696.2020.9089570.

[19] Y. Kang, J. Cho, and Y. B. Park, "An Empirical Study of a Trustworthy Cloud Common Data Model Using Decentralized Identifiers," *Applied Sciences*, vol. 11, no. 19, p. 8984, Sep. 2021, doi: 10.3390/app11198984.

[20] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain, "A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes," *IEEE Access*, vol. 8, pp. 118433–118471, 2020, doi: 10.1109/ACCESS.2020.3004790.

[21] S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty, "Interoperability and Synchronization Management of Blockchain-Based Decentralized e-Health Systems," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1363–1376, Nov. 2020, doi: 10.1109/TEM.2020.2989779.

[22] J. Sun, L. Ren, S. Wang, and X. Yao, "A blockchain-based framework for electronic medical records sharing with fine-grained access control," *PLOS ONE*, vol. 15, no. 10, p. e0239946, Oct. 2020, doi: 10.1371/journal.pone.0239946.

[23] S. S and J. S. Raj, "INTERNET OF THINGS AND BIG DATA ANALYTICS FOR HEALTH CARE WITH CLOUD COMPUTING," *JITDW*, vol. 01, no. 01, pp. 9–18, Sep. 2019, doi: 10.36548/jitdw.2019.1.002.

[24] L. Syed, S. Jabeen, M. S., and A. Alsaeedi, "Smart healthcare framework for ambient assisted living using IoMT and big data analytics techniques," *Future Generation Computer Systems*, vol. 101, pp. 136–151, Dec. 2019, doi: 10.1016/j.future.2019.06.004.

[25] C. Regueiro, I. Seco, S. de Diego, O. Lage, and L. Etxebarria, "Privacy-enhancing distributed protocol for data aggregation based on blockchain and homomorphic encryption," *Information Processing & Management*, vol. 58, no. 6, p. 102745, Nov. 2021, doi: 10.1016/j.ipm.2021.102745.

[26] S. I. Shyla and S. S. Sujatha, "Efficient secure data retrieval on cloud using multi-stage authentication and optimized blowfish algorithm," *J Ambient Intell Human Comput*, vol. 13, no. 1, pp. 151–163, Jan. 2022, doi: 10.1007/s12652-021-02893-8.