Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 20 No. 15 (2024) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v20i15.51515

PAPER

Interoperability Blockchain, InterPlanetary File System and Health Level 7 Framework for Electronic Health Records

Estefano Bran[1], Adrian Alzamora[1], Bruno Castañeda-Carbajal[2], José Luis Castillo-Sequera[3], Lenis Wong[1](✉)

[1]Program Software Engineering, Universidad Peruana de Ciencias Aplicadas, Lima, Perú

[2]Program Medicine, Universidad Peruana de Ciencias Aplicadas, Lima, Perú

[3]Department of Computer Science, Universidad de Alcalá, Alcalá de Henares, Spain

pcsilewo@upc.edu.pe

ABSTRACT

Patient medical records and their accurate recording, storage, protection, and access are essential elements to high-quality healthcare. While many parts of the world have moved to traditional digital systems and electronic health records (EHRs), these systems require complex evaluation and large infrastructure investments, lack interoperability, and introduce the constantly-increasing challenges of cyber-attacks and digital security. The aim of this study is to address these challenges through a secure and accessible EHR management system, applied to allergy and family records, based on blockchain technology, the InterPlanetary File System (IPFS) protocol, and the health level 7 (HL7) fast healthcare interoperability resources standard. The proposal was carried out in four phases: (1) blockchain architecture design, (2) blockchain network design, (3) interoperability design, and (4) web application design. A performance evaluation of the system was conducted to determine the throughput and latency metrics. The results presented a maximum medical record reading and writing throughput of approximately eight transactions per second, with a write latency averaging 5,926 ms to 51,836 ms and a reading latency of 4,783 ms to 45,500 ms. With the addition of a survey of 21 patients and 10 healthcare professionals indicating that both groups strongly agree that the system meets the criteria of high-quality healthcare, all study results present a framework that could serve as a model for the adoption of standards-based, accessible, and secure EHR systems.

KEYWORDS

electronic health record (EHR), blockchain, interoperability, Hyperledger sawtooth, InterPlanetary File System (IPFS), health level 7 (HL7)

1 INTRODUCTION

While different regions of the world have moved to electronic health records (EHRs) stored in advanced digital systems, many regions still document patient

Bran, E., Alzamora, A., Castañeda-Carbajal, B., Castillo-Sequera, J.L., Wong, L. (2024). Interoperability Blockchain, InterPlanetary File System and Health Level 7 Framework for Electronic Health Records. *International Journal of Online and Biomedical Engineering (iJOE)*, 20(15), pp. 60–78. https://doi.org/10.3991/ijoe.v20i15.51515

Article submitted 2024-08-01. Revision uploaded 2024-09-13. Final acceptance 2024-09-15.

health information on paper, generating the subsequent challenges of legibility, accessibility, and storage that jeopardize the delivery of high-quality patient care [1]. These quality challenges were found by Rodriguez-Vera et al., where 15% of handwritten medical records had legibility issues that complicated auditing, research, and communication [2]. EHRs have emerged as a new method to address these challenges by helping to accurately collect and maintain medical information [3]. EHRs offer a range of benefits, including quick access to information, reduction of medical errors, improved patient privacy, data security, and cost reduction [4]. When designed using integration standards, they also offer the benefit of interoperability, where critical patient information can be shared and accessed by different digital systems, therefore expanding the geographical range of healthcare.

In Peru, data from the Ministry of Health (MINSA) show that in the capital and largest city, Lima, less than 40% of primary care facilities have adopted EHRs [5]. In more rural regions such as Cajamarca and Loreto, these levels do not exceed 4% and present clear risks to high-quality patient care 4% [5].

While EHRs provide many benefits, they bring the challenge of data security, as breaches and cyberattacks have compromised patient privacy and confidentiality. In the United States, for example, Alder documented 5,000 cases of breaches between 2009 and 2023 that exposed over 382 million medical records [6]. This is also the case in Peru, as a leak in the MINSA database, detected on the Deep Web, ultimately compromised more than 44,000 patient records [7].

To address these EHR security challenges as well as ensure and enhance EHR interoperability, various studies have proposed solutions based on blockchain, peer-to-peer, and other new standards-based technologies. Reference [8] proposed a framework for sharing health data that secures privacy by storing encrypted information in the InterPlanetary File System (IPFS), a peer-to-peer distributed file system. Similarly, a system for searching, verifying, and storing encrypted EHRs in IPFS and in the cloud is presented in [9]. Additionally, reference [10] proposed a solution that combines blockchain, IPFS, and the Health Level 7 fast healthcare interoperability resources (HL7 FHIR) standard to securely transfer EHRs between medical entities. Further, reference [11] introduces a blockchain-based cloud EHR system utilizing Ethereum blockchain, AWS S3 for storage, and a ReactJS-based user interface. In a different approach, reference [12] proposes a platform for sharing EHRs among healthcare organizations in resource-constrained environments, leveraging AWS services, and utilizing database replication mechanisms along with RESTful web service. However, these solutions have the disadvantage of requiring a lot of computing resources, which significantly reduces scalability and increases operational costs.

To address the limitations, this study proposes a novel framework to leverage the benefits of blockchain technology, the IPFS, and the HL7 FHIR standard to facilitate and accelerate the development of interoperable healthcare applications by providing a web-based programming interface that can be used to create tools for sending, receiving, and accessing electronic medical records based on previous HL7 data format standards, such as versions 3.x and 2.x. These standards are easy to implement because they use a web-based API technology stack and a RESTful protocol based on HTTP.

In this work, we present this approach by proposing a framework for interoperability in the management of electronic medical records, specifically applied to allergy and family records. This framework uses a medical record storage system based on the IPFS protocol, combined with access control and authentication mechanisms to ensure that only authorized personnel can retrieve and modify records, all in accordance with the HL7 FHIR standard. In doing so, this proposal facilitates the exchange of records, with the primary goal of enabling smoother interoperability between healthcare systems. This will allow third-party developers to create medical applications that easily integrate with existing systems while enabling healthcare providers to access real-time patient information from any device.

The framework was developed in four phases: (1) blockchain architecture design, (2) blockchain network design, (3) interoperability design, and (4) web application design. A security analysis of the proposal was conducted to assess its resilience against identity spoofing, brute-force attacks, and man-in-the-middle attacks. The system was also evaluated to determine its performance and latency with different users. The results showed a maximum read or write performance for medical records of approximately 8 TPS, similar to other approaches, without compromising the scalability or operational cost of the system.

This paper is organized as follows: In Section 2, a literature review is conducted on previous solutions for interoperable medical record management. Section 3 presents the architectural design of the decentralized web platform, security analysis, and validation testing of the solution. Section 4 presents the results and discussion. Finally, Section 5 summarizes the findings, conclusions, and future work.

2 RELATED WORKS

In the current literature, various studies have focused on interoperability standards between medical platforms, the use of technologies to improve medical records management solutions, and the key architectural decisions for implementing these platforms.

2.1 Interoperability standards

Regarding interoperability standards, two medical data modeling standards have been recognized: HL7 FHIR, Observational Medical Outcomes Partnership (OMOP), and common data model (CDM). HL7 FHIR is a resource-based standard that offers an adaptable and scalable data model, with widespread adoption and support in the healthcare industry [13]. However, its flexibility can at times lead to variations in data representation that impede semantic interoperability and data consistency between different sources [14]. OMOP CDM is designed for observational healthcare data, providing a standardized approach to organizing and querying clinical data, especially for research and analysis purposes [15]. Additionally, it is compatible with HL7 FHIR, allowing for the creation of a cohesive data ecosystem that covers both research-oriented and clinical use case scenarios [16]. However, integrating OMOP CDM with other data sources can require extensive mapping and transformation efforts, as well as comprehensive data normalization [17].

