HEALTHSOLID 4.0: A NOVEL SOLID-POD AND BLOCKCHAIN-ENABLED FRAMEWORK FOR ROLE-BASED ACCESS CONTROL AND SECURE HEALTHCARE INFORMATION EXCHANGE

Avani Dadhania(1), Hiren Patel (2)*

[(1)]Research Scholar, Kadi Sarva Vishwavidyalaya, Sarva Vidyalaya Kelavani Mandal, Gandhinagar, 382415; [(2)]Vidush Somany Institute of Technology and Research, Kadi Sarva Vishwavidyalaya, Sarva Vidyalaya Kelavani Mandal, Kadi, 382715 India

* Corresponding Author, e-mail: avani26.22@gmail.com

Abstract: Several blockchain-based models have surfaced in recent years to offer a safe method of storing and accessing delicate electronic medical records (EMRs) and role-based access control mechanisms across the healthcare industry. However, single points of failure, Security, privacy and unauthorized access of data are measure concerns for health records access management. Blockchain technology is a decentralized digital ledger that records transactions across multiple computers to ensure security, transparency, and immutability. Solid is a decentralized platform that provides patient centric access control of Electronic Medical Records (EMRs). In this study, a blockchain and solid-pod enabled secure framework has been proposed for EMR transactions and healthcare clouds. This has a significant impact on how quickly and easily emergency EMRs may be shared in a smart healthcare system. Solid and Blockchain prioritize privacy and security by enabling users to set immutable, transparent, and fine-grained access controls for their data using solidity-based smart contracts. For the performance evaluation of our proposed system, solid-pod computing and storage results are analyzed.

Key words: Role-Based Access Control, Healthcare System, Blockchain Technology, Security

1. INTRODUCTION

For data storage and sharing in a distributed context, blockchain has evolved into an uncontestable, auditable, and timestamp-based block ledger. Smart contracts, Bitcoin, and personal data are all used in the storing of data for payment purposes. The development of important characteristics like device setup, security, privacy, and anonymity has drawn the attention of researchers to blockchain technology. The participant nodes are shared over the network while it maintains the ledger transaction in a distributed environment. The healthcare cloud architecture employs a concept to provide on-request log on and access control to a collective pool of programmable sources that may be instantly built and supplied with no preservation constraints. The main concerns surrounding EMR sharing in the healthcare industries are privacy

protection, access-control, data security, and interoperability among multiple healthcare organizations. The reliability of EMRs is crucial because a reliable healthcare record may more precisely reflect the state of the world today and advance medical care. Furthermore, EMRs contain private information about patients, which makes them appealing to cybercriminals.

The proposed research work is organized as follows: Section 2 discusses the literature survey. Section 3 discussed the details related to HealthSolid 4.0 system architecture, methodology, and process flow. Section 4 describes the obtained results, graphical analysis, and section 5 discusses the concluding remarks.

2. RELATED WORK

In this section, we present a comprehensive literature survey on the implementation of blockchain-based access control systems within the healthcare industry. Ahmed and fellow researchers have proposed an emergency record management and access control system for personal record management purposes. However, they did not discuss any ideas related to secure healthcare data retrieval and providing security using solid-pod and blockchain-enabled secure healthcare data exchange framework [1]. Su and his team have discussed cloud and edge computing-based healthcare system for healthcare record management. However, they did not propose any frameworks related to secure information exchange using blockchain and solid-pod methodology [2]. Rai has proposed a patient-centric healthcare system for handling patient history, medical records, and personal information. However, he did not discuss anything related to providing security to healthcare cloud systems [3]. Abutaleb and fellow researchers have discussed concepts related to healthcare security, integrity, and patient-centric healthcare system. However, they did not propose or discuss any frameworks related to blockchain and Solid-Pod enabled security framework for healthcare clouds. Furthermore, they did not discuss security in centralized and decentralized IoT environments [4]. Sharma and his research team have discussed ideas related to enhancing security. They also propose an IoT-enabled healthcare framework using blockchain. However, they did not discuss anything related to data retrieval and storage using Solid-Pod technology. Furthermore, they did not propose a complete healthcare framework that can secure patient personal information and medical records [5]. Wazid and fellow team members have discussed a novel blockchain enabled security solution for an IoT-enabled healthcare ecosystem [6]. Furthermore, they also discuss ideas related to securing patient personal information and medical records using block-based healthcare frameworks. However, they did not discuss any ideas related to integrating solid-pod with blockchain technology to overcome healthcare data retrieval and storage related issues. Mittal and fellow researchers have proposed a two-level healthcare security framework using blockchain technology [7]. However, they did not discuss any concepts related to integrating solid-pod with blockchain technology to resolve data storage and retrieval concerns. Fugkeaw and his team members have proposed a blockchain enabled light-weight security framework for healthcare data [8]. However, they did not discuss anything related to overcoming blockchain methodology, data access and storage concerns. Ali and fellow research team members have proposed a privacy preservation approach to secure patient personal information and medical records using blockchain technology [9]. However,

