IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 21, 2022, accepted April 12, 2022, date of publication April 22, 2022, date of current version April 29, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3169418

A Fog and Blockchain Software Architecture for a Global Scale Vaccination Strategy

HUMBERTO JORGE DE MOURA COSTA[1,2], (Member, IEEE),
CRISTIANO ANDRÉ DA COSTA[1], (Senior Member, IEEE),
RODRIGO DA ROSA RIGHI[1], (Senior Member, IEEE),
RODOLFO STOFFEL ANTUNES[1], (Member, IEEE),
JUAN FRANCISCO DE PAZ SANTANA[3],
AND VALDERI REIS QUIETINHO LEITHARDT[4,5], (Member, IEEE)

[1]SOFTWARELAB—Software Innovation Laboratory, Applied Computing Graduate Program—PPGCA, Universidade do Vale do Rio dos Sinos—UNISINOS, São Leopoldo 93022-750, Brazil
[2]IFRS Veranópolis, Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS), Veranópolis 95330-000, Brazil
[3]Expert Systems and Applications Lab, Faculty of Science, University of Salamanca, 37008 Salamanca, Spain
[4]COPELABS, University Lusófona—ULHT, 1749-024 Lisbon, Portugal
[5]VALORIZA—Research Centre for Endogenous Resource Valorization, Polytechnic Institute of Portalegre, 7301-110 Portalegre, Portugal

Corresponding author: Cristiano André Da Costa (cac@unisinos.br)

This work was supported by the Spanish Agencia Estatal de Investigación through the Project Monitoring and Tracking Systems for the Improvement of Intelligent Mobility and Behavior Analysis (SiMoMIAC) under Grant PID2019-108883RB-C21/AEI/10.13039/501100011033.

ABSTRACT Nowadays, there are many fragmented records of patient's health data in different locations like hospitals, clinics, and organizations all around the world. With the arrival of the COVID-19 pandemic, several governments and institutions struggled to have satisfactory, fast, and accurate decision-making in a wide, dispersed, and global environment. In the current literature, we found that the most common related challenges include delay (network latency), software scalability, health data privacy, and global patient identification. We propose to design, implement and evaluate a healthcare software architecture focused on a global vaccination strategy, considering healthcare privacy issues, latency mitigation, support of scalability, and the use of a global identification. We have designed and implemented a prototype of a healthcare software called Fog-Care, evaluating performance metrics like latency, throughput and send rate of a hypothetical scenario where a global integrated vaccination campaign is adopted in wide dispensed locations (Brazil, USA, and United Kingdom), with an approach based on blockchain, unique identity, and fog computing technologies. The evaluation results demonstrate that the minimum latency spends less than 1 second to run, and the average of this metric grows in a linear progression, showing that a decentralized infrastructure integrating blockchain, global unique identification, and fog computing are feasible to make a scalable solution for a global vaccination campaign within other hospitals, clinics, and research institutions around the world and its data-sharing issues of privacy, and identification.

INDEX TERMS Blockchain, cloud computing, fog computing, healthcare, hyperledger.

I. INTRODUCTION

Due to recent advances in the area of the Internet of Things and healthcare, patient data can be dispersed in multiple locations [1]. As a result, scientists have been proposing solutions based on Cloud Computing to manage healthcare data [2]. Cloud computing is an architecture model that can provide convenient access to the network for a set of fast configurable computing capabilities for delivery and release with low management effort or interaction with the service provider [3]. However, many solutions present some real-world challenges to be addressed. Common tasks such as aggregate, process, and storing a huge amount of information are hard to do in a scenario that requires real-time data analysis [4].

One possible approach to address this gap between real-time analytics and healthcare applications is the use of Fog Computing. Fog computing is defined by NIST as a

The associate editor coordinating the review of this manuscript and approving it for publication was Daniel Grosu.

layered model for enabling ubiquitous access to a shared continuum of scalable computing resources [5], [6].

For instance, due to the fact that medical sensors generate data frequently, with the use of Fog Computing, the performance of the real-time analysis may be improved, supporting intelligent data analysis and decision making based on local policies and network resources of the end-users [7], turning into a scalable solution [8]. Some of the most important key features identified of the Fog Computing paradigm are: low latency, scalability, Support of mobility, real-time interaction and wide geographical distribution [9]–[11]. In a healthcare environment, low latency is desirable because it can allow for much faster response time and data analysis across a wide geographic location, such as hospitals, clinics, and other laboratories that are certainly not close most of the time [12], [13].

In addition, in several cases, another important issue to be addressed is that hospital policies do not allow the storage of patient data on external network environments due to elevated risks of patient data leaks [14]. Another technology that has widely been proposed to address privacy and security in healthcare is the Blockchain [15], [16]. A Blockchain is a distributed and decentralized software solution formed by a peer-to-peer network consisting of cryptographically, signed transactions and a distributed ledger technology with the objective of executing transactions and storing data securely [17], [18].

Blockchain is a decentralized and distributed architecture forming a peer-to-peer network, where cryptographically signed transactions of digital currency take place. The exciting feature of Blockchain is distributed ledger technology (DLT), which contributes to address several problems of digital transparency, non-repudiation, and trustable contracts on collaboration [19], [20]. It consists of a peer-to-peer (P2P) distributed ledger database for transactions without the necessity of a central authority or a third-party verification.

The key benefits included in blockchain technology applied to healthcare can be decentralized management, immutable audit trail, data provenance, improved security, robustness, and availability. The blockchain can also improve the medical record management, enhance the insurance claim process, accelerate the clinical/biomedical research, and advance biomedical/healthcare data sharing [21].

Another important question is how to uniquely identify resources. Many organizations develop their own naming/service system to differentiate distinct entities in a healthcare system [22]. The lack of standard location identification leads to increased costs by causing medicines delivery errors and complicating the rebate process [23]. One example is the problem that a single location may have multiple names and different identification codes [24]. Currently, there are two know alternatives to the unique identification of assets in healthcare: the Health Industry Business Communication Council - HIBCC system and the GS1 system. The HIBCC system, created in 1983, provides unique identifiers for healthcare locations - HIN and Labeler Identification Code - LIC for healthcare assets but is restricted mostly to the United States market [25]. The other alternative, GS1 Standards was developed by an international, non-profit global organization that develops and implements standards to improve supply chain management in over 23 industries, including retail, healthcare, consumer electronics, and transportation [22].

This article aims to combine Fog computing, blockchain, cloud technologies, and global unique identification in order to improve distributed healthcare software in a scenario of global wide vaccination strategy. The major contributions of this work are as follows:

- the development of a software architecture that considers healthcare technological challenges and issues, identified in the current literature, including privacy, unique identity, and scalability [2];
- Support rapid healthcare decision-making through fog data access
- Propose a blockchain global network supporting smart contracts for scalability, privacy, security, and for reducing the latency and providing fast and real-time access of a vaccination process avoiding a single point of failure [26].
- propose an evaluation of a hypothetical scenario where a global integrated healthcare vaccination strategy as example of application of the architecture.

The structure of this article is divided into seven sections. The rest of this article is organized as follows. In Section II, the related work is presented, comparing the main solutions found in the literature related to the known main challenges and issues in healthcare. Section III, presents the details about the proposed architecture. In Section IV, Materials and Methods, the process and methodology applied in this research is described. In Section V, the results found are presented. In Section VI, we elaborate and discuss the results, issues, and concerns. Finally, in Section VII, we present the main conclusion of this work.

II. RELATED WORK

In the current literature, interoperability, privacy, mobility, security, unique identity and scalability are widely known as issues to be addressed in a distributed healthcare software architecture [2]. Thus, the most relevant and recent papers related to these challenges was selected through a search using most well-known scientific databases including IEEE Xplore [27], Science Direct [28] and Google Scholar [29].

In the work of Tuli *et al.* [30], a cost-efficient prototype for Sleep Apnea analysis is implemented in an architecture called Fogbus. This architecture has the goal to integrate different IoT-enabled systems into Fog and Cloud Computing infrastructures. A blockchain network has been used for integrity support and a fog strategy to reduce latency. The main contribution of this work is the integration of platforms, trying to address the latency and security of sensitive data applications such as healthcare applications.

In the article of Mutlag *et al.* [31], a Multi-Agent Fog Computing Model for Healthcare Critical Tasks Management (MAFC) is proposed. It consists of a mapping between

decision tables with the objective to optimize scheduling the critical tasks based on their priority, network load, and resource availability. The main contribution is to provide two levels of task prioritization of resources (locally and globally) for Fog Computing, providing efficient prioritization for abnormal tasks for the patient critical situation with facilitated node cooperation and resource sharing.

In the work of Tanwar *et al.* [32], the authors propose a blockchain-based EHR sharing system architecture. This architecture is composed of resources called Patient, Clinician, Lab, and System admin. In its approach, various assets and smart contracts are executed and measured by a performance evaluation using a hyperledger fabric blockchain network. The main contribution of this work is it has a strong focus on privacy and security in healthcare distributed software by eliminating the central authority and implementing a single point of failure in the system.

The architecture BCHealth [33] focuses on a privacy approach where data owners can define their desired access policies over their privacy-sensitive healthcare data, which is shared with medical staff. It is composed of a cluster to address the problems of scalability, throughput, and overhead. An experimental analysis was made to prove the efficiency of computation and processing time and resilience against several security attacks. The main contribution of this work is the implementation of its own blockchain network and the evaluation of its performance.