2.2 Technologies

Different technologies were identified and considered in order to balance the storage, consensus mechanism, encryption algorithms, and blockchain platform requirements. The storage technologies used were IPFS, Cloud, OrbitDB, and CouchDB. The consensus mechanisms used were proof of work (PoW), Practical Byzantine Fault Tolerance (PBFT), proof of stake (PoS), Proof of Authority (PoA), Byzantine Fault Tolerance (BFT), Node-state-checkable Practical Byzantine Fault Tolerance (sc-PBFT), Clique Proof of Authority, and raft. The encryption algorithms used were Rivest-Shamir-Adleman (RSA), advanced encryption standard (AES), elliptic curve cryptography (ECC), ciphertext-policy attribute-based encryption (CP-ABE), elliptic curve digital signature algorithm (ECDSA), and Proxy re-encryption. The blockchain platforms used were Hyperledger Fabric, Ethereum, and Cosmos.

2.3 Architectural decisions

The current literature presents five key architectural decisions as pivotal in the design of blockchain-based web platforms. One is the "encryption mechanism," which can be symmetric or asymmetric [18], [19]. The second is "access type," which defines which entities can join the network and provides appropriate authorization to professionals and patients and can provide public, private, or consortium-based access [18], [20], [21]. The selection of "storage type" considers the distribution and replication of records and can be on-chain or off-chain [9], [22]. "Consensus mechanism" plays an essential role in the efficient validation of records and is based on proof or voting [18], [23]. Finally, the choice of "blockchain platform" has implications for scalability and data access [19], [24].

3 MATERIALS AND METHODS

This section outlines the proposed framework that was designed following the four-phase process presented in Figure 1 [25]. In Phase 1, the blockchain architecture is designed using cloud service components. In Phase 2, the blockchain network is designed as well as the development setup, access control, consensus mechanism, and transaction processors are configured. In Phase 3, data modeling is performed for system interoperability. In the final Phase 4, the web platform that will support the functionalities is designed.

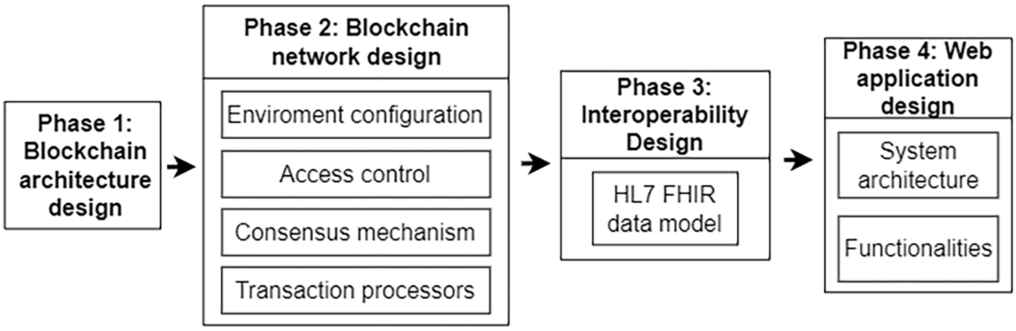
Phase 1: Blockchain architecture design
Phase 2: Blockchain network design
Enviroment configuration
Access control
Consensus mechanism
Transaction processors
Phase 3: Interoperability Design
HL7 FHIR data model
Phase 4: Web application design
System architecture
Functionalities

Fig. 1. Conceptualization of the proposed framework

3.1 Phase 1: Blockchain architecture design

The blockchain architecture consists of Azure and Infura services (see Figure 2). The Azure services included are:

Azure Active Directory B2C manages user and application authentication and authorization within the system, ensuring the privacy and security of medical data.
Application programming interface (API) management facilitates the exposure and management of APIs for healthcare system integration.
Azure Insights provides monitoring and analytics tools for system performance and health.
Azure App Service enables scalable and reliable deployment of web applications and application programming interfaces.
Azure Key Vault handles secure management of keys and secrets, ensuring the protection of sensitive data.
SQL Database is the relational database for storing non-medical data such as system notifications.
Azure Virtual Network secures a virtual private network for safe data traffic.
Azure Kubernetes Service facilitates container orchestration for scalability and flexibility in deploying medical services via a Hyperledger Sawtooth virtual network.

Hyperledger Sawtooth is pivotal in the architecture, integrating with the Azure Kubernetes Service to create and manage Hyperledger consortium blockchain networks in order to bring enhanced scalability and reliability [26]. The Azure virtual network reinforces the security and data protection within the Sawtooth network [27], ensuring the confidentiality and integrity of medical records and transactions.

The Infura services administer the IPFS protocol to provide a reliable and decentralized infrastructure for storing and sharing medical data and as an external IPFS node, ensuring the continuous availability of medical records without the need for proprietary infrastructure [28]. This guarantees access to the records and resistance to data corruption, facilitating patient data retrieval and secure distribution within the health platform, ultimately enhancing the integrity and accessibility of medical information [24].

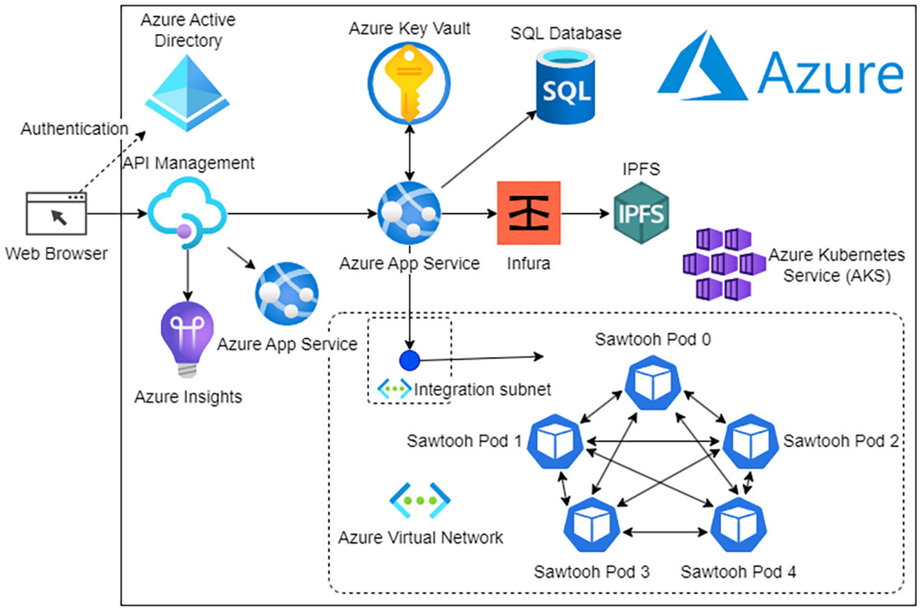

Fig. 2. Blockchain architecture

3.2 Phase 2: Blockchain network design

For the design of the blockchain network, the PBFT algorithm will serve as the consensus mechanism within the Hyperledger Sawtooth platform. Python 3 will be utilized for transaction processors. In Sawtooth, transaction processors function similarly to smart contracts in other blockchains, executing business logic when processing transactions on the network. JavaScript will be employed for the REST application programming interface.

Development setup: The blockchain network was developed using Visual Studio Code as the development environment, consisting of six transaction processors: "allergy processor," "consent processor," "family processor," "organization processor," "patient processor," and "practitioner processor." Each processor has four components: the "handler" manages transaction types, the "payload" represents transaction data, the "state" allows manipulation of network records, and the "main" initializes the processor. Additionally, a "rest-api" is included, serving as a client to interact with the blockchain network. Configuration files are also provided: "sawtooth-default.yaml" for local testing with Docker and "sawtooth-kubernetes-default.yaml" for production deployment with Kubernetes (see Figure 3).