they did not discuss anything related to data retrieval and storage using Solid-pod technology. Furthermore, they did not propose a complete healthcare framework which can secure patient personal information and medical records. Román-Martínez and team have proposed a service-oriented framework for healthcare data using blockchain technology. However, they did not discuss any concepts related to integrating solid-pod with blockchain technology to resolve data storage and retrieval concerns [10]. Alsuqah and his team have proposed a privacy-enabled framework for healthcare data using blockchain technology [11]. Sharma and fellow researchers have proposed a blockchain-enabled medical things system for healthcare data. However, they did not discuss any ideas related to integrating solid-pod with blockchain technology to overcome healthcare data retrieval and storage related issues [12]. Baucas and fellow researchers have discussed a federated machine learning based security framework integrating blockchain technology. However, they did not discuss anything related to overcoming blockchain methodology, data retrieval and storage concerns [13]. Pawar and fellow research team members have proposed a scalable security framework for healthcare data using blockchain technology. However, they did not discuss anything related to data retrieval and storage using Solid-pod technology [14]. Mokhamed and fellow researchers have discussed concepts related to applying blockchain technology to dental data. However, they did not discuss any ideas related to integrating solid-pod with blockchain technology to overcome healthcare data retrieval and storage related issues [15]. Ali and fellow research team members have proposed Metaverse-enabled healthcare framework to secure patient personal information and medical records using blockchain technology [16]. However, they did not discuss anything related to data retrieval and storage using Solid-pod technology. Mallick and team have proposed an assistive healthcare framework using blockchain technology to secure patient personal and medical information [17]. However, they did not discuss any ideas related to integrating blockchain and solid-pod technology to secure healthcare information exchange. Maher and fellow researchers have discussed a proposal related to securing healthcare data using blockchain enabled methodology. However, they did not propose any blockchain enabled framework to secure healthcare related information [18]. Gao and his fellow research members have discussed concepts related to integrating cloud computing with blockchain technology for electronic medical records. However, they did not discuss any ideas related to integrating solid-pod with blockchain technology to overcome healthcare data retrieval and storage related issues [19]. Gupta and his team have discussed the initial idea of integrating blockchain technology for healthcare monitoring and security of patient data. However, they did not propose or discuss any frameworks related to Blockchain and Solid-Pod enabled security framework for healthcare clouds [20].

3. HEALTHSOLID 4.0 SYSTEM ARCHITECTURE AND METHODOLOGY

In the presented study, a blockchain and solid-pod integrated HealthSolid 4.0 Framework has been discussed. Blockchains cannot be changed. Any healthcare data placed on the blockchain nodes cannot be removed or altered after it has been saved. It's a record-keeping system that can only be expanded upon, not changed, or eliminated. Conventional databases that handle transactions are made to be updated. This

immediately makes blockchains perfect for certain use cases, but not all of them [21]. In our published paper entitled “e-DRBAC-HC: Extended Decentralized Role-Based Access Control for Healthcare System using Blockchain" [22], we proposed a decentralized role based access control framework for healthcare system using blockchain for secure data access on IPFS (InterPlanetary File System) storage. InterPlanetary File System, is a peer-to-peer network protocol designed to make the web faster and safer. Files on IPFS are split into smaller chunks, hashed, and distributed across multiple nodes in the network. IPFS offers several advantages in decentralization and content-addressable storage that ensures data immutability and integrity. However, IPFS Storage does not provide any solution for data ownership or privacy concerns. So Solid-Pod, as a user-centered data storage solution, empowers individuals to have control over their own health information. It provides a secure personal online data store where patients can manage permissions and control access to their health data. The proposed research work Combining Solid-Pod with blockchain technology to create a framework for role-based access control (RBAC) and secure healthcare information exchange presents an innovative approach to addressing data security and privacy concerns in the healthcare sector.