In the work of [34], they implemented a private blockchain network using the framework Hyperledger Fabric with the goal of sharing Electronic Health Records with support of security and privacy. The proposed architecture was based on a study of uses cases including regulation compliance, flexibility, and scalability. Nevertheless, this work does not do an evaluation of performance, the main contribution found is key criteria for the implementation of secured healthcare applications supporting blockchain technology.

The work of [35] consists of a framework for e-Healthcare services based in Fog Computing and Blockchain for monitoring and recognition of human activities. The framework is able to extract several features from frames of the videos to identify different human actions. They collected video data from the generic datasets called Hollywood2, UCF50, and KT and have detected actions performed by humans, such as shaking hands, hugging, or running to represent some activities in a health center. The principal contribution is the use of a Fog and Blockchain strategy for enabling these features with computational efficiency and higher accuracy.

The work of [36] proposes a Fog Computing architecture for healthcare based on IoT and implemented in a blockchain platform with the goal to share data between IoT, fog nodes, patients, and doctors with security and reliability. The main contribution is the creation of a new approach to meet the QoS requirement related to the security, authenticity, and reliability of Patient Health Data.

Beeptrace [37] proposes a healthcare software architecture using blockchain to trace and share information data from the COVID-19 pandemic preserving security and privacy issues. The main contribution of this work is the discussion of its blockchain performance, and several aspects such as economic and social impacts, supporting governments, authorities, companies and research institutes globally.

The objective of the work of [15] is to create a prediction model for Diabetic Cardio diseases using Fog Computing and Blockchain. The main contribution of this work is the use of a pre-processing technique in order to reduce the size of the dimensionality of the data and the use of clusters to work more efficiently in predicting the disease compared to other related papers.

The work of [38] proposes a smart healthcare system architecture for remote patient monitoring. The architecture is divided in layers called Smart Medical Devices Layer, Fog layer, and Cloud Layer. This approach was based on the use of IoT, Blockchain, and Fog Computing technology. It was implemented an use case in diabetic monitoring. The principal contribution is the discussion of the limitation of the model, such as scalability, mainly because the big volume of data causes some issues such as performance degradation or increased response time.

For a better comprehension of these related works, these articles are organized in the following categories: Application type, Main challenges, Unique identity, Blockchain platform, Blockchain type, and Consensus algorithm, as it can be noticed in Table 1.

The Application Type category is divided into General purpose, where there is no definition of a specific healthcare application; Critical healthcare applications, representing the tasks which it is very critical like surgery; Health Record Management, including EHR, PHR, or any format of health data records; Remote patient Monitoring, consisting in video and related monitoring applications; Pandemic Tracing, where the main idea is trace data related to a pandemic such as COVID-19; and Disease prediction, which the main goal is to predict some disease with a good level of accuracy.

The main challenges categories represent the main issues addressed by the articles, like latency, privacy, and security. Unique identity indicates if the article uses a global unique identification number or a more local place or not specified. The Blockchain platform, type, and consensus algorithm represent the characteristics of some blockchain implementation, if is Hyperledger, Ethereum, or a custom made, if it is permissioned or permissionless, and the kind of algorithm used in the consensus, the review method to define if the data should be considered when registering a blockchain. Some algorithms are the Power of Work - PoW, Power of Authority - PoA, Direct Acyclic Graph - DAG or not specified.

Comparing the related work with the proposed architecture, the scalability of related works like Tuli *et al.* [30], Mutlag *et al.* [31], Hossein *et al.* [33], Antwi *et al.* [34], and Shynu *et al.* [15] is addressed by the increasing the number of fog nodes. The privacy question is approached by different strategies such as the use of encryption and blockchain of most of related works. The unique identity is implemented only locally by Antwi *et al.* [34],and Shukla *et al.* [36], being

TABLE 1. Comparison of related articles.

Paper	Application Type	Main challenges	Unique identity	Blockchain Platform	Blockchain Ttype	Consensus Algorithm	Year	Publisher
Tuli et al. [30]	General purpose	platform independence, security, resource management and multi-application execution	Not Supported	Custom	Permissioned	PoW	2019	Elsevier
Mutlag et al. [31]	Critical healthcare Applications	Tasks Scheduling Optimization	Not Supported	Not Supported	Not Supported	Not Supported	2020	MDPI
Tanwar et al. [32]	Health record management	latency, security and privacy	Not Supported	Hyperledger	Permissioned	PoW	2020	Elsevier
Hossein et al. [33]	General purpose	privacy, latency, scalability, access control	Not Supported	Custom	Permissioned	PoA	2021	Elsevier
Antwi et al. [34]	Health record management	scalability, privacy and security	Local	Hyperledger	Permissioned	PoA	2021	Elsevier
Islam et al. [35]	Remote patient monitoring	latency, security and privacy	Not Supported	Custom	Permissioned	Not Specified	2020	Elsevier
Shukla et al. [36]	Health record management	latency, security and privacy	Local	Ethereum	Permissionless	PoW	2021	Elsevier
Xu et al. [37]	Pandemic tracing	latency, security and privacy	Not Supported	Ethereum	Permissioless	DaG	2020	IEEE
Shynu et al. [15]	Disease prediction	latency, scalability, security and privacy	Not Supported	Custom	Permissionless	Not Specified	2021	IEEE
Fetjah et al. [38]	Remote Patient Monitoring	latency and privacy	Not Supported	Ethereum	Permissionless	PoW	2021	IEEE
FogCare (this work)	General Purpose	latency, scalability, data integrity, privacy	Global	Hyperledger	Permissioned	PoW	-	-

the other related works have not implemented this type of identity. The main difference is that our propose makes a different approach, considering a global unique identity implementation.

In Table 1, there is a wide implementation decision preference considering latency, security, and privacy. None of the papers considered a Global Wide Unique identification approach, even those trying to address pandemic issues. So, global identification would be a gap, because, in a more global context, assets can be managed more efficiently.

III. ARCHITECTURE

The architecture proposed in this article, called Fog-Care, has the objective to contribute to address the issues and challenges found in distributed computing software applied to the healthcare domain. The most relevant challenges are: scalability, unique identity, and privacy. Furthermore, there are real gaps to address such as the use of these technologies in a more integrated approach, considering the issues of the uniqueness of assets, like patients' identity and the concerns of gain scale from an integrated point of view and supporting distributed sharing healthcare data are considered.

Considering this, the choice of GS1 standards approach was made due to the possibility of solving the global naming problem with a scalable global solution. The GS1 Global, is an organization formed by a global community of volunteer users, such as stakeholders in the health supply chain, including manufacturers, distributors, hospitals, solution providers, regulatory and industrial bodies have developed patterns to allow healthcare providers to uniquely identify products, patients, clinics, assets and locations for transparent processes across the medical value chain with a common globally unique and unambiguous identification system for sharing data [22]. The advantages of these standards can be the Ease of Use and Usefulness, Product Identification, Accurate and Reliable Tracking, Information Accuracy, Information Availability [39].

The support of scalability [40] is implemented through a Fog Computing [5]. Healthcare applications usually need real-time interactions rather than batch processing for a quick and urgent response [41]. The low latency is implemented with fog nodes co-located close to the smart end devices, so the analysis and response are quicker than from a centralized cloud service or data center. The importance of Geographical distribution is because healthcare applications can demand widely, but geographically identifiable, distributed deployments with access points geographically positioned along with a wide scope area [42].

A Privacy [43] issue is a major challenge for health data systems to become smarter is how to collect, store and analyze personal health data without raising privacy violations. For these systems, privacy concerns have created barriers to the adoption of health data systems [43], and the definitions described in [44]. The proposed approach to address the problem of privacy is the blockchain. Blockchains are tamper-evident and tamper-resistant digital ledgers implemented in a distributed fashion, without a central repository, generally without a central authority such as a company, or government. They can permit a community of users to record transactions in a shared ledger where no transaction can be changed once published [45]. Deploying healthcare data in a blockchain can provide several benefits such as: complete, consistent, timely, accurate, and easily distributed data, agreements without the involvement of a trusted mediator. Avoiding performance bottlenecks or a possible single point of failure. Patients can have control over their data. Changes in the blockchain healthcare data are visible to all members of the blockchain network and all data insertions are immutable. In addition, any unauthorized changes can be detected easily [46].