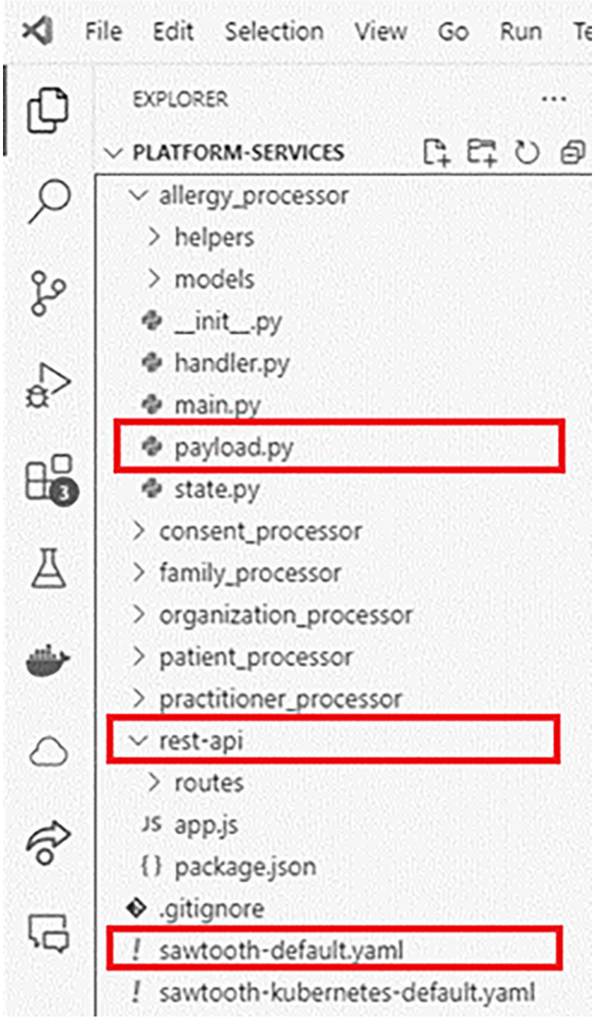

Fig. 3. Project structure in visual studio code

Access control: To manage access to information on the blockchain network, specific permissions are assigned to each user based on their role and following best practices [29], [30]. Patients have WRITE permissions that are limited to modifying their demographic information and READ permissions in order to access their medical records. Healthcare professionals have WRITE permissions in order to enter and update information in the records of patients they have access to, READ permissions to review the relevant medical records of patients under their care, and DELETE permissions to manage the deletion of specific information.

Figure 4 shows the request access sequence diagram, presenting access control measures implemented in the platform service to ensure that only authorized entities can access medical information.

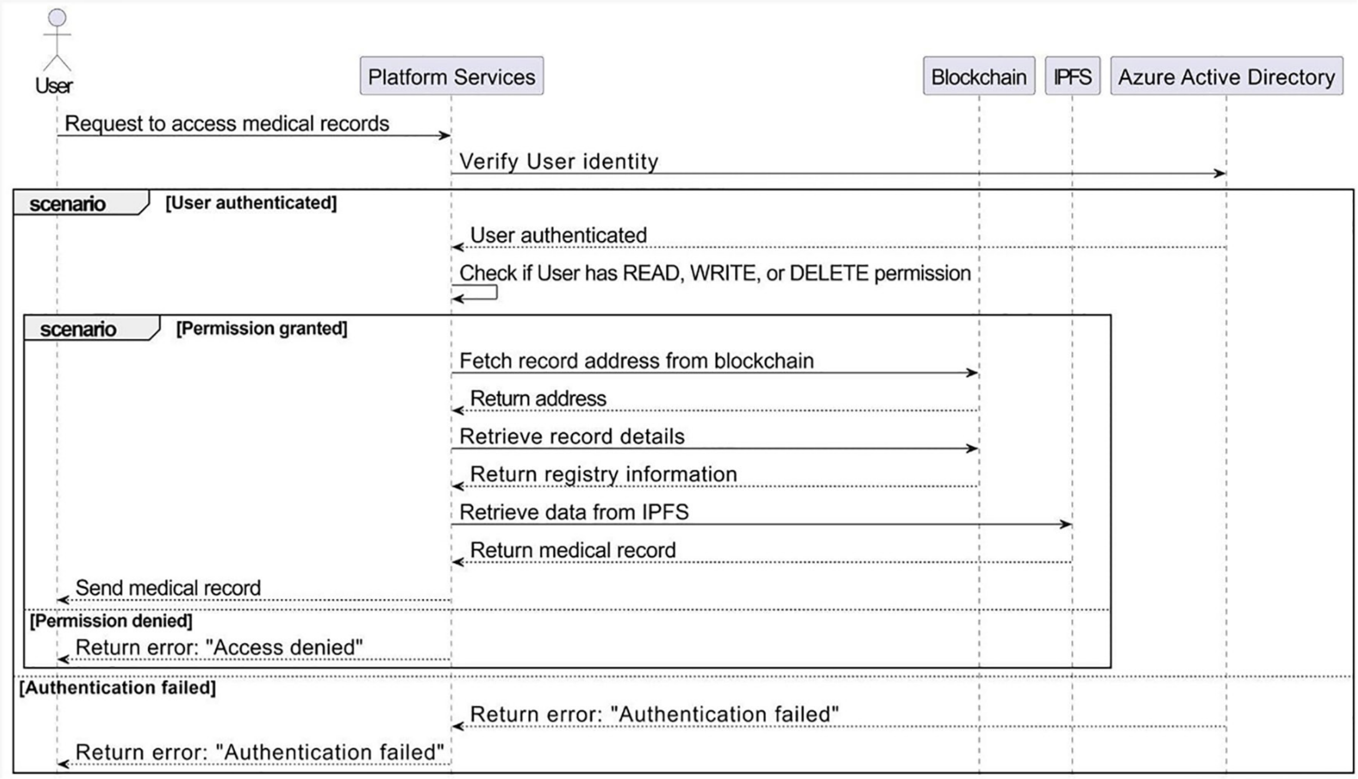

Fig. 4. Sequence diagram to request access to the platform services

The sequence begins by verifying whether the patient and/or healthcare professional has the appropriate permissions to perform the read operation. If the validation fails, an error object is returned, indicating a lack of authorization. If the validation is successful, the address on the blockchain associated with the provided identifier is determined. The registry information is retrieved from the blockchain and used to retrieve the data stored in IPFS. Finally, the retrieved information is returned as the result of the request access to medical records.

Consensus mechanism: The PBFT algorithm provides an efficient and secure consensus mechanism utilizing a set of nodes where “n” represents the maximum number of faulty nodes the system can safely handle (see Figure 5) [31]. To make decisions or approve transactions, PBFT requires the approval of at least two or three of the nodes, ensuring distributed consensus without the need for the complex mathematical calculations normally required in standard Proof of Work or Proof of Stake algorithms [23].