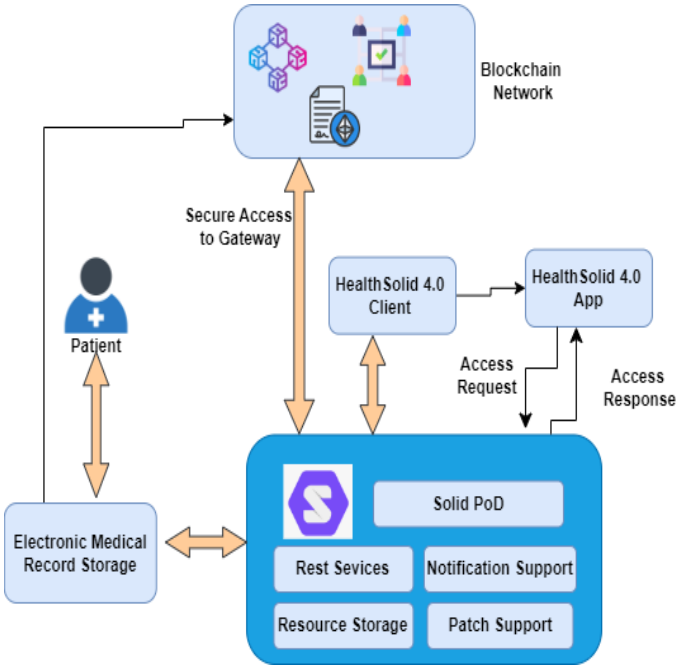

Figure 1. HealthSolid 4.0 Architecture

3.1. HealthSolid 4.0 System Architecture

In this study, we have termed Healthcare Users as “HealthSolid 4.0 clients”. We have enhanced the security of patient’s personal and medical information by integrating blockchain methodology with Solid-Pod to enable secure role-based access control and address healthcare data retrieval and storage related concerns. Figure 1 represents a blockchain and solid-pod enabled HealthSolid 4.0 Framework. As shown in Figure 1,

Healthcare users are connected to the HealthSolid 4.0 app to access their personal and medical information. The secure gateway server is responsible for providing access to remote health services and third-party API services to HealthSolid 4.0 clients. The secure gateway access uses a blockchain-based methodology to ensure secure healthcare information exchange between HealthSolid 4.0 client, gateway server, and EMR (Electronic Medical Record) storage. To overcome the issues of healthcare data retrieval and storage, the proposed HealthSolid 4.0 Framework has been integrated with Solid-pod technology.

3.2. Solid-pod Healthcare Data Storage

Pods are decentralized data stores that enable users to safely store their data according to the Solid standard. Pods are data-secured versions of private web servers. One may manage who can access data saved in their pod, including applications and users. In order for Solid to function, users must first create a personal pod, a safe location to store data such as contacts, documents, images, and more. This recorded data can be shared by users with other users, groups, or platforms. Solid's capacity to link data from many sources and build a decentralized network is one of its main features. This is made possible by the usage of linked data, which makes it possible to link and communicate various types of information between various sources. As a result, people enjoy better privacy and more control over their data on a more visible and open web. Solid-pod provides more control over personal data. It also allows users to not rely on internet services to save and access their personal and medical information to pods. Alternatively, they can handle and store data in a clear and safe manner. Furthermore, greater privacy and security over current standards result from that control. It would entail having the capacity to disseminate information while maintaining its security and making it harder for others to misuse it.

3.3. HealthSolid 4.0 role-wise client Registration

The proposed HealthSolid 4.0 Framework process flow consists of three processes: (i) HealthSolid 4.0 client registration to Gateway server (GateS) (ii) HealthSolid 4.0 Notification Support and Resource Storage (iii) Secure Access to HealthSolid 4.0 Client's Pod Directory.

3.3.1. HealthSolid 4.0 role-wise client Registration

As shown in Figure 1, the gateway server (GateS) assigns an individual pod to each HealthSolid 4.0 client. After the assignment of individual pods, the gateway server creates a separate personal, medical and temporary directory for each HealthSolid 4.0 client. The gateway server configures ACL (Access Control List) rules and assigns SolidWebID, HealthStaffID, and EMSID accordingly. Algorithm 1 describes the role-wise HealthSolid 4.0 client registration process.