A. FOG-CARE ARCHITECTURE OVERVIEW

The fog-Care Architecture overview is composed of organizations that can be geographically distributed places such as hospitals, clinics, and laboratories and people like patients and health professionals (Figure 1). The main technological components include three components: a Fog Network, responsible to reduce the traffic of healthcare shared data, including one Fog Node per organization, a Blockchain network for the support of privacy and scalability, and the use of a global standardization naming system called GS1 Standards. Each addition component is described as follows:

- **Hospitals, Clinics, and Laboratories** are any determined building or place for the hospitalization and treatment of a sick or injured person. Hospitals can belong to a determined Complex, which is a group of hospitals managed by the same organization. Generally, they may contain hospitals of each specialty and are located in the same geographic location. Clinics are healthcare centers where you can receive routine preventative care or visit your doctor. A clinic is an institution smaller than a hospital that aims to treat patients that require simple procedures and short stays. Medical laboratories are a place where clinical pathology tests are carried out on clinical specimens to obtain information about the health of a patient to aid in the diagnosis, treatment, and prevention of disease. Generally, laboratories work together with hospitals or clinics because its specialized tests. In this model, each health facility can collaborate, share health data, and can be geographically distributed close or far from each other.
- **Patients**: This component represents, in this architecture, a unique individual who had been received medical care at a hospital, clinic, or other places. Each patient is globally identified by a global identification number. Patients are a central part of the model because the goal of healthcare is to prevent diseases and help people live longer and improve their quality of life. A patient may have a device such as a cell phone, tablet, which can be can be used to consult and write down relevant data from himself.
- **Health data** is the historical data that had been found in the patients' medical records such as an Electronic Health Record. The health data can, generally, be accessed by the patient through a mobile App. Usually, this data is stored by the hospital and accessed by the doctor using some piece of software. The global data is composed of all the data found outside the local and essential data. This data comprehends the medical records in other hospitals, clinics, etc and the access must be authorized by the patient. The data can be stored in a blockchain distributed with each partner health facility.

B. FOG-CARE ARCHITECTURE COMPONENTS

In Figure 2, a diagram of the Fog-Care Architecture organized in layers is shown. It is formed by a Patient Service Layer,

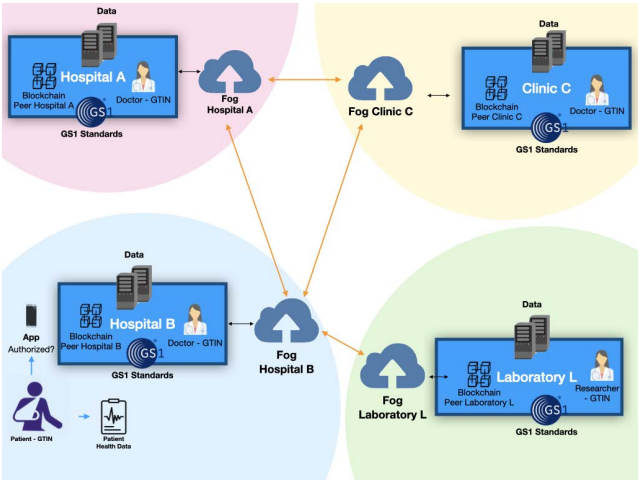


FIGURE 1. Fog-care approach overview.

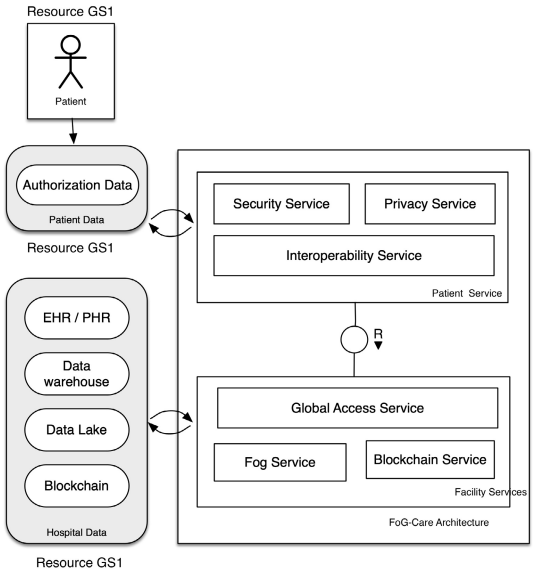


FIGURE 2. Fog-care technical architecture modelling.

a Facility Service (organization), and the healthcare data (Resource GS1).

The healthcare data (Resource GS1) is represented by the Patient Data and the hospital resources. The patient Data represents the healthcare data stored in a local hospital and the Token, which contains essential information regarding the patient. The hospital resources contain the EHR / PHR, Data warehouse, blockchain, and Data Lake. The first one is a standard in healthcare industry data format, which is widely used by hospitals to store internally the patients' data. and The last two resources are almost always being used as auxiliary data in the hospital, generally for researching issues. Each service is responsible to manage its resource.

The Patient Service Layer has 3 services: Privacy Service, Security Service, and Interoperability Service. It is the layer responsible for the security, privacy, and interoperability services related to the patient. The patient data is considered all the data that can be shared among health facilities such as hospitals, laboratories, and clinics and is

necessary the authorization of the patient. Patients and their resources have a unique number for global identification. The security service encapsulates the general idea of the basic infrastructure of security such as authentication, integrity, and access control. The privacy service addresses the issues of who has the authorization to see what data. The Interoperability Service ensures that all data communication can be made correctly, adapting to each context, for example, mobile desktop or web user interfaces.

The Privacy Service is responsible for the warranties of the data privacy. It also ensures that patient, doctors, administrative users, and staff teams have their appropriate access and control. This includes the use of a blockchain network to control and audit the health data integrity and services related to the privacy of the patient.

The Security Service is formed by the services of authentication, access control, log, encryption, and decryption in the healthcare model. For security reasons, the communication of health data is encrypted and decrypted according to the level of security needed. The Integrity of files is necessary for the validation of the patient data. Some data can be incomplete or invalid, so supporting these systems can improve security. Another important feature of this service is to protect which data specifically can be shared externally with others health facilities such as hospitals, clinics, or laboratories partners.

The Interoperability Service can help to optimize the healthcare industry operations because generally, the data comes from multiple sources of information, such as laboratories, clinics, pharmacies, hospitals and has several texts or file formats, such as JSON, XML, plain text and different standards and protocols involved. The service can support and convert these formats for communication efficiency.

The Facility Service Layer has 3 services: Global Access Service, Fog Service, and Blockchain Service. A facility is any location where healthcare is provided, for instance, a hospital, clinics laboratories, and so on. This layer contains the Global Access Service, the Blockchain Service, and Fog Service.

The Global Access Service manages all the strategies of healthcare data access of the facility. For instance, it can delegate to a Fog or Blockchain directly if necessary, according to the policies and rules of the facility.

The Fog Service represents one or more fog nodes depending on the configuration of the strategy. The Fog, with the support of fog nodes, helps to get the data with a reduced latency compared to the cloud. The fog nodes are responsible for sending and receiving health data between different hospitals or other psychical structures. Each fog runs a REST Service with an API defined to consult, edit or share data. Each time health data is requested, the fog checks whether the information exists locally in an internal server or should be requested outside the health facility. The main idea of the fog is to reduce latency and process locally all possible health data avoiding overwhelming the clouds. Its services can access the blockchain and all the facility data since the user has permission.

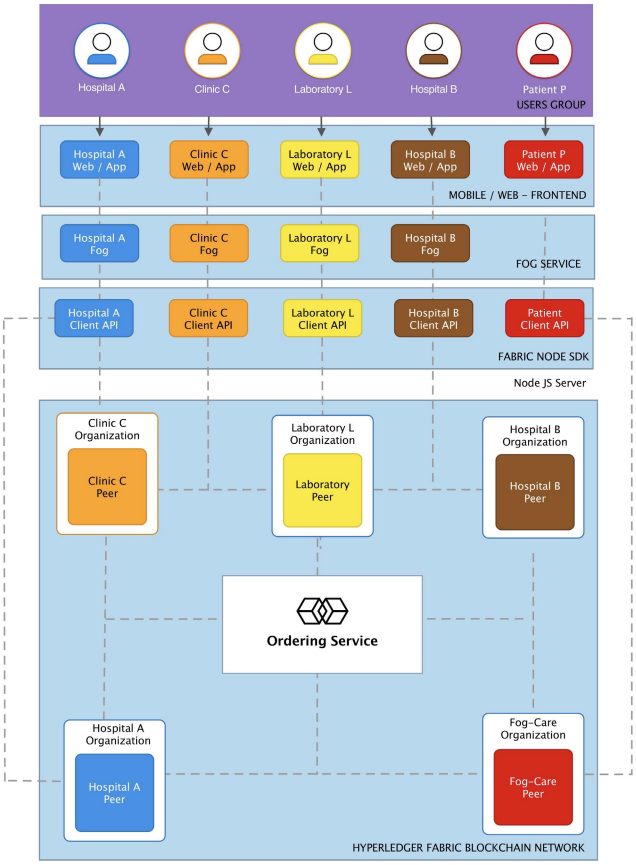


FIGURE 3. Blockchain service of fog-care architecture.

The Blockchain Service allows access to read or write the healthcare data in the same way as a database, with the difference that all the data is traced and the ledger cannot be deleted. The Blockchain implementation is included, so the essential health data may be shared with other hospitals to obtain a more detailed health history of the patients. This data structure can be stored in form of medical records in the blockchain. The advantages of this approach are the warranty of privacy of the data and the integrity and rastreability of all the processing of these records. In this model, the blockchain stores its data, such as patients and exams with standard codes with the idea of global identification for use with each actual or future partner organization. This service is formed by a set of layers described in Figure 3.