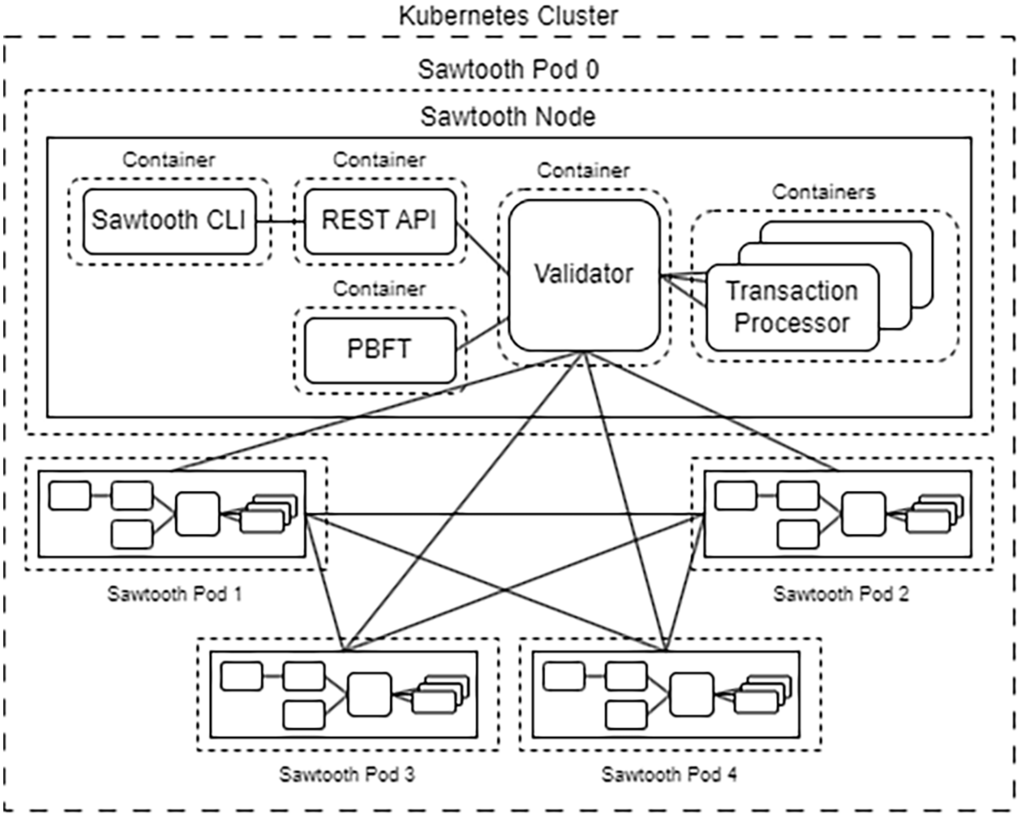

Fig. 5. Blockchain network architecture

Transaction processors: Figure 6 shows the "AllergyState" class that belongs to the allergy transaction processor. Within the "AllergyState" class, there are several methods that perform important functions in allergy record management.

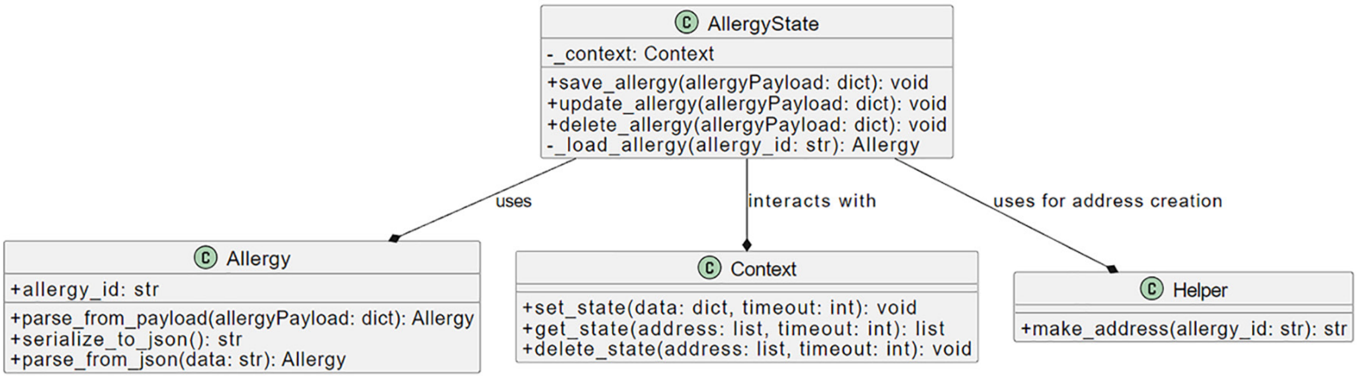
C AllergyState
-_context: Context
+save_allergy(allergyPayload: dict): void
+update_allergy(allergyPayload: dict): void
+delete_allergy(allergyPayload: dict): void
-_load_allergy(allergy_id: str): Allergy
uses
interacts with
uses for address creation
C Allergy
+allergy_id: str
+parse_from_payload(allergyPayload: dict): Allergy
+serialize_to_json(): str
+parse_from_json(data: str): Allergy
C Context
+set_state(data: dict, timeout: int): void
+get_state(address: list, timeout: int): list
+delete_state(address: list, timeout: int): void
C Helper
+make_address(allergy_id: str): str

Fig. 6. Allergy transaction processor class diagram

The "save_allergy" method is used to register new allergies in the system. An instance of the "Allergy" class is created, which is filled with the data provided in the "allergyPayload" object. If, after confirming that an allergy record does not already exist in the blockchain, a new address is generated, the data is encoded in JSON format, and the new record is stored in the system context. The "update_allergy" method is responsible for updating the information related to previously generated allergies. It checks if the record to be updated already exists, and if so, it obtains the address of the record and stores the updated data in the system context. The "delete_allergy" method allows deleting an allergy record, and like the previous methods, it first checks if the record is registered in the network, and if so, proceeds to remove it from the context. Finally, a private method called "load_allergy" is included, whose function is to retrieve information about an allergy record. This method creates an address from the record ID, obtains the state data associated with that address, and decodes it to generate an instance of the record, or returns *none* if the record is not found.

3.3 Phase 3: Interoperability design

Data model: Based on the HL7 FHIR standard, the proposed framework selects five resources: organization, patient, practitioner, allergy intolerance, and family member history. Figure 7 illustrates the entity relationship model among these resources.

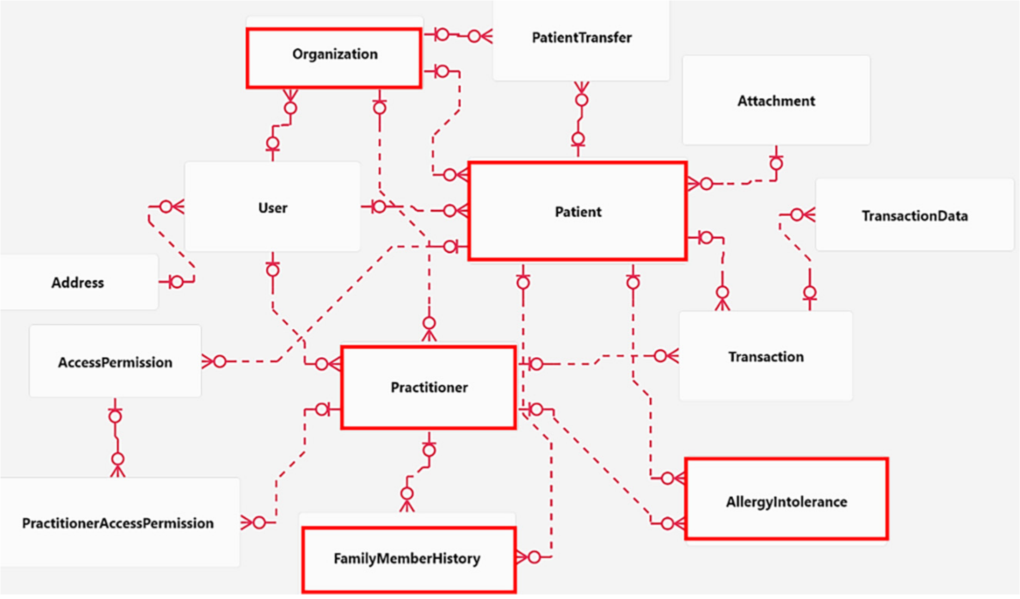

Fig. 7. Entity-relationship diagram

Organization: Organizations can be classified as hospitals, clinics, laboratories, or pharmacies. They have the authority to create and delete credentials for patients and practitioners. Additionally, they license healthcare professionals to operate within the system.

Patient: The patient is registered by an organization to access medical care. The registration includes details such as name, gender, date of birth, address, and other relevant information.

Practitioner: Practitioners must follow regional certification standards; in this case, the system conforms to the Medical College of Peru standards and their corresponding registration information. They can modify EHRs with prior consent from the patient [32].

Allergy Intolerance: This resource links patient data with information about their allergies, recording details such as clinical status, verification status, type of allergy, allergy category, and criticality level.