Algorithm 1. HeathSolid 4.0 Role-wise Client Registration to Gateway Server
Step 1 Gateway Server(GateS) ←HealthSolid 4.0 Client
Step 2 Gateway Server(GateS), GID, pod→ HealthSolid 4.0 Client
Step 3 Gateway Server(GateS) creates client's personal, medical, and temporary directories in the pod

Step 4 Creation of personal and medical files in temporary directory for HealthSolid 4.0
For client in [SolidWebID, HealthStaffID, EMSID] do Gateway server(GateS) creates a separate file in temporary directory
Step 5 Selecting ACL rules for temporary directories
If HealthSolid 4.0 Client == SolidWebID then
Set ACL rule = append for temporary created HealthSolid client file(solid_client).
If HealthSolid 4.0 Client == HealthStaffID then
Set ACL rule = append for temporary created temporary created HealthSolid staff file (solid_staff).
If HealthSolid 4.0 Client == EMSID then
Set ACL rule = append for temporary created temporary created HealthSolid EMS system file(solid_EMS).

3.3.2. HealthSolid 4.0 role-based notification Support and resource

According to the configured ACL rules by the gateway server and the selected HealthSolid 4.0 client identification information, a gateway server will allows access to HealthSolid 4.0 Pod or deny the access to Pod services. If the selected ID is SolidWebID, ACL access is 'append', and selected file is solid_client then a gateway server will allow access to HealthSolid 4.0 Pod else it will deny the access if any of the HealthSolid 4.0 client authorization information is incorrect. Accordingly, the same process will be followed for all the HealthSollid 4.0 client roles. Algorithm 2 describes the step-wise process to access HealthSolid 4.0 Pod according to the selected client roles, and identity information.

Algorithm 2. HealthSolid 4.0 role-based notification support and resource Storage

Step 1 Gateway Server ←HealthSolid 4.0 Client Operation[SolidWebID, HealthStaffID, EMSID]
If HealthSolid 4.0Client == SolidWebID &&ACL rule == append && File == solid_client then Allow access to HealthSolid 4.0 Pod
Notify the HealthSolid 4.0 client and a Gateway server(GateS)
else
Deny access to HealthSolid 4.0 Pod
If HealthSolid 4.0 Client == HealthStaffID && ACL rule == append && File == solid_staff then Allow access to HealthSolid 4.0 Pod
Notify the HealthSolid 4.0 client and a Gateway server(GateS).
else
Deny access to HealthSolid 4.0 Pod
If HealthSolid 4.0 Client == EMSID && ACL rule == append && File == solid_EMS then Allow access to HealthSolid 4.0 Pod
Notify the HealthSolid 4.0 client and a Gateway server(GateS).
else Deny access to HealthSolid 4.0 Pod

3.3.3. Role-based Secure Access to HealthSolid 4.0 Pod and HeathSolid 4.0 Repository

According to the selected HealthSolid 4.0 client roles, configured ACL rules, a gateway server(GateS) will verify the HealthSolid 4.0 client authorisation, assign a security token and SecretSolidID to each HealthSolid 4.0 client. If HTTP_HealthSolid

4.0_Response_Code is 401 then a gateway server(GateS) authorizes the HeathSolid 4.0 client information and allow access to HeathSolid 4.0 Repository. Algorithm 3 describes the step-wise process of role-based secure access to HealthSolid 4.0 Pod and HeathSolid 4.0 Repository as per the selected client roles, and identity information.

Algorithm 3 Role-based Secure Access to HealthSolid 4.0 Pod and HeathSolid 4.0 Repository

Step 1 HeathSolid 4.0 Repository ← HealthSolid 4.0 Client[SolidWebID, HealthStaffID, EMSID]
Step 2 HeathSolid 4.0 Repository ←HealthSolid 4.0 Client Role-based Authorisation
If HTTP_HealthSolid 4.0_Response_Code == 401 &&HealthSolid 4.0 Client[SolidWebID, HealthStaffID, EMSID] then
HealthSolid 4.0 client is authorized to a Gateway Server(GateS)
HealthSolid 4.0_Provider ←HealthSolid 4.0 Client[SolidWebID, SecretSolidID]
HealthSolid 4.0_Provider ←HealthSolid 4.0_Authorisation_Code[SolidWebID, SecretSolidID]
If HealthSolid 4.0 Client_Authorisation == successful then Allow access to HealthSolid 4.0 Pod Notify the HealthSolid 4.0 client and a Gateway server(GateS)..
else Deny access to HealthSolid 4.0 Pod
Step3HealthSolid 4.0_Provider Token←HealthSolid 4.0_Authorisation_Code[SolidWebID, HealthSolid 4.0_Pod_Access_Token]
HealthSolid 4.0_Provider Token ←HealthSolid 4.0_Authorisation_Code[SolidWebID, SecretSolidID]
If HealthSolid 4.0 Client_Request_Access_File == successful&&HealthSolid client file[solid_client, solid_staff, solid_EMS] then
Allow access to HealthSolid 4.0 Pod and associated resources
HealthSolid 4.0_Provider grants/denies the access to the HealthSolid 4.0 Pod and verifies the HealthSolid 4.0_Provider Token according to ACL rules and HealthSolid 4.0 client roles.
Notify the HealthSolid 4.0 client and a Gateway server(GateS)..
else Deny access to HealthSolid 4.0 Pod