This proposed blockchain is divided into five layers: Users Groups, Mobile/Web - Front-end, Fog Service, Fabric Node SDK, and Hyperledger Fabric Blockchain Network as follows:

- **The Users Groups Layer** represent the authorized users of the blockchain. They are grouped by affiliations or companies called Organizations. Several organizations can exist, such as Hospital A, Hospital B, Clinic C, Laboratory L, and Patient P as examples demonstrated in this layer. There are doctors, nurseries, and attendants of such organizations, like Hospital A, Hospital B, and all the health facilities participating in the blockchain

network. Each group of users belongs to a health facility (organization) where these individuals and groups do not know each other and can be geographically distributed. Therefore, they may trust to share health data, because of the consensus of blockchain providing the privacy and integrity of all operations made. Each organization controls its users, access, and permissions independently.

- **Mobile/Web - Front-end Layer** layer represents the user interface. This software can be a mobile, web application, or both. Each healthcare facility hosts this software in its organization, except for the patient group, because it belongs to the FogCare group, a special organization created to manage the global identity of all patients of the blockchain. The authentication in this application is made based on the users of the organization defined in the previous layer, all participating in the blockchain. The main features were presented in the previous model section. For instance, a doctor can search exams of a determined patient or a patient can authorize his healthcare data to be visualized by all healthcare facility organizations.
- **The Fog Service Layer** consists of a set of Web Services to attend and serve requests of the Front-end layer. There is at least one Fog Service including Fog nodes in each organization. Fog nodes can be routers, switches, or any server responsible for the communication of devices in their geographical area, being able to provide them with services [47]. Fog nodes are positioned close to the IoT devices and they handle the heterogeneity of the data coming from different devices.This fog receives the internal requests and verifies if the data can be brought from the local network or the request need to be passed to an external organization. The objective of this layer is to reduce network latency and provide a near real-time scalable healthcare application. The structure of Fog Service is described and explained in the next subsection Healthcare Communication Service.
- **The Fabric Node SDK Layer** contains the server code that receives requests from Fog Service to call the essential Client APIs to interact with the blockchain network. Each organization such as a healthcare facility must have this code implemented and running in your network. The exception is the Patient Client API because the user uses the front-end or mobile application for patients that interacts directly with this layer instead of Fog Service Layers and it is not implemented in a healthcare facility. Some basic operations might be: create channels, ask peer nodes to join the channel, install chaincodes in peers, instantiate chaincodes in a channel, invoke transactions by calling the chaincode, and query the ledger for transactions or blocks.

  All the code of this layer, as a client, make an interface with the ordering services and peers of the next layer, Hyperledger Fabric Blockchain Network.
- **The Hyperledger Fabric Blockchain Network** is the core layer of the proposed blockchain architecture. It is formed by the Peers, Ledger, and the Ordering Service.
  - **The Peers** are the foundation of a blockchain network and each of which can hold copies of ledgers and copies of smart contracts. A contract consists of an agreement signed between the parties to do determined activities [48]. The Ledger can be consulted and updated by applications through smart contracts. The healthcare peers host instances of the ledger, and instances of the smart contracts (chaincode) containing the code and healthcare data of the health facility. This provides a deliberate redundancy to avoid single points of failure. Every blockchain network is composed mainly of a set of peer nodes. In this layer, each health facility has a different and own peer. Additionally, there is an exclusive Fog-Care peer for managing the patients globally and addressing the global unique identification of them. Peers, in conjunction with orderers, ensure that the ledger is kept up-to-date on every peer.
  - **The blockchain Ledger** is used to store the patient health data such as exams, location, medicines, comorbidities, blood type, diseases, tolerance, and allergies, for example. In this healthcare proposed blockchain architecture, the ledger can store the EHR of the patients with security and privacy. The GS1 standards are used in the resources to ensure the identification, localization, and rastreability of these essential resources. The main idea beyond this approach is to provide essential information for quicker attendance and a better healthcare response time, providing transparency, efficiency, and security [49].
  - **The Fog Service** consists of a set of Web Services to attend and serve requests of the Front-end layer. There is at least one Fog Service in each organization. This fog receives the internal requests and verifies if the data can be brought from the local network or the request need to be passed to an external organization. The objective of this layer is to reduce network latency and provide a near real-time scalable healthcare application. The structure of Fog Service is described and explained in the next subsection Healthcare Communication Service.

IV. MATERIAL AND METHODS

For the evaluation of this work, is proposed an use case of vaccination where are included health data about worldwide patients distributed in a continent geographical space. This scenario simulates a global integrated COVID-19 vaccination campaign, being stressed by a peak of vaccination process. It has the objective to verify, if the architecture supports the requirements and addresses the challenges of healthcare architecture studied.

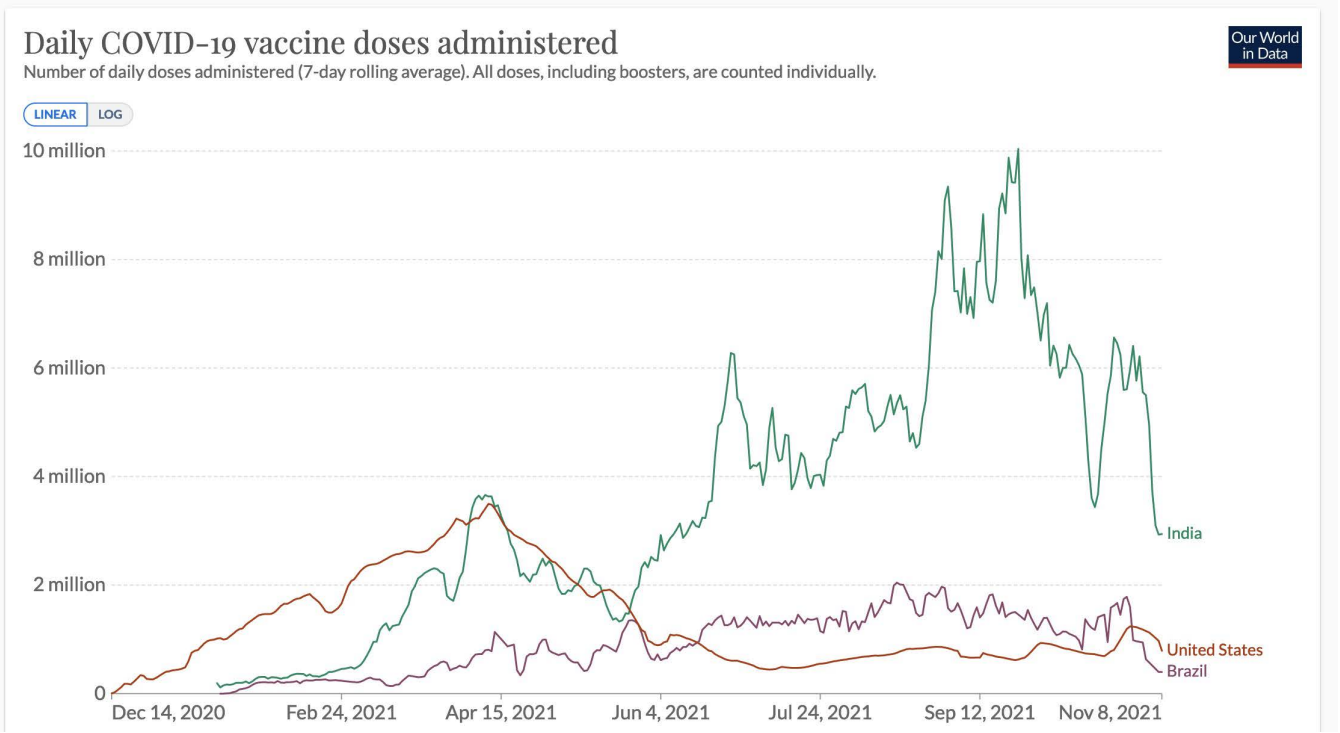


FIGURE 4. Moving average of 7 days vaccination in US, India and Brazil. Source: [50].

A. VACCINATION SCENARIO

This scenario comprises in some assumptions. We are in the year 2021 and the COVID-19 pandemic must be brought under control Quickly. Due to the risk of new SARS-CoV-2 variants arriving, a consortium of countries decided to invest in the Fog-Care solution in order to enable faster decision-making through the use data from the vaccination process around the world. That decision could be, for example, donating vaccines to certain countries, investing in booster shots, proposing strategies to block or restrict access, or even provide faster access to global health data for scientists around the world.

Thus, the consortium of countries, initially, draws up a vaccination plan covering 3 countries that are widely dispersed geographically: Brazil, the USA, and England. In this case, each country will try to prevent more deaths by vaccinating as many people as possible. The requirements for this process are to support global unique patients identification, data privacy, and scalability. After a mutual meeting, the countries decided to implement a solution based on the Fog-Care architecture and the objective is to support the vaccination around the world, supporting the values of countries with the higher picks (10 million / day) in the vaccination of COVID-19 pandemic, as can be noticed in Figure 4, data source from Our World in Data [50]. India have reached the pick of 10 millions vaccinations while United States and Brazil almost 4 millions.