Family Member History: This resource includes relevant medical details about the patient's family members, such as health conditions, demographic data, reasons for the absence of certain information, and other pertinent information.

3.4 Phase 4: Web application design

Figure 8 illustrates the web architecture of the proposed framework. The "presentation layer" represents the graphical interface through which users interact with the system and is deployed on an Azure App Service. The section "application layer" presents the logic for managing medical records, mapping data according to the HL7 FHIR standard, and interacting with IPFS. The section "data layer" contains two components: an Azure SQL Server 2022 relational database for storing non-medical information and IPFS for the decentralized storage of medical records and other patient data. Finally, the section "blockchain layer" ensures the immutability, traceability, and security of medical records. In this layer, transactions related to records management are recorded in a secure and decentralized manner. This layer is developed using the Hyperledger Sawtooth platform and deployed on Azure Kubernetes Services.

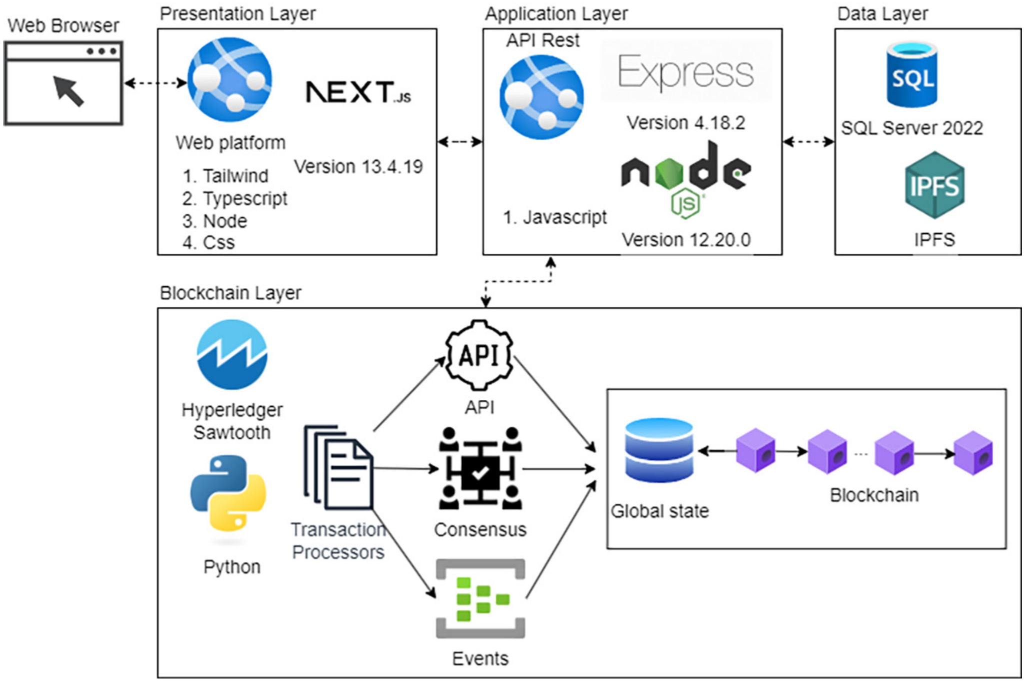

Fig. 8. Architecture diagram

3.5 Data security measures

The following security measures are implemented to prevent phishing, brute force, and man-in-the-middle attacks.

Spoofing attack: To mitigate spoofing risks, the platform uses API authentication with short-lived JWT (JSON Web Tokens) and Azure Access Directory for user authentication. In addition, role-based access control (RBAC) ensures that only authorized users can access sensitive medical information.

Brute force: Several protocols are used to ensure the confidentiality of the data. Along with the standard username and password access, password policies require 1 special character, 1 capital letter, 1 number, and a minimum length of 8 characters in order to increase the complexity of passwords, making them more difficult for attackers to determine through brute force attacks. The number of login attempts is also limited to three. This measure stops automated password guessing attempts after a small number of failed attempts, temporarily locking the affected account.

Man-in-the-middle: The use of HTTPS ensures that all communications between clients and servers are encrypted, preventing interception and manipulation of data by attackers during transmission. In addition, transactions to the blockchain are encrypted using the AES-256 encryption algorithm and signed by a user generated private key [33]. This validates the transaction with a confirmed signature associated with the address of the issuing user, thus complicating forgery attacks.

3.6 Validation

An evaluation of the system's performance in different scenarios was carried out to determine the throughput and latency for different numbers of users. In addition, a survey was conducted with the participation of twenty-one patients and ten health professionals who work in different medical entities across the city of Lima, with the aim of surveying their perception of the quality of the proposed framework based on the ISO/IEC 25000 standard that guides the evaluation of software quality, usability, interoperability, security, and adaptability [34].

System performance evaluation. *Dataset:* A dataset of 1,000 synthetic patient records in HL7 FHIR format generated by the open-source health data generator Synthea was loaded into the system [35].

Environment configuration: The experiment was conducted using the following hardware specifications for the client computer: Intel(R) Core (TM) i5-8300H 2.30 GHz processor, 24.0 GB RAM, 1600 MHz DDR4, and 1 TB SSD. The transaction processors were developed in Python 3 using Sawtooth SDK version 1.2.5. The REST API implemented for communication with the blockchain network uses Node.js 12.20.0 and version 1.0.5 of the Sawtooth SDK. The consortium-type blockchain network, composed of five nodes, used the PBFT consensus algorithm and was deployed in a Kubernetes cluster on the client computer. The performance evaluation of the system was carried out using Apache JMeter v5.6.3, with the experimental parameters detailed in Table 1 [36].

Table 1. Experimental parameters

Parameter	Description	Value
Number of threads (users)	The number of concurrent user requests (transactions)	50, 100, 150, 200, 250, 300, 350, 400, 450, 500
Ramp-up period (seconds)	The time it takes for adding all user threads	1
Loop count	The number of times to repeat the test	1
Same user on each iteration	Whether to use the same user(s) for each iteration	Yes

Performance metrics: The selected performance indicators, derived from the research of Zaabar et al. and Hashim et al. are: 'Latency', the response time per request made in the system, expressed in milliseconds (ms), and 'Throughput', the number of transactions that can be processed by the system per second, expressed in transactions per second (TPS) [22], [31].

Validation of expert judgement. Additionally, a validation of the study was carried out with expert judgement consisting of twenty-one patients and ten health professionals evaluating the (i) training methods, (ii) system interaction, and (iii) survey development.

Training: This was carried out virtually. The objective of the system was presented and a demonstration of the main functionalities of the system was performed. This stage lasted 15 minutes for each participant.

Interaction with the system: The experts were given access to the system to interact with it for a period of ten minutes. During this phase, they carried out various actions, such as logging in, accessing existing allergy and family history records, adding new medical records, and managing access permissions to these records.

Survey development: Two online surveys were developed, one for patients (refer to Table 2) and one for health professionals (refer to Table 3) using the Likert scale (1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree).

Table 2. Patient survey questions

Category	Question	
Usability	QPA1	Does the web platform facilitate access to your electronic health record?
	QPA2	Can you easily share your medical records with other health professionals when needed?
	QPA3	Does the platform allow you to control who can access your medical records?
Security	QPA4	Do you feel that your information is protected on this platform?
Adaptability	QPA5	Would you recommend this platform to other patients for managing their medical records?
	QPA6	Overall, are you satisfied with your experience using this electronic health record management platform?

Table 3. Health professionals survey questions

Category	Question	
Usability	QPR1	Can you easily access your patients' medical records?
	QPR2	Does the platform allow you to add new medical records easily?
	QPR3	Is it easy to request access to a patient's medical record?
Interoperability	QPR4	Do you consider that the platform adequately implements the HL7 FHIR standard?
Security	QPR5	Do you consider that the information is protected on this platform?
Adaptability	QPR6	Would you recommend this platform to your colleagues?
	QPR7	Overall, are you satisfied with your experience using this electronic health record management platform?