4. RESULTS AND DISCUSSIONS

The integration of the blockchain methodology and solid-pod into healthcare ecosystems and EMR systems brings about a paradigm shift in the way healthcare is managed. This section validates and evaluates the proposed HealthSolid 4.0 Framework to traditional medical practices, highlighting its advantages, drawbacks, and possible effects. The performance evaluation of the proposed HealthSolid 4.0 Framework is divided into two subsections, section 4.1 describes the performance evaluation of the proposed methodology, its organization and implementation settings. Section 4.2 discusses the system's performance by estimating the time required to upload files of various sizes to the HealthSolid 4.0 client's pod and comparing the available decentralization methods for data storage.

4.1. Experimental Setup and Implementation Settings

The proposed HealthSolid 4.0 Framework provides decentralized data storage using blockchain innovation and a stable environment. The presented HealthSolid 4.0 Framework is tested and made by the Dapps using the Ganache tool, which has ten

participants with 100 Ether apiece. Blockchain software experts use Vanilla JavaScript to create a simple user interface (UI) for the framework because it works well with Ethereum. As a back-end framework, we have applied Hub JS framework associated with Web3 programming interface. The working environment was Windows 10, RAM 64 GB, and Ethereum 2.0 software. The Web3 programming interface was designed using HTML 5.0, Hub JavaScript, and MD 5(Message Digest 5) encryption methodology. For the performance measurement of the proposed HealthSolid 4.0 Framework, we have used OPEX/CAPEX tools along with Solid-pod storage services. Furthermore, we have also analyzed the time required to authorize role-based HealthSolid 4.0 client information against Ethereum blockchain-based smart contracts.

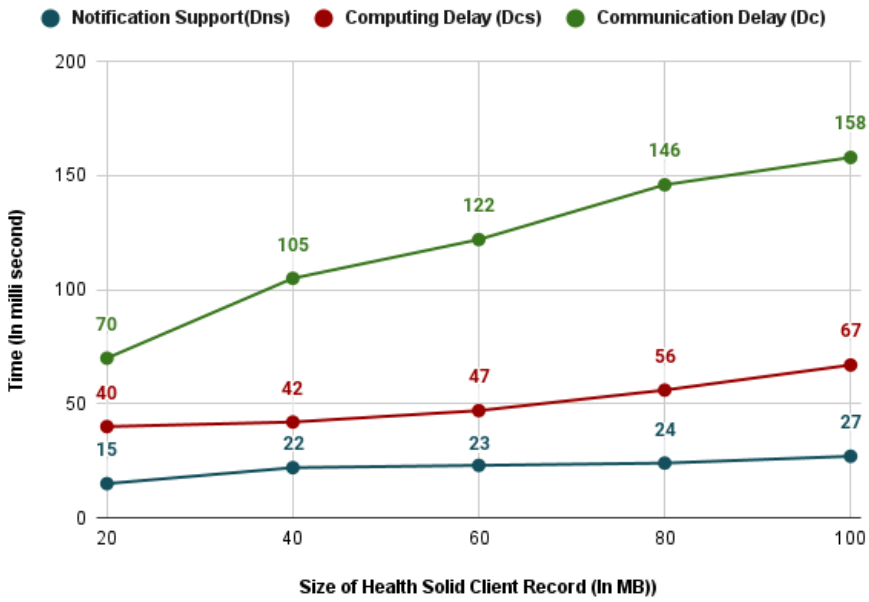

Figure 2. Representation of communication, computing, and notification support delays in maintaining HealthSolid 4.0 pod

Since Solid-Pod is an open-source distributed storage support, there is very little expense associated with implementing it within a healthcare provider's private network. Furthermore, we avoided purchasing a specialized infrastructure configuration for constructing a Gateway Server(GateS) by using already existing underutilized resources to provide distributed storage services for pods. The cost of communication between the HealthSolid 4.0 client's pod and the data source is now an issue. We have taken into account variables such as the size of the healthcare record that needs to be saved (Shrec), delay in the notification support(Dns), communication delay(Dc) and the computing delay(Dcs) have been considered. Each of these elements plays a part in determining how much it will cost to store the record at a GateWay(GateS) server. Furthermore, we have examined how much it costs to keep a record while processing more requests in a given amount of time. Different delays during the storage of resources of varying amounts onto the pod are depicted in Fig 2.