B. INFRASTRUCTURE

For the evaluation, was installed 3 virtual machines of the Amazon Web Service - AWS (Figure 5). Each VM was instantiated in your own country, serving as a Fog node. The configuration used for the tests was a standard AWS t2.micro machine. This machine has the following standard specification [51]:

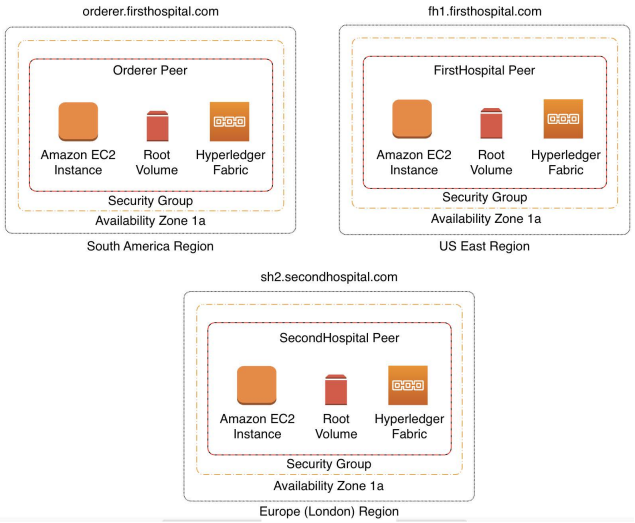


FIGURE 5. Fog-care implementation on amazon web services - AWS.

- 1 vCPUs;
- 1 RAM (GiB);
- $0.0116 On-Demand Price/h.

For the blockchain network was used the Hyperledger Fabric version 2.0 and the evaluation was conducted with Hyperledger Caliper version 0.43. All the values are filtered to exclude outliers.

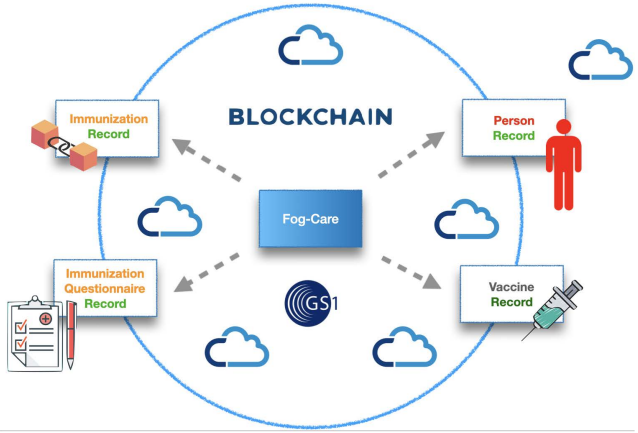


FIGURE 6. Fog-Care implementation in a vaccination use case.

```
type PersonSmartContract struct {
        contractapi.Contract
}

type Person struct {
        IdPerson     int     `json:"IdPerson"`
        Name         string  `json:"name"`
        Gender       string  `json:"gender"`
        Birthdate    string  `json:"birthdate"`
    (...)
}
```

LISTING 1. Fragment of source code of person smart contract.

TABLE 2. Fog-care blockchain implementation.

Vaccine	Vaccination	Person	Questions	Answers
IdVaccine	idVaccination	IdPerson	IdQuestion	IdAnswer
gtin	idPerson	name	idVaccine	idPerson
name	idVaccine	gender	version	date
version	idQuestions	birthdate	date	answer01
country	idAnswers	mother	entity	answer02
minTemp	applicator	father	question01	answer03
maxTemp	minTemp	address	question02	answer04
expirityInDays	maxTemp	city	question03	answer05
laboratory	expirityInDays	state	question04	answer06
minDose	facility	country	question05	answer07
maxDose	dose	zip	question06	answer08
doseInterval	local	cid10_01	question07	answer09
	lot	cid10_02	question08	answer10
	expirationDate	cid10_03	question09	
		cid10_04	question10	
		cid10_05		

To support the privacy of vaccination data, is developed a Hyperledger Blockchain implementation that includes the definition of 5 main assets: Person, Vaccine, Vaccination, Questions and Answers (Figure 6).

The **Vaccine Record** consists of a representation of a Vaccine and it is implemented in a Smart Contract with the ReadVaccine and WriteVaccine methods. The fields include some characteristics such name, minimum temperature, maximum temperature, a unique identification id, and others shown in Table 2.

Person Record represents a person who will be vaccinated. He or she also has globally unique identification, based on GS1 Global Standards, including general enrollment data such as name, birth date, and the identification of possible comorbidities.

This data structure also contains the methods ReadPerson() and WritePerson(). The Smart Contract Questions contains all the custom questions to be presented to the patient before the vaccination. ReadQuestion and WriteQuestion are functions available as well. So, complementing the questions there are the Answers smart Contract. They are responsible to manage the answers of each person and provides the functions WriteAnswer and ReadAnswer. The last smart contract is the Vaccination. It will store the process of being immunized of each person. In the fields are stored the person, vaccine, questions, and answers of each immunization applied. WriteVaccination and ReadVaccination are available.

C. METRICS

The evaluation is based on a performance benchmark test software called Hyperledger Caliper,[1] which is a performance tool maintained by the Hyperledger Foundation that supports custom use cases tests for testing several blockchain networks, such as Hyperledger Fabric and Ethereal. The caliper can generate reports including several performance metrics like latency, throughput, and send rate. The Caliper components includes a benchmark and network configurations, and a report. The choice of Caliper is due to the fact that it is currently a established benchmark set for a large existing blockchain technologies, like Ethereun, Hyperledger Fabric, Besu, Burrow, Iroha, Sawtooth, and FISCO BCOS.

The following Caliper configuration parameters were used [52]:

- workers number: 5
- rounds txNumber: 500
- rounds rateControl fixed-rate: from 10 to 100

The workers number represents the number of worker processes to use for executing the workload, rounds txNumber is the number of transactions Caliper should submit during the round, and rounds rateControl type, which represents the desired rate of transactions send. When we use a fixed-rate, means the Caliper will send input transactions at a fixed interval that is specified as transactions per second. in this case, 10 to 100 per time.

The following metrics were measured [52]:

- Average, minimum and maximum latency
- Throughput
- Send rate

The **Latency** is calculated by the following formula:

$$Latency = TimeResponseReceived - SubmittedTime$$

This measurement includes the time, in seconds, that the function of smart contract is submitted to the moment that the result is available for all the peers in the network, including the propagation time and the consensus mechanism. In other words, the latency is the difference, in seconds, between a transaction submitted and finished considering all the network.

[1] https://www.hyperledger.org/use/caliper

As the same idea, the **Send Rate** is defined by the Caliper as follows:

$$SendRate = TotalSubmittedTransactions/TotalTime$$

The difference is that the Send Rate measure considers the real capacity to send transactions to the blockchain. Total Time is measured in seconds. The metric considers only the rate at which requests were sent to the blockchain, without considering the time needed to obtain a response.

An the last one, **Throughput** is described as follows:

$$Throughput = TotalCommittedTransactions/TotalTime$$

The Throughput measure differs from the Send Rate when considering the actual execution capacity. While Send Rate measures the capacity to send code to execute on the blockchain, throughput measures the ability to execute it. In other words, this metric also measures the rate at which the blockchain is able to respond to requests. For example, the blockchain can send 50 transactions per second (Send Rate), but only process 25 transaction per second (Throughput) This happened because the blockchain does not have enough resources to meet the number of requests identified in the send rate.

In fact, using these metrics, it will be possible to verify the performance of latency in the Fog-Care architecture and it will be possible to verify the scalability support of the proposal.

The main configuration of Caliper consists in describing the network in a file called network-config.yaml, and define the general configuration. The network config file holds the setting of Organizations (FirstHospital and SecondHospital), channels (fogcarechannel), and peers involved, and the general configuration file, stores all the configurations related to the workload. In this case, the parameters for a fixed load of 10 to 100 transactions per second per execution was chosen, limiting to a total of 500 total transactions.

For a better understanding of results the metrics average latency, minimum latency maximum latency, send Rate, and throughput, It is divided in write operations and read operations. Write operations save a data on blockchain and read operation, read a data. In the previous definition of the implementation of Fog-Care smart contract, was selected the best representative functions which are ReadVaccination() and ReadPerson() for measuring the read operations and CreatePerson() and CreateVaccination() functions for measure the writing on blockchain.

It is also considered the interquartile range (IQR) for the outliers tratment. It is a measure of variability, based on dividing a data set into quartiles. The values that divide each part are called the first, second, and third quartiles, and they are denoted by Q1, Q2, and Q3, respectively.

- Q1 is the ''middle'' value in the first half of the rank-ordered data set.
- Q2 is the median value in the set.
- Q3 is the ''middle'' value in the second half of the rank-ordered data set.

The IQR is calculated by:

$$IQR = Q_3 - Q_1$$

where the q^{th} element is calculated by:

$$\left(\frac{i(n+1)}{4}\right)^{th}$$

Furthermore, it is considered a blockchain network with one orderer peer and two anchor peers. These computers were simulated on a virtual environment using Amazon Web Service - AWS. The Orderer was hosted in Brazil (São Paulo) and the peers called FirstHospital and SecondHospital was hosted in the USA (Northern Virginia) and United Kingdom (London). The machines used was of T2.Micro type (5) to standardize to a cheap and widely known pattern specification. It is also considered the highest vaccination rate, moving average of 7 days in India, consisting of 10 million vaccinations per day (Figure 4).

V. RESULTS

All the results were considered of an average of 5 executions of the same smart contract code. After this procedure, were took out the outliers using the IQR method. The results were finally grouped them in Read Operations and Write Operations for a better understanding of processes..