4 RESULTS AND DISCUSSION

In Table 4, we compare our proposal with the reviewed studies, focusing on five key aspects: access control, data encryption, interoperability, decentralized storage, and scalability. The comparison demonstrates that all the reviewed studies, including our own, implement access control and data encryption to ensure the security of medical information. However, our solution is distinguished by its use of the HL7 FHIR standard, which is not employed by studies [8], [9], and [12]. In terms of storage, while [11] and [12] rely on centralized solutions such as AWS S3, our proposal uses IPFS, offering greater decentralization. Finally, in terms of scalability, our Hyperledger Sawtooth-based solution outperforms the solutions in [9] and [10], which use Ethereum, by avoiding its cost and speed limitations.

Table 4. Comparison between the proposed and related solutions

Ref	Access Control	Data Encryption	Interoperability	Decentralized Storage	Scalability
[8]	Y	Y	N	Y	Y
[9]	Y	Y	N	Y	N
[10]	Y	Y	Y	Y	N
[11]	Y	Y	Y	N	Y
[12]	Y	Y	N	N	Y
Proposed	Y	Y	Y	Y	Y

The performance metrics are based on the TPS required to write and read both family and allergy records, as shown in Figure 9. The family record and allergy writing performances reached peak values of 8.22166 TPS at 200 transactions and 8.06257 TPS at 300 transactions, respectively (see Figure 9a). The family record and allergy reading performances reached peak values of 8.09061 TPS at 150 transactions and 7.86535 TPS at 50 transactions, respectively (see Figure 9b). Overall, the lowest TPS across this proposed framework's performance metrics was well above the 3.3750 TPS reported by Mauricio et al. [10].

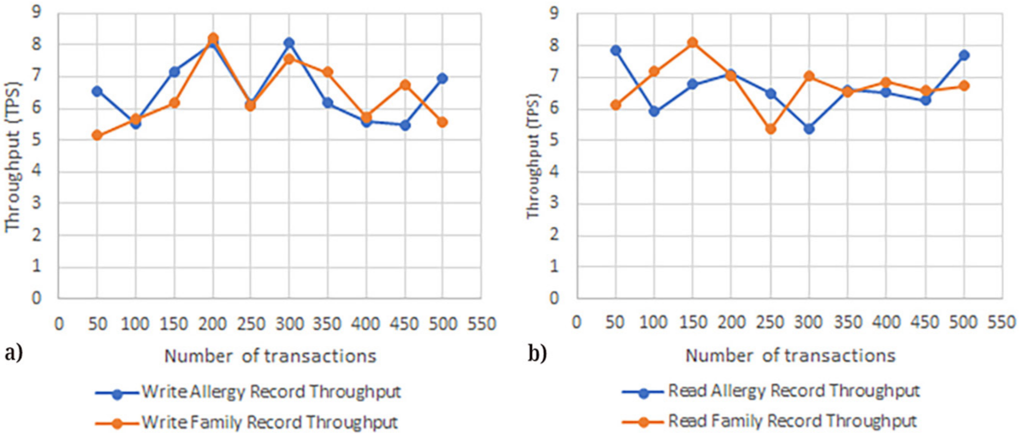

Fig. 9. Transaction throughput of the proposed framework

Figure 10 shows the minimum, maximum, and average latency in milliseconds for family and allergy record write transactions. An average latency range was obtained between 5,926 ms to 47,345 ms for allergy record writing transactions (see Figure 10a) and between 7,856 ms to 51,836 ms for family record writing transactions (see Figure 10b). The proposed framework requires 29,932 ms to perform 300 transactions, significantly reducing the 50 s latency that was found for the same number of transactions reported by Majdoubi et al. [8].

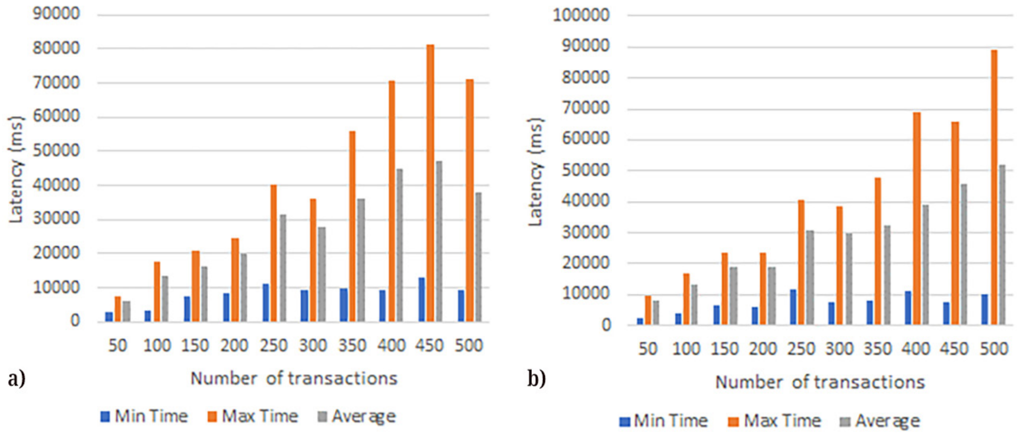

Fig. 10. The transaction latency of the proposed framework

Figure 11 shows the minimum, maximum, and average latency in milliseconds for family and allergy record read transactions. An average latency range was obtained between 4,783 ms to 44,674 ms for allergy record reading transactions (see Figure 11a) and from 6,723 ms to 45,500 ms for family record reading transactions (see Figure 11b).

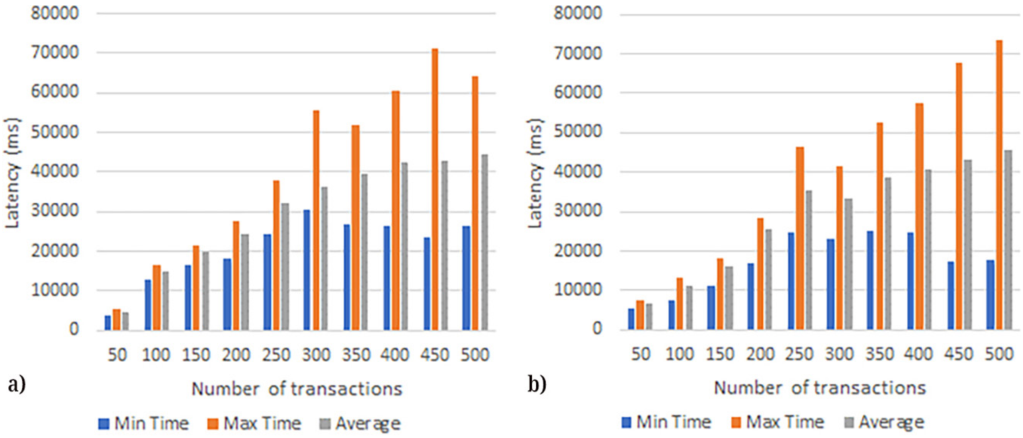

Fig. 11. Transaction latency of the proposed framework

Overall, the data show that as the number of transactions increases, latency also tends to increase for both writing and reading allergies as well as family records. Additionally, write latency tends to be higher than read latency for both types of records. These results demonstrate that the proposed system provides substantial improvements over previous studies, efficiently handling a significant number of transactions for both writing and reading family and allergy records. Thus, the framework achieves higher throughput and lower latency compared to previous solutions.

Figure 12 shows the results of the patient survey. More than 81% of the patients "strongly agree" that the platform meets the criteria of "usability" (QPA1, QPA2, and QPA3) and "adaptability" (QPA5 and QPA6). Additionally, 76% of patients believe that information is protected on the platform and "strongly agree" that it meets the "security" criterion (QPA4).