4.2. HealthSolid 4.0 Framework validation using Blockchain and Solid-pod

During the performance evaluation of HealthSolid 4.0 Framework using Blockchain, HealthSolid Client records were statistically stored on HealthSolid pod, solid_client, solid_staff, and solid_EMS files were uploaded to a gateway server (GateS). The estimated performance evaluation time depends on a variety of factors such as, no. of HealthSolid clients active on the Ethereum network, and the available bandwidth at the time of performance validation. The conducted experiments were satisfactory and validated the proposed HealthSolid 4.0 Framework efficiently. In conducted experiments, the uploading time of 15 seconds was considered for each HealthSolid 4.0 client file. Figure 3 represents the performance evaluation of the time required to upload a HealthSolid-Pod record into HealthSolid pod. As shown in Figure 3, the average time taken by the HealthSolid 4.0 client file size of 100 MB is approximately 230 seconds. During the process of time analysis, no delay in the notification support(Tns) time, communication time(Tc) and computing time(Tcs) have been observed.

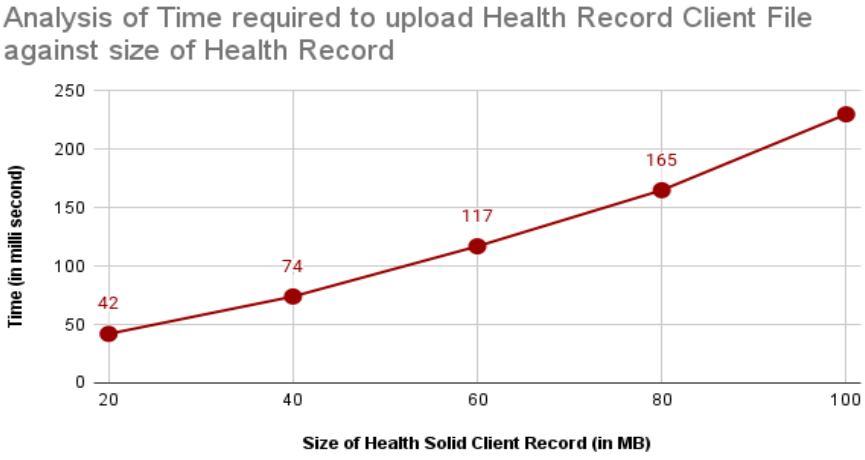

Figure 3. Upload Time Analysis of HealthSolid 4.0 client record against size of HealthSolid 4.0 client files

4.3. HealthSolid 4.0 Pod Computing and Uploading Cost Analysis

Along with the performance evaluation of the proposed HealthSolid 4.0 concerning variety of delays, no. of parallel requests against time, and size analysis of the HealthSolid 4.0 client files, it is essential to carry out cost analysis of Pod computing and uploading. Figure 4 represents the comparison analysis of HealthSolid 4.0 pod computing and uploading costs on the Ethereum network.

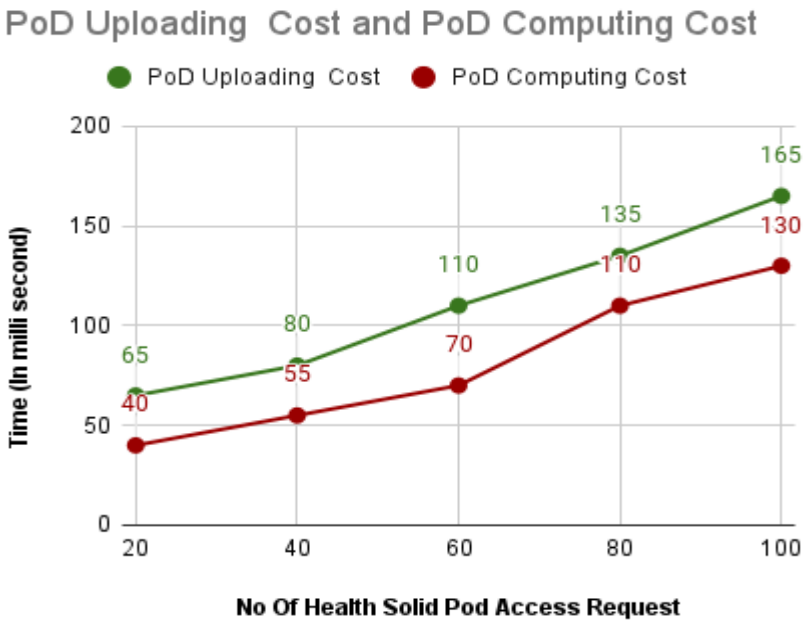

Figure 4. Comparison analysis representation of HealthSolid 4.0 pod computing and uploading cost