In Figure 7, the maximum, average, and minimum latency for the blockchain read operations are shown. The values of the minimum are low (above 1 second) and the average latency grows consistently in a linear progression. The peak of Maximum latency are expected due to network traffic of a wide geographic dispersed network.

The Latency, the maximum, average, and minimum latency for the blockchain write operations concerning Transaction per seconds is showed. The values of the minimum are low (above 1 second) and the average latency grows consistently with the maximum latency.

In Figure 8, the send rate for blockchain is shown. It grows quickly like an exponential function in both, read and write operations. In Figure 9, the throughput for read operations grows consistently until the 80 requests where it reverse the movement, causing some randomness. Likewise, the throughput for write operations increases until the 70 requests, where it reverses the movement in similar behavior with the read operation.

In the results, the peak was achieved of effectively sending 61.2 transactions per second, or 5,287,680 per day, assuming a total period of 24 hours. The peak of 35.3 transactions per second processed (throughput) or 3,049,920 per day. In this case, including only three peers. The maximum vaccination peak was in India, with 10 million vaccinations per day, a moving average of 7 days. In fact, even considering only three low-cost hardware peers it was possible to obtain good performance results considering that the use of Fog-Care architecture in a widely populated country would be multiple fog nodes, such as 1 per state and better hardware as well. Considering the linear scalability found in the results of latency, send rate, and throughput, a blockchain with one peer

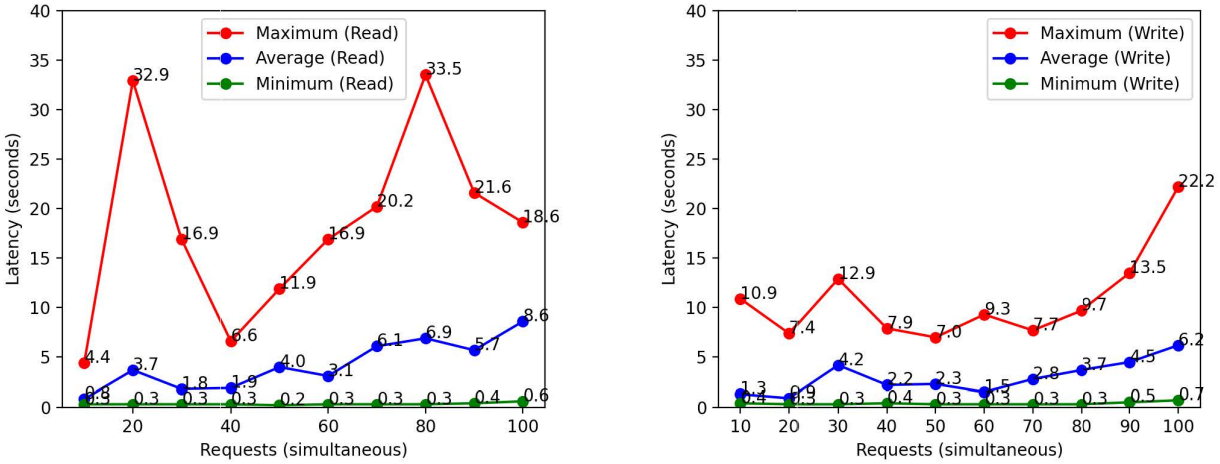


FIGURE 7. Minimum, maximum and average latency - read and write operations.

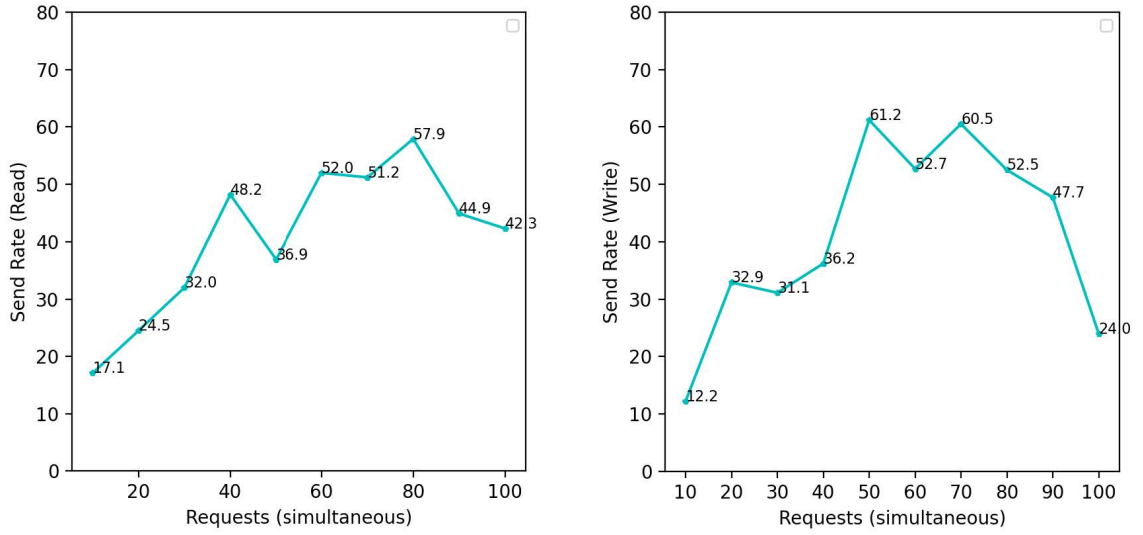


FIGURE 8. Send rate - read and write operations.

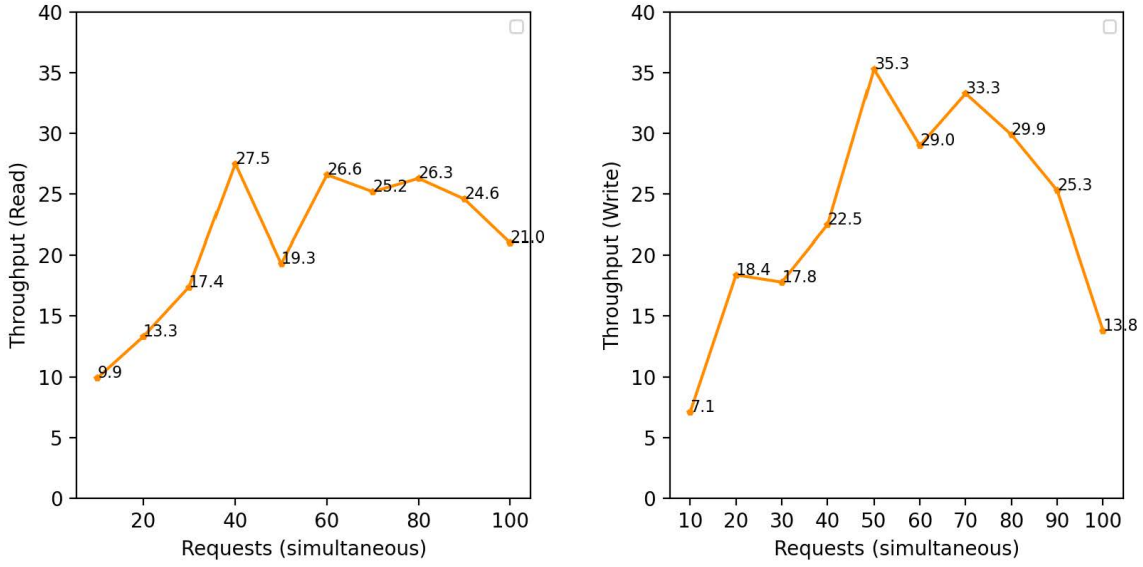


FIGURE 9. Throughput - read and write operations.

per state will certainly be able to handle a larger workload and more than 10 million transactions per day.

VI. DISCUSSION

In this section, is discussed the result of the performance of the executed tests.

Remembering that all the results were considered of an average of 5 executions of the same smart contract code. Both read and write methods. After this procedure, outliers were removed using the Interquartile Range - IQR method described in the Materials and Methods section. It was also grouped them in reading Operations and Write Operations.

The transaction throughput and latency metrics are two most relevant performance metrics of blockchain and they have not always satisfactory in recent popular blockchain applications [53]

The result of the performance evaluation in latency is considered satisfactory for the scope of this project. Both read and write minimum latency are under 1 second, indicating that in optimal conditions the scalability is possible. Since about the 60 transaction requests, the transaction per second begins to grow quickly.

One of the most important metrics is the average latency. The result shows a crescent result with good support delay until 100 transactions per second. It can be noticed that due to network traffic of a wide geographic dispersed network, some little seconds are expected. Considering these results, It can be inferred that the Fog-Care Architecture can support a vaccination of about 27.5 shots per second, or more than 2.300.000 shots per day, in this use case.

The good performance of Throughput, witch is characterized by a measure of how many operations are transactions processed per second. As the values increases to between 70 and 80 transactions load, there are 26.3 and 33.3 transactions per second in a read and write operation. Comparing these values of the performance of send rate, the rate at which Caliper send the transactions (57.9 and 60.5 for reading and writing), indicating that the number of transactions effectively processed is suitable to support more than 50% of the transactions send.