Figure 13 shows the results of the health professional survey. It shows that more than 60% of respondents “strongly agree” that the platform meets the “usability” criterion (QPR1, QPR2, and QPR3). Additionally, 70% “strongly agree” that the platform meets the “interoperability” criterion by properly implementing the HL7 FHIR standard (QPR4). Furthermore, 60% of health professionals believe that the platform adequately protects information and “strongly agree” that it meets the “security” criterion (QPR5). Finally, 60% state that they would recommend the platform to their colleagues (QPR6), and 80% are delighted with their experience (QPR7); that is, they “strongly agree” that the platform meets the “adaptability” criterion.

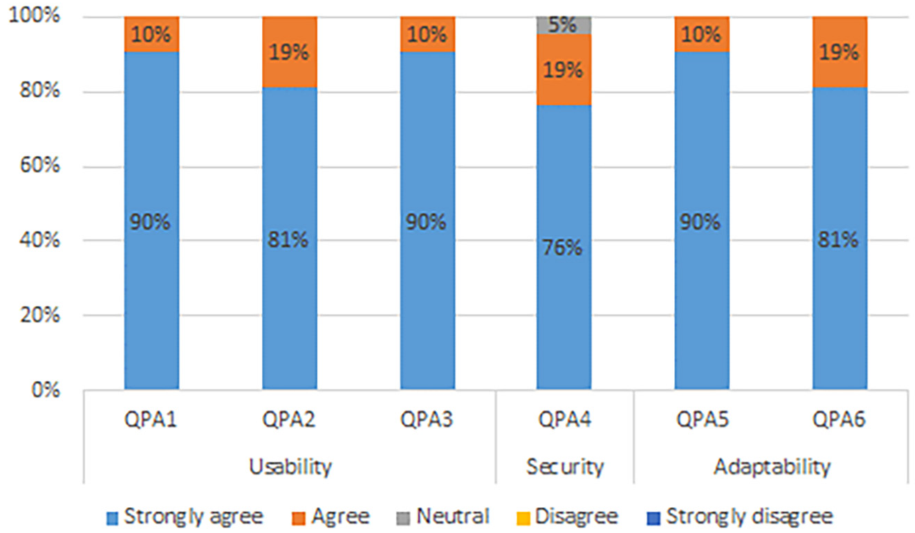

Fig. 12. Summary of responses to the patient survey

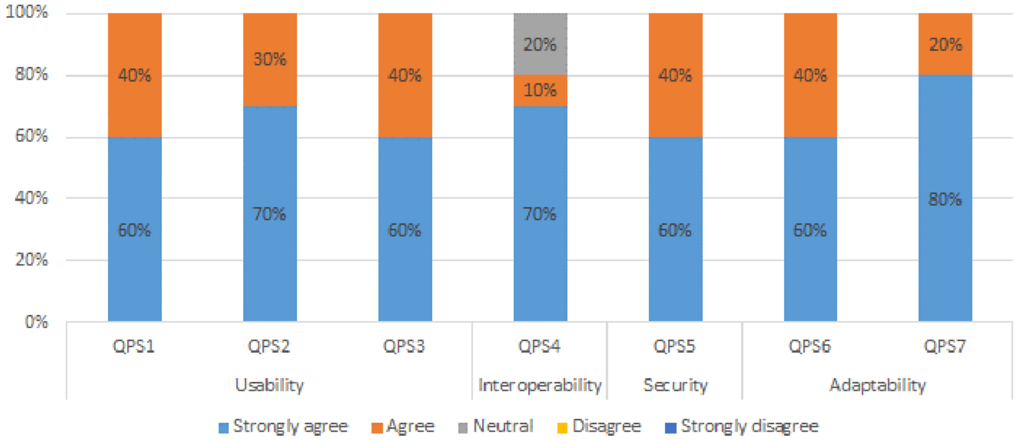

Fig. 13. Summary of responses to the health professional survey

5 CONCLUSIONS

In this study, a framework for interoperability in EHRs management based on blockchain, IPFS, and HL7 FHIR was presented. The proposal was carried out in four phases: (1) blockchain architecture design, (2) blockchain network design, (3) interoperability design, and (4) web application design. An analysis of the system’s security against spoofing, brute force, and man-in-the-middle attacks was conducted, followed by an evaluation to determine the throughput and latency for different numbers of users. In addition, a survey was performed with the participation of 21 patients and 10 health professionals involved in different medical entities in Lima. The result demonstrates improved performance over previous studies. These results indicate that the system can efficiently handle a substantial number of transactions for both writing and reading family and allergy records.

Furthermore, a survey showed that patients and healthcare professionals felt that the proposal meets the quality criteria of *usability, interoperability, security,* and *adaptability*. In future work, the introduction of a mechanism for authorizing access to the patient's medical information through an electronic identity document could increase security.

6 ACKNOWLEDGMENT

The authors express their sincerest gratitude to the medical professionals and patients who participated in the surveys. Furthermore, they extend their appreciation to the Research Department of the Universidad Peruana de Ciencias Aplicadas for their support through the UPC-Expost-2024-1 incentive.

7 REFERENCES

[1] PostDICOM, "Pros and Cons of Electronic Health Records [Health Professional's Perspective]," 2024. [Online]. Available: https://www.postdicom.com/es/blog/pros-and-cons-of-electronic-health-records

[2] F. J. Rodriguez-Vera, Y. Marin, A. Sanchez, C. Borrachero, and E. Pujol, "Illegible handwriting in medical records," *Journal of the Royal Society of Medicine*, vol. 95, no. 11, pp. 545–546, 2002. https://doi.org/10.1177/014107680209501105

[3] American Medical Association, "Electronic Health Records," 2024. [Online]. Available: https://www.ama-assn.org/topics/electronic-health-records-ehr#:~:text=An%20electronic%20health%20record%20(EHR,view%20of%20the%20patient's%20care

[4] HealthIT, "What are the advantages of electronic health records?" 2022. [Online]. Available: https://www.healthit.gov/faq/what-are-advantages-electronic-health-records

[5] Ministerio de Salud, "Repositorio Único Nacional de Información en Salud," 2024. [Online]. Available: https://www.minsa.gob.pe/reunis

[6] HIPAA Journal, "Healthcare Data Breach Statistics," https://www.hipaajournal.com/healthcare-data-breach-statistics/

[7] Presidencia del Consejo de Ministros, *Alerta integrada de seguridad digital N° 221-2022-CNSD*, Lima, 2022. https://www.gob.pe/institucion/pcm/informes-publicaciones/3341770-alerta-integrada-de-seguridad-digital-n-221-2022-cnsd

[8] D. El Majdoubi, H. El Bakkali, and S. Sadki, "SmartMedChain: A blockchain-based privacy-preserving smart healthcare framework," *J. Healthc. Eng.*, vol. 2021, no. 1, pp. 1–19, 2021. https://doi.org/10.1155/2021/4145512

[9] N. Alrebdi, A. Alabdulatif, C. Iwendi, and Z. Lian, "SVBE: searchable and verifiable blockchain-based electronic medical records system," *Sci. Rep.*, vol. 12, 2022. https://doi.org/10.1038/s41598-021-04124-8

[10] D. Mauricio *et al.*, "Electronic health record interoperability system in Peru using blockchain," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 20, no. 3, pp. 136–153, 2024. https://doi.org/10.3991/ijoe.v20i03.44507

[11] A. D. Samala and S. Rawas, "Transforming healthcare data management: A blockchain-based cloud EHR system for enhanced security and interoperability," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 20, no. 2, pp. 46–60, 2024. https://doi.org/10.3991/ijoe.v20i02.45693

[12] M. F. Kacamarga, A. Budiarto, and B. Pardamean, "A platform for electronic health record sharing in environments with scarce resource using cloud computing," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 16, no. 9, pp. 63–76, 2020. https://doi.org/10.3991/ijoe.v16i09.13187