5. CONCLUSION

The healthcare ecosystem stakeholders often make the use of the patient's personal and medical information in making critical decisions, risk assessment, and future patient care. The role-based access control mechanism allows flexibility to healthcare ecosystem stakeholders to access stored personal and medical information in emergency situations with reliability. In this study, our emphasis has remained on integrating solid-pod with a blockchain-based methodology to design a reliable, efficient, and secure role-based access control mechanism to ensure smooth health information access, data retrieval and storage. Furthermore, in this study, we have proposed a complete blockchain and solid-pod enabled security framework termed "HealthSolid 4.0" to ensure secure Healthcare data access, retrieval and storage into HealthSolid pods. The presented HealthSolid 4.0 Framework has made a few contributions: (i) An integrated customized solid-pod and blockchain-enabled HealthSolid 4.0 Framework to secure healthcare data and address data retrieval and storage concerns, (ii) A smooth role-based HealthSolid 4.0 client file access mechanism to maintain smooth and secure healthcare information exchange in EMR(Electronic Medical Record) systems.

REFERENCES

[1] Rajput, A. R., Li, Q., Ahvanooey, M. T., Masood. I. EACMS: Emergency access control management system for personal health record based on blockchain. *IEEE Access*, vol.7, 2019, pp. 84304-84317. https://doi.org/10.1109/ACCESS.2019.2917976.

[2] Su, X., An, L., Cheng, Z., Weng, Y. Cloud–edge collaboration-based bi-level optimal scheduling for intelligent healthcare systems. *Future Generation Computer Systems,* vol.141, 2023, pp.28-39. https://doi.org/10.1016/j.future.2022.11.005.

[3] Rai, B. K. PcBEHR: patient-controlled blockchain enabled electronic health records for healthcare 4.0. *Health Services and Outcomes Research Methodology*, vol.23, no.1, 2023, pp.80-102. https://doi: 10.1007/s10742-022-00279-7.

[4] Abutaleb, R. A., Alqahtany, S. S., Syed, T. A. Integrity and Privacy-Aware, Patient-Centric Health Record Access Control Framework Using a Blockchain. *Applied Sciences*, vol. 13, no. 2, 2023. https://doi: 10.3390/app13021028.

[5] Sharma, P., Namasudra, S., Crespo, R. G., Parra-Fuente, J., Trivedi, M. C. EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. *Information Sciences*, vol. 629, 2023, pp.703-718. https://doi: 10.1016/j.ins.2023.01.148.

[6] Wazid, M., Gope, P. BACKM-EHA: A novel blockchain-enabled security solution for IoMT-based e-healthcare applications. *ACM Transactions on Internet Technology*, vol.23, no.3, 2023, pp.1-28. https://doi: 10.1145/3511898.

[7] Mittal, S., Ghosh, M. A novel two-level secure access control approach for blockchain platform in healthcare. *International Journal of Information Security*, vol. 22, no. 4, 2023. pp. 799–817. https://doi: 10.1007/s10207-023-00664-4.

[8] Fugkeaw, S., Wirz, L., Hak, L. Secure and lightweight blockchain-enabled access control for fog-assisted IoT cloud based electronic medical records sharing. *IEEE Access,* vol. 11, 2023, pp. 62998–63012. https://doi: 10.1109/ACCESS.2023.3288332.