As the blockchain size increases, processing power, storage, and throughput need also increase or it will not be possible for all nodes to process blocks at some point [54]. The limitation of results consider 3 peers in blockchain, 1 being the orderer in a standard t2.micro AWS machine. This type of virtual machine is very basic and the focus is low cost with reasonable computer performance. The support of scalability can be made through the adding of at least 2 more peers and allocation of better CPU end Memory virtual machines, but the value of 1 peer/fog node per state is the ideal. Some limitations of blockchain testing should be considered, because the test environment can drastically affect the results. Some examples are: the geographic distribution of nodes, weather the nodes and peers are dispersed, not in a local environment, the type of hardware of virtual machines, the type of data stored, the number of nodes involved in a transaction, and the complexity of the smart contract. This work differs from others, because it was used a wide geographical approach (Brazil, United Stated and United Kingdom), considering testing the blockchain not in a local environment, but in a simulated global vaccination use case. In this case, the latency, throughput, and send rate are strongly affected by the distance between peers and orderer, since each transaction operation must be accepted and replicated by computers in different continents, compared to related works which generally run your tests in a single machine or a small local area network. Despite the use of several fog nodes for improve the scalability, the results achieved with this tests can be compared with future related works because the use of a standard parameter like number of rounds, rate control, total transactions, and others provided by the Caliper tool permits emulate the environment and test alternatives configurations. There are several approaches that can be used to improve the scalability, such as increasing the block size, reducing the transaction size or reducing the quantity of transaction processed by the nodes [55]. The alternative of increase the block size includes more transactions per block in order to increase the throughput, but this approach need more nodes to process the data and causes more delay due the propagation process. Reducing the transaction size by increasing the number of transaction per block is also an alternative, reducing the necessary digital signature per block. The last choice can be the reduction of transactions processed by nodes, which can be achieved by the use of off-chain transactions, increasing the throughout.

VII. CONCLUSION

Technology is considered a great allied tool to healthcare. In the current scientific environment, there are many good related works and available computer technologies like cloud computing, fog, and blockchain that can be potentially applied to healthcare area. However, many of these works discusses challenges and performance issues considering small local environments, like a single hospital or a group of them in a local and centralized area. With the arrive of COVID pandemic, many scientists and organizations are focusing on global wide healthcare solutions and applications. This article demonstrated the design,implementation and evaluation of a healthcare software architecture focused on mitigating latency, and improving scalability considering healthcare privacy issues in a dispersed and global environment. It was implemented a prototype of a software evaluating with success a hypothetical scenario where a global integrated vaccination campaign is adopted, simulating a solution approach based on an integrated blockchain and fog computing technologies. from the results, it can be concluded that (1) in terms of scalability is crucial to add more fog nodes, like one per state to support the increase of demand of transactions in a blockchain with wide nodes dispersed. (2) the average latency of transactions is just a few seconds even 100 of simultaneous requests per peer are considered. (3) As the send rate increases, approximately half of the transactions are actually processed at that time, according to the throughput

results. (4) privacy can be supported and treated globally with blockchain with the writing of blockchain smart contracts that represent these features. (5) The no mutation and integrity of the ledger in a healthcare global environment can help to protect the privacy of the patients. (6) the unique and globally identification of persons and resources are necessary and can be made with GS1 Standards properly. (7) It is possible to implement better political decision-making and a more global coordinated healthcare strategy with faster and earlier results available. For future work, we intend to evaluate the architecture with the inclusion of several changes. Firstly, a increase number of more peers, such as 3, 5 7 and 9. A different network with more Fog nodes, different parameters of smart contract benchmark and other virtual machine configuration to comparing the results.

ACKNOWLEDGMENT

The authors would like to thank the Spanish Agencia Estatal de Investigación. Project Monitoring and tracking systems for the improvement of intelligent mobility and behavior analysis (SiMoMIAC). PID2019-108883RB-C21 / AEI / 10.13039/501100011033 for supporting parts of this study. We would also thank the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES (Brazil), Conselho Nacional de Desenvolvimento Científico e Tecológico (Brazil), and Instituto Federal de Educação, Ciência e Tecnologia -IFRS (Brazil).

REFERENCES

[1] A. Roehrs, C. A. da Costa, R. da Rosa Righi, V. F. da Silva, J. R. Goldim, and D. C. Schmidt, "Analyzing the performance of a blockchain-based personal health record implementation," *J. Biomed. Informat.*, vol. 92, Apr. 2019, Art. no. 103140.
[2] H. J. de Moura Costa, C. A. da Costa, R. da Rosa Righi, and R. S. Antunes, "Fog computing in health: A systematic literature review," *Health Technol.*, vol. 10, no. 5, pp. 1025–1044, Sep. 2020.
[3] P. Mell and T. Grance, "The NIST definition of cloud computing," *Commun. ACM*, vol. 53, no. 6, p. 50, 2011.
[4] L. Cerina, S. Notargiacomo, M. G. Paccanit, and M. D. Santambrogio, "A fog-computing architecture for preventive healthcare and assisted living in smart ambients," in *Proc. IEEE 3rd Int. Forum Res. Technol. Soc. Ind. (RTSI)*, Sep. 2017, pp. 1–6.
[5] M. Iorga, *et al.* "Fog computing conceptual model," NIST (SP), Nat. Inst. Standards Technol., Tech. Rep. 500-325, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf, doi: 10.6028/NIST.SP.500-325.
[6] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2016.
[7] F. Andriopoulou, T. Dagiuklas, and T. Orphanoudakis, "Integrating IoT and fog computing for healthcare service delivery," in *Components and Services for IoT Platforms*, G. Keramidas, N. Voros, M. Hübner, Eds. Cham, Switzerland: Springer, 2017, pp. 213–232, doi: 10.1007/978-3-319-42304-3_11.
[8] G. Mokhtari, A. Anvari-Moghaddam, and Q. Zhang, "A new layered architecture for future big data-driven smart Homes," *IEEE Access*, vol. 7, pp. 19002–19012, 2019.
[9] Y. Harbi, Z. Aliouat, A. Refoufi, and S. Harous, "Recent security trends in Internet of Things: A comprehensive survey," *IEEE Access*, vol. 9, pp. 113292–113314, 2021.
[10] J. Kharel, H. T. Reda, and S. Y. Shin, "An architecture for smart health monitoring system based," *J. Commun.*, vol. 12, no. 4, pp. 228–233, 2017.
[11] M. Debe, K. Salah, M. H. U. Rehman, and D. Svetinovic, "Blockchain-based decentralized reverse bidding in fog computing," *IEEE Access*, vol. 8, pp. 81686–81697, 2020.
[12] C. Nunez-Gomez, B. Caminero, and C. Carrion, "HIDRA: A distributed blockchain-based architecture for Fog/Edge computing environments," *IEEE Access*, vol. 9, pp. 75231–75251, 2021.
[13] A. M. Elmisery, S. Rho, and M. Aborizka, "A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services," *Cluster Comput.*, vol. 22, pp. 1–28, Jan. 2017.
[14] A. Kraemer, E. Braten, N. Tamkittikhun, D. Palma, P. Liljeberg, and H. Tenhunen, "Fog computing in healthcare—A review and discussion," *IEEE Access*, vol. 5, pp. 9206–9222, 2017.
[15] P. G. Shynu, V. G. Menon, R. L. Kumar, S. Kadry, and Y. Nam, "Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing," *IEEE Access*, vol. 9, pp. 45706–45720, 2021.
[16] M. Whaiduzzaman, M. J. N. Mahi, A. Barros, M. I. Khalil, C. Fidge, and R. Buyya, "BFIM: Performance measurement of a blockchain based hierarchical tree layered fog-IoT microservice architecture," *IEEE Access*, vol. 9, pp. 106655–106674, 2021.
[17] Q. Wang, T. Ji, Y. Guo, L. Yu, X. Chen, and P. Li, "TrafficChain: A blockchain-based secure and privacy-preserving traffic map," *IEEE Access*, vol. 8, pp. 60598–60612, 2020.
[18] R. A. Memon, J. P. Li, M. I. Nazeer, A. N. Khan, and J. Ahmed, "DualFog-IoT: Additional fog layer for solving blockchain integration problem in Internet of Things," *IEEE Access*, vol. 7, pp. 169073–169093, 2019.
[19] J. Al-Jaroodi, N. Mohamed, and E. Abukhousa, "Health 4.0: On the way to realizing the healthcare of the future," *IEEE Access*, vol. 8, pp. 211189–211210, 2020.
[20] G. Leeming, J. Ainsworth, and D. A. Clifton, "Blockchain in health care: Hype, trust, and digital health," *Lancet*, vol. 393, no. 10190, pp. 2476–2477, Jun. 2019.
[21] A. Rejeb and L. Bell, "Potentials of blockchain for healthcare: Case of Tunisia," Sci. Publishing House 'DARWIN', West Pomerania, Poland, Tech. Rep. 22, 2019. [Online]. Available: https://bibliotekanauki.pl/articles/1046533
[22] (2020). GS1. *About GS1*. [Online]. Available: https://www.gs1.org/about
[23] D. Templeton, "Be an early riser. There's still time to prepare hospitals for global location number sunrise," *Modern Healthcare*, vol. 40, no. 10, p. 23, 2010.
[24] B. K. Smith, H. Nachtmann, and E. A. Pohl, "Improving healthcare supply chain processes via data standardization," *Eng. Manage. J.*, vol. 24, no. 1, pp. 3–10, Mar. 2012.
[25] R. Jayaraman, N. Buyurgan, R. L. Rardin, V. M. Varghese, and J. A. Pazour, "An exploratory pilot study on supply chain data standards in a hospital pharmacy," *Eng. Manage. J.*, vol. 27, no. 3, pp. 141–151, Jul. 2015.
[26] A. H. Mayer, V. F. Rodrigues, C. A. D. Costa, R. D. R. Righi, A. Roehrs, and R. S. Antunes, "FogChain: A fog computing architecture integrating blockchain and Internet of Things for personal health records," *IEEE Access*, vol. 9, pp. 122723–122737, 2021.
[27] (2021). *IEEE Xplore*. Accessed: Dec. 20, 2021. [Online]. Available: https://ieeexplore.ieee.org
[28] (2021). *Science Direct*. Accessed: Dec. 20, 2021. [Online]. Available: https://www.sciencedirect.com
[29] (2021). *Google Scholar*. Accessed: Dec. 20, 2021. [Online]. Available: https://scholar.google.com
[30] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, "FogBus: A blockchain-based lightweight framework for edge and fog computing," *J. Syst. Softw.*, vol. 154, pp. 22–36, Aug. 2019.
[31] A. A. Mutlag, M. K. A. Ghani, M. A. Mohammed, M. S. Maashi, O. Mohd, S. A. Mostafa, K. H. Abdulkareem, G. Marques, and I. de la Torre Díez, "MAFC: Multi-agent fog computing model for healthcare critical tasks management," *Sensors*, vol. 20, no. 7, p. 1853, Mar. 2020.
[32] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102407.
[33] K. M. Hossein, M. E. Esmaeili, T. Dargahi, A. Khonsari, and M. Conti, "BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications," *Comput. Commun.*, vol. 180, pp. 31–47, Dec. 2021.
[34] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. H. Ur Rehman, and C. A. Kerrache, "The case of HyperLedger fabric as a blockchain solution for healthcare applications," *Blockchain, Res. Appl.*, vol. 2, no. 1, Mar. 2021, Art. no. 100012.
[35] N. Islam, Y. Faheem, I. U. Din, M. Talha, M. Guizani, and M. Khalil, "A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services," *Future Gener. Comput. Syst.*, vol. 100, pp. 569–578, Nov. 2019.