[13] F. A. Reegu *et al.*, "Blockchain-based framework for interoperable electronic health records for an improved healthcare system," *Sustainability,* vol. 15, no. 8, p. 6337, 2023. https://doi.org/10.3390/su15086337

[14] Y. S. Bae *et al.*, "Development of blockchain-based health information exchange platform using HL7 FHIR standards: Usability test," *IEEE Access*, vol. 10, pp. 79264–79271, 2022. https://doi.org/10.1109/ACCESS.2022.3194159

[15] S. Kohler *et al.*, "Eos and OMOCL: Towards a seamless integration of openEHR records into the OMOP common data model," *J. Biomed. Inform.*, vol. 144, p. 104437, 2023. https://doi.org/10.1016/j.jbi.2023.104437

[16] S. Purohit, P. Calyam, M. L. Alarcon, N. R. Bhamidipati, A. Mosa, and K. Salah, "HonestChain: Consortium blockchain for protected data sharing in health information systems," *Peer-to-Peer Netw. Appl.*, vol. 14, pp. 3012–3028, 2021. https://doi.org/10.1007/s12083-021-01153-y

[17] A. Rossander and D. Karlsson, "Structure of health information with different information models: Evaluation study with competency questions," *JMIR Med. Inform.*, vol. 11, p. e46477, 2023. https://doi.org/10.2196/46477

[18] K. Azbeg, O. Ouchetto, and S. Jai Andaloussi, "BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security," *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 329–343, 2022. https://doi.org/10.1016/j.eij.2022.02.004

[19] A. G. de Moraes Rossetto, C. Sega, and V. R. Q. Leithardt, "An architecture for managing data privacy in healthcare with blockchain," *Sensors*, vol. 22, no. 21, p. 8292, 2022. https://doi.org/10.3390/s22218292

[20] P. Pawar, N. Parolia, S. Shinde, T. O. Edoh, and M. Singh, "eHealthChain—a blockchain-based personal health information management system," *Annals of Telecommunications*, vol. 77, pp. 33–45, 2022. https://doi.org/10.1007/s12243-021-00868-6

[21] E. S. Babu, B. V. R. N. Yadav, A. K. Nikhath, S. R. Nayak, and W. Alnumay, "MediBlocks: Secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns," *Cluster Computing*, vol. 26, pp. 2217–2244, 2022. https://doi.org/10.1007/s10586-022-03652-w

[22] F. Hashim, K. Shuaib, and F. Sallabi, "Connected blockchain federations for sharing electronic health records," *Cryptography*, vol. 6, no. 3, p. 47, 2022. https://doi.org/10.3390/cryptography6030047

[23] Z. Pang, Y. Yao, Q. Li, X. Zhang, and J. Zhang, "Electronic health records sharing model based on blockchain with checkable state PBFT consensus algorithm," *IEEE Access*, vol. 10, pp. 87803–87815, 2022. https://doi.org/10.1109/ACCESS.2022.3186682

[24] V. Mani, P. Manickam, Y. Alotaibi, S. Alghamdi, and O. I. Khalaf, "Hyperledger healthchain: Patient-centric IPFS-based storage of health records," *Electronics*, vol. 10, no. 23, p. 3003, 2021. https://doi.org/10.3390/electronics10233003

[25] A. Garcia, J. Davila, and L. Wong, "Framework to improve the traceability of the coffee production chain in perú by applying a blockchain architecture," in *2022 32nd Conference of Open Innovations Association (FRUCT)*, 2022, pp. 93–101. https://doi.org/10.23919/FRUCT56874.2022.9953846

[26] Microsoft, "Cloud Computing Services | Microsoft Azure," 2024. [Online]. Available: https://azure.microsoft.com/es-es/products/cloud-services

[27] Asudbring *et al.*, "What is Azure Virtual Network?" Microsoft Ignite, 2024. https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

[28] INFURA INC, "Scalable and distributed storage infrastructure for your application." https://www.infura.io/product/ipfs

[29] Sawtooth, "Permissioning Design," 2018. https://sawtooth.splinter.dev/docs/1.2/architecture/permissioning_requirement.html

[30] Rolyon *et al.*, "Best practices for Azure RBAC," Microsoft Ignite, 2024. https://learn.microsoft.com/en-us/azure/role-based-access-control/best-practices

[31] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system," *Computer Networks*, vol. 200, p. 108500, 2021. https://doi.org/10.1016/j.comnet.2021.108500

[32] Ministerio de Salud, "Norma Técnica de Salud para la Gestión de la Historia Clínica," N° 139-MINSA/2018/DGAIN, 2019.

[33] D. Ramesh, R. Mishra, P. K. Atrey, D. R. Edla, S. Misra, and L. Qi, "Blockchain based efficient tamper-proof EHR storage for decentralized cloud-assisted storage," *Alexandria Engineering Journal*, vol. 68, pp. 205–226, 2023. https://doi.org/10.1016/j.aej.2023.01.012

[34] P. Roa, C. Morales, and P. Gutiérrez, "Norma ISO/IEC 25000," *Universidad Distrital Francisco Jose De Caldas*, vol. 3, no. 2, 2015.

[35] J. Walonoski *et al.*, "Synthea: An approach, method, and software mechanism for generating synthetic patients and the synthetic electronic health care record," *Journal of the American Medical Informatics Association*, vol. 25, no. 3, pp. 230–238, 2018. https://doi.org/10.1093/jamia/ocx079

[36] "Apache Software Foundation," *Apache JMeter – Apache JMeter*™. https://jmeter.apache.org/

8 AUTHORS

Estefano Bran graduated from the Software Engineering program at the Universidad Peruana de Ciencias Aplicadas in Lima, Peru. He currently works as a full-stack developer in a company specializing in the implementation of electronic commerce stores in different countries in Latin America, the United States, and Europe (E-mail: U201920151@upc.edu.pe).

Adrian Alzamora graduated from the Software Engineering program at the Universidad Peruana de Ciencias Aplicadas in Lima, Peru. Currently, he works on several projects in the Macroeconomic Database Department at the Central Reserve Bank of Peru, where he applies his expertise in data engineering and process automation (E-mail: U202015385@upc.edu.pe).

Bruno Castañeda-Carbajal graduated with a medical degree from Universidad Peruana de Ciencias Aplicadas, he has further distinguished himself by earning a certification as a Medical Auditor from the same institution. He has studies related to Clinical Management, Patient Safety, and Health Investment Projects. He has extensive experience in managing telehealth projects at the national level and currently serves as a Contracting Manager, a major insurance company in Peru (E-mail: U813568@upc.edu.pe).

José Luis Castillo-Sequera received the degree in computing from the Universidad Nacional Mayor de San Marcos, Peru, the master's degree in computer project management and the master's degree in university teaching in Spain, and the Ph.D. degree in information systems, documentation, and knowledge from the Universidad de Alcalá, Spain. He is currently a Full Professor with the Department of Computer Science, Universidad de Alcalá. He has multiple publications at the level of

high-level indexed JCR journals and is the author of books and book chapters related to the field of artificial intelligence (E-mail: jluis.castillo@uah.es).

Lenis Wong is a Professor and researcher of Software Engineering and Information Systems Engineering at the Universidad Nacional Mayor de San Marcos and Universidad Peruana de Ciencias Aplicadas, Peru. She holds a PhD in Systems Engineering and Computer Science. MSc. in Systems and Computer Engineering with mention in Software Engineering. She is a member of the AI research group and has carried out different multidisciplinary projects where Artificial Intelligence, Software Engineering and Information Systems Engineering have been applied in education, health, medicine and healthcare. She has published several international peer-reviewed scientific articles in different multidisciplinary areas such as: ML, DL, IoT, e-Health, Software Engineering, Requirements Engineering, Cloud Computing, E-Learning, Gamification, Cyberattacks, Natural Language Processing, Networks and Blockchain Technologies (E-mail: pcsilewo@upc.edu.pe).