[9] Ali, A., Al-Rimy, B. A. S., Alsubaei, F. S., Almazroi, A. A., Almazroi, A. A. HealthLock: blockchain-based privacy preservation using homomorphic encryption in Internet of Things healthcare applications. *Sensors*,vol. 23, no. 15, 2023. https://doi: 10.3390/s23156762

[10] Román-Martínez, I., Calvillo-Arbizu, J., Mayor-Gallego, V. J., Madinabeitia-Luque, G., Estepa-Alonso, A. J., Estepa-Alonso, R. M. Blockchain-based service-oriented architecture for consent management, access control, and auditing. *IEEE Access*, vol. 11, 2023,pp. 12726–12740, https://doi: 10.1109/ACCESS.2023.3242605

[11] Alsuqaih, H. N., Hamdan, W., Elmessiry, H., Abulkasim, H., An efficient privacy-preserving control mechanism based on blockchain for E-health applications. *Alexandria Engineering Journal*, vol. 73, 2023, pp. 159–172, https://doi: 10.1016/j.aej.2023.04.037.

[12] Sharma, P., Namasudra, S., Chilamkurti, N., Kim, B. G., Gonzalez Crespo, R. Blockchain-based privacy preservation for IoT-enabled healthcare system. *ACM Transactions on Sensor Networks*, vol. 19, no. 3, 2023, pp.1-17. https://doi: 10.1145/3577926.

[13] Baucas, M. J., Spachos, P., Plataniotis, K. N. Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare. *IEEE Transactions on Computational Social Systems*, vol. 10, no. 4, 2023, pp. 1732–1741, https://doi: 10.1109/TCSS.2023.3235950.

[14] Pawar, V., Sachdeva, S., ParallelChain: a scalable healthcare framework with low-energy consumption using blockchain. *International Transactions in Operational Research*, 2023. https://doi: 10.1111/itor.13278.

[15] Mokhamed, T., Talib, M. A., Moufti, M. A., Abbas, S., Khan, F. The potential of blockchain technology in dental healthcare: a literature review. *Sensors*, vol. 23, no. 6, 2023, https://doi: 10.3390/s23063277.

[16] Ali, S., Abdullah, Armand, T. P. T., Athar, A., Hussain, A., Ali, M., ... Kim, H. C., Metaverse in healthcare integrated with explainable ai and blockchain: enabling immersiveness, ensuring trust, and providing patient data security. *Sensors*, vol. 23, no. 2, 2023, https://doi: 10.3390/s23020565.

[17] Mallick, S. R., Lenka, R. K., Goswami, V., Sharma, S., Dalai, A. K., Das, H., Barik, R. K., BCGeo: Blockchain-assisted geospatial web service for smart healthcare system. *IEEE Access*, vol. 11, 2023,pp. 58610–58623, https://doi: 10.1109/ACCESS.2023.3283776.

[18] Maher, M., Khan, I., Prikshat, V. Monetisation of digital health data through a GDPR-compliant and blockchain enabled digital health data marketplace: A proposal to enhance patient's engagement with health data repositories. *International Journal of Information Management Data Insights*, vol. 3, no. 1, 2023, https://doi: 10.1016/j.jjimei.2023.100159.

[19] Gao, H., Huang, H., Xue, L., Xiao, F., Li, Q. Blockchain-enabled fine-grained searchable encryption with cloud-edge computing for electronic health records sharing. *IEEE Internet of Things Journal*, vol. 10, no. 20, 2023, pp. 18414–18425, https://doi: 10.1109/JIOT.2023.3279893.

[20] Gupta, A., Bhagat, M., Jain, V. Blockchain-enabled healthcare monitoring system for early Monkeypox detection, *The Journal of Supercomputing*, vol. 79, no. 14, 2023, pp. 15675–15699, https://doi: 10.1007/s11227-023-05288-y.

[21] Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., Akella,V.Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International journal of information management*, vol. 49, 2019,pp. 114–129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005

[22] Dadhania A, Patel H.e-DRBAC-HC: Extended Decentralized Role-Based Access Control for Healthcare System using Blockchain. *International Journal of Intelligent Systems and Applications in Engineering*, vol.12, no.3, 2023, pp.2046–2055. https://ijisae.org/index.php/IJISAE/article/view/5672

Information about the authors:

Avani Dadhania is a research Scholar in Kadi Sarva Vishwavidyalaya, Gandhinagar. She is working as Assistant Professor in the Department of Computer Engineering at LDRP Institute of Technology, Gandhinagar. She has more than 15 years of academic experience and her research areas include Blockchain Technology, Internet of Things, Network Security.

Hiren Patelis currently working as a Principal of Vidush Somany Institute of Technology and Research, Kadi, Gujarat. He completed his Ph.D. from National Institute of Technology (NIT), Surat with Cloud Computing as the domain of research. He has more than 20 years of teaching experience. His main areas of interest are Cloud computing, parallel Processing, Networking and Security and Blockchain Technology.

Manuscript received on 17 June 2024