[36] S. Shukla, S. Thakur, S. Hussain, J. G. Breslin, and S. M. Jameel, "Identification and authentication in healthcare Internet-of-Things using integrated fog computing based blockchain model," *Internet Things*, vol. 15, Sep. 2021, Art. no. 100422.

[37] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, and M. A. Imran, "BeepTrace: Blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3915–3929, Mar. 2021.

[38] L. Fetjah, K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "Towards a smart healthcare system: An architecture based on iot, blockchain, and fog computing," *Int. J. Healthcare Inf. Syst. Informat. (IJHISI)*, vol. 16, no. 4, pp. 1–18, 2021.

[39] D. Kritchanchai, S. Hoeur, and P. Engelseth, "Develop a strategy for improving healthcare logistics performance," in *Supply Chain Forum: An International Journal*, vol. 19. London, U.K.: Taylor & Francis, 2018, pp. 55–69. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/16258312.2017.1416876, doi: 10.1080/16258312.2017.1416876 .

[40] R. Barik, H. Dubey, S. Sasane, C. Misra, N. Constant, and K. Mankodiya, "Fog2Fog: Augmenting scalability in fog computing for health GIS systems," in *Proc. IEEE/ACM Int. Conf. Connected Health: Appl., Syst. Eng. Technol. (CHASE)*, Jul. 2017, pp. 241–242.

[41] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Generat. Comput. Syst.*, vol. 78, pp. 659–676, Jan. 2018.

[42] S. Nastic, T. Rausch, O. Scekic, S. Dustdar, M. Gusev, B. Koteska, M. Kostoska, B. Jakimovski, S. Ristov, and R. Prodan, "A serverless real-time data analytics platform for edge computing," *IEEE Internet Comput.*, vol. 21, no. 4, pp. 64–71, Jul. 2017.

[43] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, 2016.

[44] F. Pereira, P. Crocker, and V. R. Q. Leithardt, "PADRES: Tool for PrivAcy, data REgulation and security," *SoftwareX*, vol. 17, Jan. 2022, Art. no. 100895.

[45] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," 2019, *arXiv:1906.11078*.

[46] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan./Feb. 2018.

[47] M. Debe, K. Salah, M. H. Ur Rehman, and D. Svetinovic, "Monetization of services provided by public fog nodes using blockchain and smart contracts," *IEEE Access*, vol. 8, pp. 20118–20128, 2020.

[48] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, "Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges," *IEEE Access*, vol. 8, pp. 24746–24772, 2020.

[49] 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.

[50] H. Ritchie, E. Mathieu, L. Rodés-Guirao, C. Appel, C. Giattino, E. Ortiz-Ospina, J. Hasell, B. Macdonald, D. Beltekian and M. Roser. (2020). *Coronavirus pandemic (COVID-19)*. Our World in Data. [Online]. Available: https://ourworldindata.org/coronavirus

[51] (2012). *Amazon EC2 T2 Instances*. Accessed: Aug. 15, 2019. [Online]. Available: https://aws.amazon.com/ec2/instance-types/t2/

[52] (2021). *Hyperledger Blockchain Performance Metrics*. Accessed: Dec. 20, 2021. [Online]. Available: https://www.hyperledger.org/learn/publications/blockchain-performance-metrics

[53] P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, "A detailed and real-time performance monitoring framework for blockchain systems," in *Proc. IEEE/ACM 40th Int. Conf. Softw. Eng., Softw. Eng. Practice Track (ICSE-SEIP)*, New York, NY, USA, May 2018, pp. 134–143.

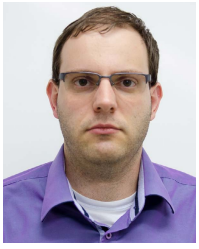
[54] I. Romashkova, M. Komarov, and A. Ometov, "Demystifying blockchain technology for resource-constrained IoT devices: Parameters, challenges and future perspective," *IEEE Access*, vol. 9, pp. 129264–129277, 2021.

[55] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Netw.*, vol. 33, no. 5, pp. 166–173, Sep. 2019.

HUMBERTO JORGE DE MOURA COSTA (Member, IEEE) received the master's degree in applied computing graduate program from the Universidade do Vale do Rio dos Sinos—UNISINOS, where he is currently pursuing the Ph.D. degree. He is a Professor at the Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul—IFRS. He is a member of ACM.

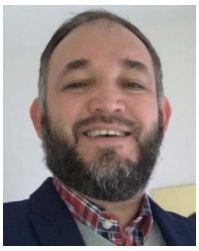
CRISTIANO ANDRÉ DA COSTA (Senior Member, IEEE) received the Ph.D. degree in computer science from UFRGS University, Brazil, in 2008. He is currently a Full Professor at the Universidade do Vale do Rio dos Sinos (UNISINOS), Brazil; and a Researcher on productivity at the National Council for Scientific and Technological Development (CNPq). His research interests include ubiquitous, mobile, parallel, and distributed computing. He is a member of ACM and the Brazilian Computer Society.

RODRIGO DA ROSA RIGHI (Senior Member, IEEE) received the Ph.D. degree in computer science from UFRGS, Brazil, in 2009. He has concluded his postdoctoral studies at the Korea Advanced Institute of Science and Technology (KAIST), under the following topics: RFID and cloud computing. He is currently an Assistant Professor and a Researcher at the University of Vale do Rio dos Sinos, Brazil. His research interests include load balancing and process migration. He is a member of ACM.



RODOLFO STOFFEL ANTUNES (Member, IEEE) received the B.Sc. degree in computer science from the Universidade do Vale do Rio dos Sinos (UNISINOS), in 2009, and the Ph.D. degree in computer science from the Universidade Federal do Rio Grande do Sul (UFRGS), in 2016. He is currently an Assistant Professor and a Researcher at UNISINOS. His research interests include the Internet of Things, information-centric networking, distributed systems, and mobile and ubiquitous computing.

JUAN FRANCISCO DE PAZ SANTANA received the degree in technical engineering in systems computer sciences, in 2003, and the Engineering degree in computer sciences, the degree in statistics, and the Ph.D. degree in computer science from the University of Salamanca, Spain, in 2005, 2007, and 2010, respectively. He is currently a Full Professor with the University of Salamanca, where he is also a Researcher with the Expert Systems and Applications Laboratory (ESALab). He has been a coauthor of published articles in several journals, workshops, and symposiums.



VALDERI REIS QUIETINHO LEITHARDT (Member, IEEE) received the Ph.D. degree in computer science from INF-UFRGS, Brazil, in 2015. He is currently a Professor with the Polytechnic Institute of Portalegre and a Researcher integrated with the VALORIZA—Research Centre for Endogenous Resource Valorization. He is also a Collaborating Researcher at the Expert Systems and Applications Laboratory (ESALab), University of Salamanca, Spain. His mainline of research interests include distributed systems with a focus on data privacy, communication, and programming protocols, involving scenarios and applications for the Internet of Things, smart cities, big data, cloud computing, and blockchain.